Ivan Korec

# Structures related to Pascal's triangle modulo $2$ and their elementary theories

*Mathematica Slovaca*, Vol. 44 (1994), No. 5, 531--554

Persistent URL: http://dml.cz/dmlcz/136627

Mathematica Slovaca
©1994
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **44** (1994), No. 5, 531–554

# STRUCTURES RELATED TO PASCAL'S TRIANGLE MODULO 2 AND THEIR ELEMENTARY THEORIES

IVAN KOREC[1]

(Communicated by Stanislav Jakubec)

ABSTRACT. The elementary theory of the structure $(\mathbb{N}; B_2)$, where $\mathbb{N}$ is the set of nonnegative integers and $B_2(x,y) = \binom{x+y}{x} \text{ MOD } 2$, is decidable. On the other hand, addition and multiplication on $\mathbb{N}$ are definable in the structure $(\mathbb{N}; B_2, \mathrm{Sq})$, where Sq is the set of squares of integers, and hence the elementary theory of $(\mathbb{N}; B_2, \mathrm{Sq})$ is undecidable. Further definability results are presented.

## 1. Introduction and notation

Let $\mathbb{N}$ denote the set of nonnegative integers, Sq the set of their squares, $\leq$ the usual ordering of $\mathbb{N}$, and $|$ the divisibility relation on $\mathbb{N}$. The digits $0, 1, 2, \ldots$ will be used in their usual sense and $+$, $\times$, $\mathbf{s}$, $\mathbf{p}$ will denote the usual addition, multiplication, successor and predecessor, respectively (i.e. $\mathbf{p}(x+1) = x$ for every $x \in \mathbb{N}$ and $\mathbf{p}(0) = 0$). Let DIV, MOD denote the quotient and the remainder for integer division, and let gcd denote the greatest common divisor. Further, let $\binom{x}{y}$ denote the binomial coefficient, and let $B_2$ be the binary function on $\mathbb{N}$ defined by

$$B_2(x,y) = \binom{x+y}{x} \text{ MOD } 2\,. \tag{1.1}$$

The function $B_2$ will be called *Pascal's triangle modulo* 2. It can be displayed in the plane in the way usually used for the classical Pascal triangle $B(x,y) =$

AMS Subject Classification (1991): Primary 11B65. Secondary 68Q80.
Key words: Pascal's triangle, Decidability, Elementary definability,.
[1] This work was supported by Grant 363 of Slovak Academy of Sciences.

$\binom{x+y}{x}$. Some special symbols will be introduced later. For example, the formula $x \sqsubseteq y$ will mean that the binary digits of $x$ are less than or equal to the corresponding digits of $y$.

For the notions of the (first order) formulae, truth etc. we refer to [Sh] or to some other textbook on mathematical logic. However, we do not distinguish between the function or predicate and the corresponding symbol for it. The equality sign is considered as a logical symbol. If $\leq$ on $\mathbb{N}$ is defined in a considered structure, we shall also freely use $<$, $>$, $\geq$; moreover, since $0, 1, 2, \ldots$ and $\mathbf{s}$, $\mathbf{p}$ are also first order definable we may use them, too. The letters $v$, $w$, $x$, $y$, $z$ (possibly with subscripts) will be used as individual variables in formulae, the symbols $\neg$, $\wedge$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$ as logical connectives (they are written in the order given by their priorities) and $\exists$, $\forall$ as quantifiers. The symbol $\exists!$ will denote "there is exactly one". The signs $\bigwedge$, $\bigvee$ will abbreviate conjunction and disjunction of several formulae, respectively; to specify these formulae, metavariables $i, j, k, \ldots$ will also be used. We shall work rather with the truth (and satisfiability) than with the provability.

A relation $R \subseteq A^n$ is *first order* (or: *elementarily*) *definable* in the structure $\mathcal{A} = (A; S_1, \ldots, S_k)$ if there is a first order formula $\sigma(x_1, \ldots, x_n)$ with no non-logical symbols except $S_1, \ldots, S_k$ and no free variables except $x_1, \ldots, x_n$ such that the formula

$$R(x_1, \ldots, x_n) \Longleftrightarrow \sigma(x_1, \ldots, x_n)$$

is true in the structure $\mathcal{A}' = (A; S_1, \ldots, S_k, R)$. For functions we introduce a similar definition. (We do not consider parametrical definability unless explicitly mentioned.) We shall say that the structure $\mathcal{A}$ is *d-weaker* than the structure $\mathcal{B}$ if both structures have the same base sets and all functions and relations of $\mathcal{A}$ are first order definable in $\mathcal{B}$. Two structures will be called *d-equivalent* if each of them is d-weaker than the other. We shall also use the terms *strictly d-weaker* and (*strictly*) *d-stronger* in the obvious sense.

All structures considered in the present paper will have the same domain $\mathbb{N}$, they will have finitely many basic relations and operations, which will be recursive. (We shall not build the (meta-)theory of this class. If yes, maybe "arithmetical" would be more suitable than "recursive".) The structure $(\mathbb{N}; +, \times)$ is the d-strongest structure among them. Its first order theory (the true first order arithmetic) is the most complicated; it is not recursively axiomatizable (Gödel Incompleteness Theorem), and even not arithmetical.

Definability of some predicates or functions on the set $\mathbb{N}$ from other predicates or functions on $\mathbb{N}$ has been widely investigated, see e.g. [Ri], [Ro], [Se] and [Wo]. For example, $\times$ is first order definable in $(\mathbb{N}; +, \mathrm{Sq})$. To show that,

we can define the operation of squaring, and then multiplication as follows:

$$\begin{aligned} y = sqr(x) &\iff \mathrm{Sq}(y) \wedge \mathrm{Sq}(y + x + x + 1) \\ &\quad \wedge \forall z\,(z > x \wedge \mathrm{Sq}(z) \implies y + x + x + 1 \leq z)\,; \qquad (1.2) \\ z = x \times y &\iff sqr(x + y) = sqr(x) + z + z + sqr(y)\,. \end{aligned}$$

Hence the structure $(\mathbb{N}; +, \mathrm{Sq})$ is d-equivalent to $(\mathbb{N}; +, \times)$. A deeper result is that $(\mathbb{N}; \mathbf{s}, |)$, where $|$ is the divisibility relation, is d-equivalent to $(\mathbb{N}; +, \times)$. On the other hand, $\leq$ is not definable in $(\mathbb{N}; \mathbf{s})$, and analogously the relation $\leq$ does not suffice to define $+$, and $+$ does not suffice to define $\times$. (This concerns the definability by first order formulae; for second order definability, $\mathbf{s}$ suffices to define $\leq$, $+$, $\times$.)

In the present paper we shall investigate the structure $(\mathbb{N}; B_2)$ and some richer structures obtained by adding further basic relations or operations into them. We will be interested whether (the usual) addition $+$ and multiplication $\times$ are first order definable in them. It will also be proved that the elementary theory of $(\mathbb{N}; B_2)$ is decidable, and hence $+$, $\times$ are not definable in it.

Many other problems concerning Pascal triangles modulo 2, or more generally modulo $n$ (which can be defined in the obvious way) have been investigated e.g. in [Si] and [Bo] (where a wide bibliography was contained). Some algorithmic questions are considered in [K1] and [K2]. The main result of [K3] states that the structure $(\mathbb{N}; B_n)$ is d-equivalent to $(\mathbb{N}; +, \times)$ provided $n > 0$ is divisible by two distinct primes.

## 2. The structures $(\mathbb{N}; B_2)$ and $(\mathbb{N}; \sqsubseteq)$

The results of this section are contained in [K3], where they are proved in a more general form, for arbitrary prime instead of 2. We shall repeat them here because the notation will be useful in the following sections, and because the formalism is sometimes much simpler than in the general case.

All integers are considered in their binary representation. (This concerns their digits, addition carries etc.) If a number is given by its digits $a_r, a_{r-1}, \ldots, a_0$ we shall write $m = [a_r a_{r-1} \ldots a_0]_2$. Leading zeros are allowed if necessary (e.g., to have equal numbers of digits in two integers).

Our main tool will be the following consequence of Lucas' theorem, see e.g. [Bo].

**LEMMA 2.1.** *If* $x = [a_r \dots a_1 a_0]_2$, $y = [b_r \dots b_1 b_0]_2$, *then*

$$B_2(x,y) = 0 \iff a_i = b_i = 1 \text{ for some } i \in \{0,1,\dots,r\}.$$

In words, $B_2(x,y) = 0$ if and only if a carry occurs in the computation of $x + y$. Let $x \sqsubseteq y$ mean that the binary digits of $x$ are less or equal than the corresponding binary digits of $y$. For example, $4 \sqsubseteq 7$, $4 \not\sqsubseteq 9$ because $4 = [100]_2 = [0100]_2$, $7 = [111]_2$, $9 = [1001]_2$. Since the formulae

$$x \sqsubseteq y \iff \forall z \left(B_2(x,z) = 0 \implies B_2(y,z) = 0\right)$$
$$x = 1 \iff \exists y \forall z \left(B_2(y,z) = x\right)$$

are true in the structure $(\mathbb{N}; B_2, \sqsubseteq, 1)$, we have:

**LEMMA 2.2.** *The predicate* $\sqsubseteq$ *and the constant* 1 *are first order definable in the structure* $(\mathbb{N}; B_2)$.

Now we shall give a list of predicates and functions which are definable in the structure $(\mathbb{N}; \sqsubseteq)$. Of course, Lemma 2.2 implies that each of them is also definable in the structure $(\mathbb{N}; B_2)$. To avoid duplicity, we introduce notation and explain it immediately in the lemma. Notice also that $(\mathbb{N}; \sqsubseteq)$ is a partially ordered set (and even a distributive lattice, in essence). We can also consider any $x \in \mathbb{N}$ as a code of the finite set of powers of 2 whose sum is $x$. Then $\sqsubseteq$ can be understood as the set inclusion. These remarks are given only to explain the system of notation below. (In most cases we follow [K3], but we often delete the subscript 2.)

**LEMMA 2.3.** *The following predicates and functions are first order definable in the structure* $(\mathbb{N}; \sqsubseteq)$:

| | |
|---|---|
| $x \sqsubset y$ | *proper set inclusion;* |
| $x \prec y$ | *covering relation in* $(\mathbb{N}; \sqsubseteq)$; |
| $x \sqcap y$ | *meet operation in* $(\mathbb{N}; \sqsubseteq)$; |
| $x \sqcup y$ | *join operation in* $(\mathbb{N}; \sqsubseteq)$; |
| $0$ | *the constant* 0 *(zero);* |
| $\mathrm{Pow}_2(x)$ | $x$ *is a power of* 2; |
| $\mathrm{EqB}_2(u,v,x,y)$ | $B_2(u,v) = B_2(x,y)$; |
| $\mathrm{CFAdd}(x,y,z)$ | *carry-free addition:* $x + y = z$, *and no carry occurs when* $x + y$ *is computed.* |

P r o o f. We shall give defining formulae, without any comment.

$$
\begin{aligned}
x \sqsubset y &\iff x \sqsubseteq y \wedge x \neq y\,;\\
x \prec y &\iff x \sqsubset y \wedge \neg\exists z\,(x \sqsubset z \wedge z \sqsubset y)\,;\\
z = x \sqcap y &\iff z \sqsubseteq x \wedge z \sqsubseteq y \wedge \forall w\,(w \sqsubseteq x \wedge w \sqsubseteq y \implies w \sqsubseteq z)\,;\\
z = x \sqcup y &\iff x \sqsubseteq z \wedge y \sqsubseteq z \wedge \forall w\,(x \sqsubseteq w \wedge y \sqsubseteq w \implies z \sqsubseteq w)\,;\\
x = 0 &\iff \forall y\,(x \sqsubseteq y)\,;\\
\mathrm{Pow}_2(x) &\iff 0 \prec x\,;\\
\mathrm{EqB}_2(u,v,x,y) &\iff (u \sqcap v = 0 \iff x \sqcap y = 0);\\
\mathrm{CFAdd}(x,y,z) &\iff x \sqcup y = z \wedge x \sqcap y = 0\,.
\end{aligned}
$$

□

**LEMMA 2.4.** *The function $B_2$ is first order definable in $(\mathbb{N};\sqsubseteq,1)$.*

P r o o f. We can define $\sqcup$ as in Lemma 2.3, and then

$$z = B_2(x,y) \iff x \sqcap y = 0 \wedge z = 1 \vee x \sqcap y \neq 0 \wedge z = 0\,.$$

□

**LEMMA 2.5.**

(i) *No nonzero constant is first order definable in $(\mathbb{N};\sqsubseteq)$.*
(ii) *No constant except $0$, $1$ is first order definable in $(\mathbb{N};B_2)$.*
(iii) *The operations $+$, $\times$ are first order definable neither in $(\mathbb{N};B_2)$ nor in $(\mathbb{N};\sqsubseteq)$.*

P r o o f. Every permutation $\varphi$ of the set $\mathrm{Pow}_2$ (or of $\mathrm{Pow}_2\setminus\{1\}$) induces an automorphism $\overline{\varphi}$ of the structure $(\mathbb{N};\sqsubseteq)$ (of $(\mathbb{N};B_2)$, respectively). The automorphism $\overline{\varphi}$ can be defined by

$$\overline{\varphi}\left(\sum_{i=0}^{n} a_i \cdot 2^i\right) = \sum_{i=0}^{n} a_i \varphi(2^i) \qquad \text{for all } n \in \mathbb{N} \text{ and } a_i \in \{0,1\},\ 0 \leq i \leq n\,. \tag{2.5.1}$$

Every definable function or operation must be invariant under all of these automorphisms. In particular, every definable constant must be their fixed point; this condition is only fulfilled for $0$ in case (i) and for $0$, $1$ in case (ii). To prove (iii), it suffices to consider any nontrivial automorphism of the considered structures; neither $+$ nor $\times$ is invariant under it. □

A similar argument will often be used below to prove that some relations or functions are not definable. We shall refer to it as to the automorphism argument.

**THEOREM 2.6.**

(i) *The structures* $(\mathbb{N}, \mathrm{EqB}_2)$, $(\mathbb{N}; \sqsubseteq)$, $(\mathbb{N}; \sqcap)$ *are d-equivalent.*

(ii) *The structures* $(\mathbb{N}; B_2)$, $(\mathbb{N}; \sqsubseteq, 1)$, $(\mathbb{N}; \sqcap, 1)$ *are d-equivalent.*

(iii) *The structures in* (i) *are strictly d-weaker than the structures in* (ii).

P r o o f. For (i) and (ii) it suffices to show that $\sqsubseteq$ is definable in $(\mathbb{N}, \mathrm{EqB}_2)$; all other necessary definitions are contained in Lemmas 2.2, 2.3, 2.4. We can define

$$\mathrm{ZB}_2(x,y) \iff x \neq 0 \wedge \mathrm{EqB}_2(x,y,x,x) \vee y \neq 0 \wedge \mathrm{EqB}_2(x,y,y,y)\,;$$

$$x \sqsubseteq y \iff \forall z \left(\mathrm{ZB}_2(x,z) \implies \mathrm{ZB}_2(y,z)\right).$$

Here $\mathrm{ZB}_2(x,y)$ replaces $B_2(x,y) = 0$; notice that the function $B_2$ itself cannot be defined.

The statement (iii) follows from Lemma 2.5. The constant 1 is definable in the structures of (ii) but it is not definable in the structures of (i). (Of course, the statement (iii) would fail if *parametrical* definability is considered.) □

**THEOREM 2.7.** *The elementary theories of the structures* $(\mathbb{N}; \sqsubseteq)$, $(\mathbb{N}; \sqsubseteq, 1)$ *and* $(\mathbb{N}; B_2)$ *are decidable.*

P r o o f. It can be easily verified that $(\mathbb{N}; \sqsubseteq)$ is a distributive relative complemented lattice, and by [Ye; p. 281, Proposition 2.1], every such lattice has decidable elementary theory. The elementary theory of $(\mathbb{N}; \sqsubseteq, 1)$ is also decidable because any its formula $\alpha(1)$ is true in $(\mathbb{N}; \sqsubseteq, 1)$ if and only if the formula $0 \prec y \implies \alpha(\dot{y})$ is true in $(\mathbb{N}; \sqsubseteq)$ (here $y$ is a variable which does not occur in $\alpha(1)$). The third structure is d-weaker than (in fact, d-equivalent to) the structure $(\mathbb{N}; \sqsubseteq, 1)$, and hence its elementary theory is decidable, too. □

## 3. The structure $(\mathbb{N}; B_2, +)$ and its d-equivalents

We shall investigate what relations or functions must be added to $(\mathbb{N}; B_2)$ or $(\mathbb{N}; \mathrm{EqB}_2)$ so that $+$ will be definable in the enriched structure. A very weak relation which suffices is

$$\mathrm{Neib} = \left\{(i,j) \mid\ i,j \in \mathbb{N} \wedge (i = j+1 \vee j = i+1)\right\}.$$

The author conjectures that the structure $(\mathbb{N}; \mathrm{Neib})$ is strictly d-weaker than the structure $(\mathbb{N}; \mathbf{s})$. Nevertheless, the constants $0, 1, 2, \ldots$ are definable:

$$x = 0 \iff \exists! y\ \mathrm{Neib}(x,y), \qquad x = 1 \iff \mathrm{Neib}(0,x),$$

$$x = 2 \iff x \neq 0 \wedge \mathrm{Neib}(1,x), \qquad \ldots$$

Therefore the structures $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{Neib})$ and $(\mathbb{N}; B_2, \mathrm{Neib})$ are d-equivalent.

**LEMMA 3.1.** *The addition* $+$ *is first order definable in* $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{Neib})$.

P r o o f. We shall start with the definition of an auxiliary function

$$\mathit{NextPow}_2(x) = \begin{cases} 2x & \text{if } x \text{ is a power of } 2\,, \\ 0 & \text{otherwise.} \end{cases} \tag{3.1.1}$$

It can be defined by the formula

$$\begin{aligned} y = \mathit{NextPow}_2(x) \iff & \neg\,\mathrm{Pow}_2(x) \wedge y = 0 \ \vee\ x = 1 \wedge y = 2 \\ & \vee\ \mathrm{Pow}_2(x) \wedge x \neq 1 \wedge \mathrm{Pow}_2(y) \wedge y \neq x \\ & \wedge\, \exists z \big(\mathrm{Neib}(x, z) \wedge \mathrm{Neib}(x \sqcup z, y)\big)\,. \end{aligned} \tag{3.1.2}$$

The above definition is based on the form of binary expansions of the integers $2^i - 1$, $i \in \mathbb{N}$: all their digits are equal to 1 (but the leading zeros if any).

As an idea for the definition of $z = x + y$ the usual algorithm of binary addition can be used. The definition looks like

$$\begin{aligned} z = x + y \iff \exists v \Big(1 \not\sqsubseteq v \wedge \forall w \Big(\mathrm{Pow}_2(w) \implies \mathbf{Sum}\big(w \sqsubseteq x, w \sqsubseteq y, \\ w \sqsubseteq v, w \sqsubseteq z, \mathit{NextPow}(w) \sqsubseteq v\big)\Big)\Big)\,, \end{aligned} \tag{3.1.3}$$

where $v$ is "the vector of carries" and $\mathbf{Sum}(q_1, q_2, q_3, q_4, q_5)$ is a suitable propositional formula. Its meaning can be expressed as $q_1 + q_2 + q_3 = q_4 + 2q_5$ provided that *true, false* are identified with the numbers 1, 0. □

As an immediate consequence we obtain:

**THEOREM 3.2.** *The structures* $(\mathbb{N}; B_2, \mathrm{Neib})$, $(\mathbb{N}; B_2, \mathbf{s})$, $(\mathbb{N}; B_2, \leq)$, $(\mathbb{N}; B_2, +)$, $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{Neib})$, $(\mathbb{N}; \mathrm{EqB}_2, \mathbf{s})$, $(\mathbb{N}; \mathrm{EqB}_2, \leq)$, $(\mathbb{N}; \mathrm{EqB}_2, +)$ *are d-equivalent.*

Besides Lemma 3.1 we need only usual definitions of $\leq$ from $+$, the successor from $\leq$, and a definition of Neib from $\mathbf{s}$, e.g.

$$\mathrm{Neib}(x, y) \iff y = \mathbf{s}(x) \vee x = \mathbf{s}(y)\,.$$

From now on we shall usually choose the structure $(\mathbb{N}; B_2, +)$ from the list in Theorem 3.2.

**THEOREM 3.3.** *The following structures are d-equivalent to* $(\mathbb{N}; B_2, +)$:
$(\mathbb{N}; \mathrm{EqB}_2, \mathit{mult}_2)$, *where* $\mathit{mult}_2(x) = 2x$ *for every* $x \in \mathbb{N}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathrm{SPow}_2)$, *where* $\mathrm{SPow}_2 = \{(2^i, 2^{i+1}) \mid i \in \mathbb{N}\}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_3)$, *where* $\mathrm{PMult}_3 = \{3 \cdot 2^i \mid i \in \mathbb{N}\}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathrm{NeibPow}_2)$,
*where* $\mathrm{NeibPow}_2 = \{(2^i, 2^j) \mid i, j \in \mathbb{N} \wedge (i = j + 1 \vee j = i + 1)\}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathrm{LePow}_2)$, *where* $\mathrm{LePow}_2 = \{(2^i, 2^{i+j}) \mid i, j \in \mathbb{N}\}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PrPow}_2)$, *where* $\mathrm{PrPow}_2 = \{2^i - 1 \mid i \in \mathbb{N}\}$;
$(\mathbb{N}; \mathrm{EqB}_2, \mathit{NextPow}_2)$, *where* $\mathit{NextPow}_2$ *is defined in* (3.1.1),
*and also the structures obtained from the above if* $\mathrm{EqB}_2$ *is replaced by* $B_2$.

P r o o f. Notice that the constant 1 is definable in each of the mentioned structures; for example

$$x = 1 \iff \mathrm{Pow}_2(x) \wedge \mathrm{PrPow}_2(x);$$
$$x = 1 \iff \mathrm{Pow}_2(x) \wedge \exists! y \left(\mathrm{PMult}_3(y) \wedge x \sqsubseteq y\right);$$
$$x = 1 \iff \mathrm{Pow}_2(x) \wedge \neg\exists y \left(x = \mathit{NextPow}_2(y)\right).$$

Therefore it is not substantial which of $\mathrm{EqB}_2$, $B_2$ occurs in the structures. Now the proof will be organized cyclically; the structures are considered in the order given in the theorem, and each of them is shown to be d-weaker than the previous one. The necessary defining formulae can be:

$$\begin{aligned}
y = \mathit{mult}_2(x) &\iff y = x + x;\\
\mathrm{SPow}_2(x, y) &\iff \mathrm{Pow}_2(x) \wedge y = \mathit{mult}_2(x);\\
\mathrm{PMult}_3(x) &\iff \exists y, z \left(\mathrm{SPow}_2(y, z) \wedge x = y \sqcup z\right);\\
\mathrm{NeibPow}_2(x, y) &\iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \mathrm{PMult}_3(x \sqcup y);\\
\mathrm{LePow}_2(x, y) &\iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y)\\
&\quad \wedge \exists z \left(1 \sqsubseteq z \wedge x \sqsubseteq z \wedge (y = x \vee y \not\sqsubseteq z)\right.\\
&\quad \left. \wedge \forall u, v \left(\mathrm{NeibPow}_2(u, v) \wedge u \sqsubseteq z \wedge u \neq x \implies v \sqsubseteq z\right)\right);\\
\mathrm{PrPow}_2(x) &\iff \forall u, v \left(\mathrm{LePow}_2(u, v) \wedge v \sqsubseteq x \implies u \sqsubseteq x\right);\\
y = \mathit{NextPow}_2(x) &\iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \exists! z \left(\mathrm{PrPow}_2(z) \wedge x \sqsubseteq z \wedge y \not\sqsubseteq z\right).
\end{aligned}$$

The cycle can be closed by the formula (3.1.3); therefore all structures in the cycle are d-equivalent. □

**THEOREM 3.4.** *Let* $a_0 < a_1 < \cdots < a_k$ *be nonnegative integers,*

$$n = \sum_{i=0}^{k} 2^{a_i}, \qquad g = \gcd(0, a_1 - a_0, \ldots, a_k - a_0),$$

*and* $\mathrm{PMult}_n = \{n \cdot 2^i \mid i \in \mathbb{N}\}$. *Then the structure* $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_n)$ *is d-equivalent to* $(\mathbb{N}; B_2, +)$ *if and only if* $a_0 \leq 1$ *and* $g = 1$.

P r o o f. If $n$ does not fulfil the conditions from the theorem, we can use the automorphism argument, see Lemma 2.5. If $g > 1$ and $\alpha$ is any non-identical permutation of the set $\{0, 1, \ldots, g-1\}$, then we can set $\varphi(2^{gi+j}) = 2^{gi+\alpha(j)}$. If $a_0 > 1$, then $\varphi$ can interchange 1 and 2, and be identical on other powers of 2. If $g = 0$, then $n$ is a power of 2, and $\varphi$ can arbitrarily permute the greater powers of 2. In all these cases $\varphi$ induces a nontrivial automorphism of the structure $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_n)$, and hence $+$ cannot be defined in it. (The trivial case $n = 0$, which is not covered by the theorem, also belongs here.)

Now assume that $n$ fulfils the conditions in the theorem. It is clear that the structure $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_n)$ is d-weaker than $(\mathbb{N}; B_2, +)$. To prove the converse we shall apply Theorem 3.3; hence it suffices to define $\mathrm{SPow}_2$.

We shall show that the relations

$$\mathrm{Step}_i = \{(2^{a_0+j}, 2^{a_i+j}) \mid j \in \mathbb{N}\},$$

$i = 1, \ldots, k$, are definable in $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_2)$. Informally, $\mathrm{Step}_i(x, y)$ means that $y$ can be reached from $x$ by the forward step of length $a_i - a_0$ among powers of 2 (not smaller than $2^{a_0}$). Since $g = 1$ we can combine these steps with similar backward steps to obtain the step of length 1. More formally, there are integers $i_1, \ldots, i_r, j_1, \ldots, j_s \in \{1, \ldots, k\}$ such that

$$\sum_{t=1}^{r} (a_{i_t} - a_0) = 1 + \sum_{t=1}^{s} (a_{j_t} - a_0).$$

Let us define

$$\mathrm{SPow}(x_0, y_0) \iff \exists x_1, \ldots, x_r, y_1, \ldots y_s \Bigg( \bigwedge_{t=1}^{r} \mathrm{Step}_{i_t}(x_{t-1}, x_t) \wedge \bigwedge_{t=1}^{s} \mathrm{Step}_{j_t}(y_{t-1}, y_t) \wedge x_r = y_s \Bigg).$$

If $a_0 = 0$, then we obviously have $\mathrm{SPow} = \mathrm{SPow}_2$. Otherwise (i.e. if $a_0 = 1$) we have $\mathrm{SPow} = \{(2^{i+1}, 2^{i+2}) \mid i \in \mathbb{N}\}$, and we can define $\mathrm{SPow}_2$ as follows:

$$\begin{aligned} x = 1 &\iff \mathrm{Pow}_2(x) \wedge \neg\exists z\ \mathrm{SPow}(x, z)\,, \\ x = 2 &\iff \exists z\ \mathrm{SPow}(x, z) \wedge \neg\exists z\ \mathrm{SPow}(z, x)\,, \\ \mathrm{SPow}_2(x, y) &\iff x = 1 \wedge y = 2 \ \vee\ \mathrm{SPow}(x, y)\,. \end{aligned}$$

It remains to show that the predicates $\mathrm{Step}_i$, $i = 1, \ldots, k$ are definable. Let us define

$$\mathrm{Step}(x, y) \iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \exists z \left(\mathrm{PMult}_n(z) \wedge x \sqsubseteq z \wedge y \sqsubseteq z\right);$$

this relation contains steps of lengths $|a_i - a_j|$, $i, j \in \{0, \ldots, k\}$ in both directions (including also the steps of length 0).

$$\mathrm{UnPath}_r(z_0, z_1, \ldots, z_r) \iff \bigwedge_{i=1}^{r} \mathrm{Step}(z_{i-1}, z_i)$$

$$\wedge\, \forall w_0, w_1, \ldots, w_r \left(w_0 = z_0 \wedge w_r = z_r \wedge \bigwedge_{i=1}^{r} \mathrm{Step}(w_{i-1}, w_i) \implies \bigwedge_{i=0}^{r} w_i = z_i\right).$$

(We have here a schema of definitions, one definition for every $r \in \mathbb{N}$.) Informally, $\mathrm{UnPath}_r(z_0, z_1, \ldots, z_r)$ means that there is a unique path consisting of exactly $r$ steps between $z_0$ and $z_r$;

If $r = r(n)$ is sufficiently large (e.g. $r = (a_k - a_0)^2 + 1$) and $\mathrm{UnPath}_r(z_0, z_1, \ldots, z_r)$ holds, then

$$\frac{z_1}{z_0} = \frac{z_2}{z_1} = \cdots = \frac{z_r}{z_{r-1}} \quad (= 2^{a_k - a_0} \text{ or } 2^{a_0 - a_k})\,;$$

informally, all steps have maximal possible length (and the same direction). So one step of maximal length can be defined as follows:

$$\mathrm{MaxStep}(x, y) \iff \exists z_0, \ldots, z_r \left(\mathrm{UnPath}_r(z_0, z_1, \ldots, z_r) \wedge \left((x = z_0 \wedge y = z_1) \vee (y = z_0 \wedge x = z_1)\right)\right).$$

Notice that MaxStep contains all forward steps of length $a_k - a_0$ and some (but not necessarily all) backward steps of this length. The backward steps can be eliminated as follows:

$$\mathrm{Step}_k(x, y) \iff \mathrm{MaxStep}(x, y) \wedge \exists z \left(x \sqsubseteq z \wedge y \not\sqsubseteq z \wedge \forall u, v \left(\mathrm{MaxStep}(u, v) \wedge u \sqsubseteq z \wedge v \neq y \implies v \sqsubseteq z\right)\right).$$

Now denote $m = n - 2^{a_k}$. We can define $\mathrm{PMult}_m$ by

$$\mathrm{PMult}_m(x) \iff \exists y, z \left(\mathrm{Step}_k(y,z) \wedge y \sqsubseteq x \wedge z \not\sqsubseteq x \wedge \mathrm{PMult}_n(x \sqcup z)\right).$$

Now we can define the predicate $\mathrm{Step}_{k-1}$ by the above method, and so on, up to the predicate $\mathrm{Step}_1$. □

R e m a r k 3.5. The structures $(\mathbb{N}; B_2, \mathrm{PMult}_n)$ can be considered similarly except the case $a_0 = 2$, $g = 2$; it covers e.g. $n = 20$ or $n = 68$. For this case the automorphism argument does not work. Nevertheless, the author conjectures that $+$ is not first order definable in $(\mathbb{N}; B_2, \mathrm{PMult}_n)$ for these $n$.

**THEOREM 3.6.** *Let us define*

$$mult_n(x) = x + x + \cdots + x \quad (n\text{-}times)$$

*for every* $n \in \mathbb{N}$. *Then* $(\mathbb{N}; \mathrm{EqB}_2, mult_n)$ *is d-equivalent to* $(\mathbb{N}; B_2, +)$ *if and only if* $n \geq 2$ *and* $n \neq 2^{i+2}$ *for any* $i \in \mathbb{N}$.

P r o o f. If $n = 0$ or $n = 1$ or $n = 2^i$ for some $i \geq 2$, then the structure $(\mathbb{N}; \mathrm{EqB}_2, mult_n)$ has a nontrivial automorphism and therefore $+$ is not definable in it.

The opposite implication for $n = 2$ is contained in Theorem 3.5. If $n > 2$ and $n$ is not a power of 2, then (the binary expansion of) a power of $n$ starts with $11\ldots$. The predicate $\mathrm{PMult}_m$, where $m = n \sqcup 1$, can be defined by

$$\mathrm{PMult}_m(x) \iff \exists y \left(\mathrm{Pow}_2(y) \wedge x = mult_n(y) \sqcup y\right).$$

Now we can use Theorem 3.5 with $a_0 = 1$ and $g = 1$. □

**THEOREM 3.7.** *Let us define* $add_n(x) = x + n$ *for every* $n \in \mathbb{N}$. *Then*

(i) *the structure* $(\mathbb{N}; \mathrm{EqB}_2, add_n)$ *is d-equivalent to* $(\mathbb{N}; B_2, +)$ *if and only if* $4 \nmid n$;

(ii) *the structure* $(\mathbb{N}; B_2, add_n)$ *is d-equivalent to* $(\mathbb{N}; B_2, +)$ *if and only if* $8 \nmid n$.

P r o o f. We shall start with (i). If $4 \mid n$, then the structure $(\mathbb{N}; \mathrm{EqB}_2, add_n)$ has a nontrivial automorphism (induced by $\varphi(1) = 2$, $\varphi(2) = 1$ and $\varphi(2^i) = 2^i$ for $i \geq 2$). Therefore $+$ is not definable in it. Now let $4 \nmid n$. Let us define

$$\mathrm{LeP}_2(x,y) \iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \exists u, v \left(x = add_n(u) \wedge y = add_n(v) \wedge u \sqsubseteq v\right).$$

Then $\mathrm{LeP}_2$ is the ordering of all powers of 2 which are not less than $n$. However, to apply Theorem 3.3, we need e.g. the ordering $\mathrm{LePow}_2$ of all powers of 2. We can define it as follows. If $2^i < n$ and $i \neq 0$, then there is $m > 0$ such that $2^i + mn$ is a power of 2. (Here the assumption $4 \nmid n$ is used; for $n$ odd we need not assume $i \neq 0$.) Since the constant $k = 2^i + mn$ is definable using $\mathrm{LeP}_2$, the constant $2^i$ is also definable:

$$x = 2^i \iff add_n\big(add_n\big(\ldots\big(add_n(x)\ldots\big)\big) = k \qquad (add_n \text{ repeated } m \text{ times}).$$

If $n$ is even (and $4 \nmid n$), then 1 can be defined as the power of 2 which is less than $n$ and distinct from all powers of 2 defined by the method above. Now we can easily define $\mathrm{LePow}_2$ by using $\mathrm{LeP}_2$ and "listing the remaining cases"; for example, if $n = 3$ we can use the formula

$$\begin{aligned} &\mathrm{LePow}_2(x,y) \iff \\ \iff\ &\mathrm{LeP}_2(x,y) \vee x = 1 \wedge y = 1 \vee (x = 1 \vee x = 2) \wedge \big(y = 2 \vee \mathrm{LeP}_2(y,y)\big)\,. \end{aligned}$$

The proof of (ii) is similar, only 2 and 4 ought to be used instead of 1 and 2; notice that 1 is definable as $B_2(0,0)$. □

R e m a r k 3.8. The structure $(\mathbb{N}; B_2, +)$ is *elementarily interpretable* in the structure $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{PMult}_n)$ whenever $g > 0$ (i.e., $n \neq 0 \wedge \neg \mathrm{Pow}_2(n)$). (We shall not strictly define elementary interpretability here. Roughly speaking, it means that all components (including the base set) of an isomorphic copy of the interpreted structure are definable in the other structure.) Analogously $(\mathbb{N}; B_2, +)$ is elementarily interpretable in $(\mathbb{N}; \mathrm{EqB}_2, mult_n)$ for every $n \geq 2$ and in $(\mathbb{N}; B_2, add_n)$ for every $n > 0$.

Now let us consider the function

$$B_2'(x,y) = \binom{x+y-1}{x-1} \text{ MOD } 2\,,$$

where we put $\binom{z}{-1} = 0$ for every $z \in \mathbb{N} \cup \{-1\}$. In essence, $B_2'$ is obtained from $B_2$ only by a shift to the right; however, this small change substantially changes the theories. The function $\mathrm{EqB}_2'$ is displayed in Figure 1.

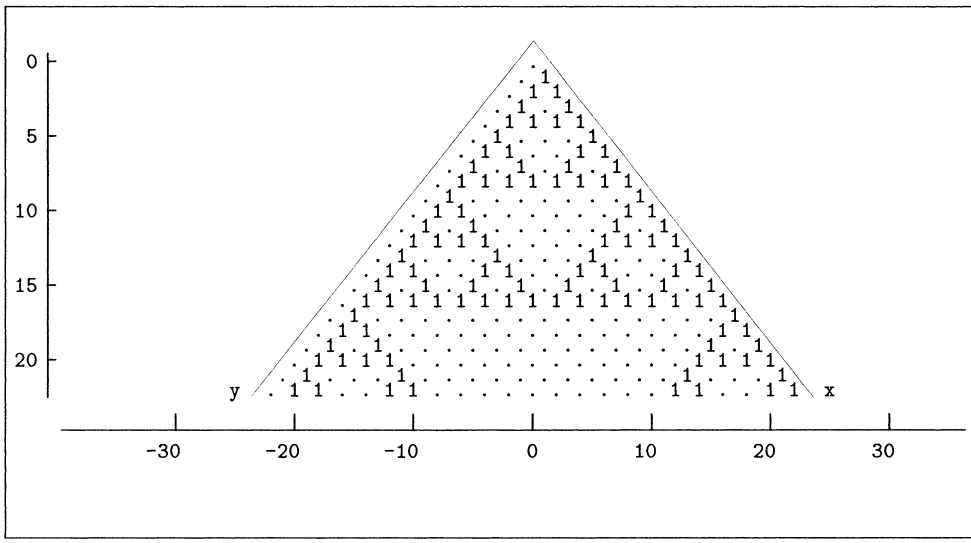


Figure 1.

**THEOREM 3.9.** *The structures* $(\mathbb{N}; \mathrm{EqB}_2')$ *and* $(\mathbb{N}; B_2')$ *are d-equivalent to* $(\mathbb{N}; B_2, +)$.

P r o o f. Let us start with the structure $(\mathbb{N}; \mathrm{EqB}_2')$. The constants 0, 1 can be defined as follows

$$y = 0 \iff \forall x, z \left(x \neq y \wedge z \neq y \implies \mathrm{EqB}_2'(x, y, z, y)\right);$$
$$x = 1 \iff x \neq 0 \wedge \forall y, z \ \mathrm{EqB}_2'(x, y, x, z).$$

Now we can define the function $B_2'$ similarly as $B_2$ is defined in Theorem 2.6. Therefore the structure $(\mathbb{N}; B_2')$ is d-weaker than $(\mathbb{N}; \mathrm{EqB}_2')$. Since the converse is obvious both structures are d-equivalent. Hence it suffices to consider $(\mathbb{N}; B_2')$ in what follows. By the formula

$$y_1 \sqsubseteq y_2 \iff \forall x \left(B_2'(x, y_1) = 0 \implies B_2'(x, y_2) = 0\right),$$

the relation $\sqsubseteq$ is definable. Hence by Lemma 2.4 the function $B_2$ is definable, too. The successor function can be defined by

$$z = \mathbf{s}(x) \iff \forall y \left(B_2(x, y) = B_2'(z, y)\right).$$

Hence by Theorem 3.3 the structure $(\mathbb{N}; B_2, +)$ is d-weaker than $(\mathbb{N}; B_2')$. The converse statement is clear from the formula

$$z = B_2'(x, y) \iff x = 0 \wedge z = 0 \vee x > 0 \wedge z = B_2\big(\mathbf{p}(x), y\big).$$

□

The author claims that the elementary theory of $(\mathbb{N}; B_2, +)$ is decidable and hence $\times$ is not definable in $(\mathbb{N}; B_2, +)$. Therefore the structures above are not d-equivalent to those considered in the following section. Of course, this statement is not used in any theorem below.

## 4. The structures d-equivalent to $(\mathbb{N}; +, \times)$

The structure $(\mathbb{N}; +, \times)$ is the d-strongest one among the structures with the base set $\mathbb{N}$ and finitely many recursive (or even arithmetical) basic relations and operations. We shall investigate how the structure $(\mathbb{N}; B_2)$ must be enriched (by some special recursive relations or operations) so that the obtained structure is d-equivalent to $(\mathbb{N}; +, \times)$, i.e. as strong as possible in the considered class of structures.

We shall start with an auxiliary lemma about squares with small number of nonzero digits (in binary system).

**Lemma 4.1.** *For every $i, j, k \in \mathbb{N}$ we have:*

a) *If $2^{2i} + 2^{2j+1}$ is a square, then $2j + 1 = 2i + 3$;*
b) *if $i < j < k$ and $2^i + 2^j + 2^k$ is a square, then $i$ is even and at least one of $j, k$ is even;*
c) *if $9 \cdot 2^{2i} + 2^{2j}$ is a square, then $2j = 2i + 4$;*
d) *if $17 \cdot 2^{2i} + 2^{2j+3}$ and $17 \cdot 2^{2i} + 2^{2j+4}$ are squares, then $j = i + 1$;*
e) *if $5 \cdot 2^{2i} + 2^j$ is a square and $j \neq 2i + 2$, then $j = 2i - 4$;*
f) *the number $65 \cdot 2^{2i} + 2^{2j+1}$ is not a square;*
g) *if $17 \cdot 2^{2i} + 2^{2j+1}$ and $17 \cdot 2^{2i+2} + 2^{2j+1}$ are squares, then $j = i + 2$;*
h) *if $2^{2i} + 2^{j+1} + 1$ is a square and $j + 1 < 2i$, then $j = i$.*

Proof.

a) In this case obviously $j \geq i$, and then $2^{2j-2i+1} = z^2 - 1 = (z-1)(z+1)$ for some positive integer $z$. Then $z - 1$, $z + 1$ are powers of 2, which gives $z = 3$ and $2j - 2i + 1 = 3$.

b) The exponent of 2 in the factorization of the considered square is equal to $i$, and hence $i$ must be even. If both $j, k$ are odd, then we have

$$2^i + 2^j + 2^k \equiv 1 + 2 + 2 \equiv 2 \pmod 3,$$

which is a contradiction because 2 is a quadratic non-residue modulo 3.

c) Denote $k = |i - j|$; obviously $k \neq 0$. If $i > j$, then $9 \cdot 2^{2k} + 1$ would be a square, which is impossible. Therefore $i < j$. Then $9 + 2^{2k} = w^2$, i.e.

$2^{2k} = (w-3)(w+3)$ for some integer $w > 3$, and hence $w-3$, $w+3$ are powers of 2. Therefore $w-3 = 2$, $w+3 = 8$, $k = 2$, and $2j = 2i+4$.

d) The first mentioned number can be a square only if $2j+3 > 2i$, i.e. $j \geq i-1$. However, $j = i-1$ is also excluded (because 19 is not a square); therefore $j \geq i$. If we denote $k = j-i$ we obtain

$$17 + 2^{2k+3} = y^2, \qquad 17 + 2^{2k+4} = z^2$$

for some positive integers $y, z$. The second equation implies

$$17 = (z - 2^{k+2})(z + 2^{k+2}),$$

both factors are positive and hence they are equal to 1 and 17. Therefore $z = 9$, $2^{k+2} = 8$, and hence $k = 1$, which gives $j = i+1$.

e) Let $5 \cdot 2^{2i} + 2^j = x^2$. If $j$ is odd, then we have $x^2 \equiv 2$ or $3 \pmod 5$, which is a contradiction; therefore $j$ is even. If $j > 2i+2$, we have

$$\left(x \cdot 2^{-i}\right)^2 \equiv 5 + 2^{j-2i} \equiv 5 \pmod 8,$$

which is also impossible. The case $j = 2i+2$ is excluded by the assumption, and in the case $j = 2i$ can we obtain $6 \cdot 2^{2i} = x^2$, which is impossible. It remains the case $j < 2i$. Then $5 \cdot 2^{2k} + 1 = y^2$ for some $y \in \mathbb{N}$ and $k = i - \frac{j}{2} \in \mathbb{N}$; we have to prove $k = 2$. Since $5 \cdot 2^{2k} = (y-1) \cdot (y+1)$ and only one of the factors $y-1$, $y+1$ is divisible by 4, we have $2^{2k-1} \mid y-1$ or $2^{2k-1} \mid y+1$. Therefore $y \geq 2^{2k-1} - 1$ and

$$5 \cdot 2^{2k} + 1 = y^2 \geq \left(2^{2k-1} - 1\right)^2 = 2^{4k-2} - 2^{2k} + 1,$$

$6 \cdot 2^{2k} \geq 2^{4k-2}$, $24 \geq 2^{2k}$, and hence $k \leq 2$. For $k = 0, 1$ the expression $5 \cdot 2^{2k} + 1$ is not a square. It remains $k = 2$, i.e. $j = 2i-4$.

f) We have $65 \cdot 2^{2i} + 2^{2j+1} \equiv 2$ or $3 \pmod 5$, which is a contradiction because both $2, 3$ are quadratic non-residues modulo 5.

g) By 4.1.b we know that $2i < 2j+1$, and hence we can divide both squares by $2^{2i}$. Then

$$2^{2k+1} + 17 = x^2, \qquad 2^{2k+1} + 68 = y^2, \qquad (y-x) \cdot (y+x) = y^2 - x^2 = 51$$

for some integers $0 < x < y$ and $k = j - i > 0$. Since $0 < y - x < y + x$ the last equation gives

either $y - x = 1$, $y + x = 51$, i.e. $x = 25$, $2^{2k+1} = 625 - 17 = 608$
or $y - x = 3$, $y + x = 17$, i.e. $x = 7$, $2^{2k+1} = 49 - 17 = 32$.

The first case does not hold for any $k \in \mathbb{N}$. In the second case we have $k = 2$, and hence $j = i + 2$.

h) If $2^{2i} + 2^{j+1} + 1 = x^2$, then $2^{j+1} \mid (x-1)(x+1)$ which implies $2^j \mid x - 1$ or $2^j \mid x + 1$. We may assume $x > 0$, and then we have $x \geq 2^j - 1$. Further $x \geq 2^i + 1$ which gives $2^{2i} + 2^{i+1} + 1 \leq 2^{2i} + 2^{j+1} + 1$, and hence $j \geq i$. If $j \geq i + 1$ we have

$$x^2 \geq (2^j - 1)^2 \geq (2^{i+1} - 2^{i-1})^2 > 2^{i+1} > 2^{2i} + 2^{j+1} + 1 = x^2,$$

which is a contradiction. Therefore $j = i$. (Remark: the condition $j + 1 < 2i$ cannot be omitted because of $49 = 2^4 + 2^5 + 1$ and $529 = 2^4 + 2^9 + 1$. As A. Schinzel informed me, [Le; Theorem 2] implies that if $2^i + 2^j + 1 = x^2$ and $j > i > 0$, then $(j, i) = (5, 4)$ or $(j, i) = (9, 4)$ or $j = 2i - 2$. Hence the "exceptional" solutions above are the unique ones.) □

**LEMMA 4.2.** *The relation* $\mathrm{SPow}_2 = \{(2^i, 2^{i+1}) \mid i \in \mathbb{N}\}$ *is first order definable in the structure* $(\mathbb{N}; \sqsubseteq, \mathrm{Sq})$.

P r o o f. Let us define

$$\begin{aligned} \mathrm{Pow}_4(x) &\iff \mathrm{Pow}_2(x) \wedge \mathrm{Sq}(x), \\ \mathrm{OddPow}_2(x) &\iff \mathrm{Pow}_2(x) \wedge \neg\, \mathrm{Pow}_4(x); \end{aligned}$$

the meaning is obvious. Now we shall introduce (for this proof only) auxiliary predicates $\mathrm{Q}_{i_1 \ldots i_k}$ for several $k$-tuples $(i_1, \ldots, i_k)$. Our aim is to obtain

$$\mathrm{Q}_{i_1 \ldots i_k} = \{(2^{2j+i_1}, \ldots, 2^{2j+i_k}) \mid j \in \mathbb{N}\} \tag{4.2.1}$$

in every case. However, sometimes this fact will not be obvious immediately from the definition, and will have to be proved. (Notice that we also could write $\mathrm{Q}_0$, $\mathrm{Q}_1$ instead of $\mathrm{Pow}_4$, $\mathrm{OddPow}_2$.) Let us define

$$\begin{aligned} \mathrm{Q}_{03}(x, y) &\iff \mathrm{Pow}_4(x) \wedge \mathrm{OddPow}_2(y) \wedge \mathrm{Sq}(x \sqcup y); \\ \mathrm{Q}_{034}(x, y, z) &\iff \mathrm{Q}_{03}(x, y) \wedge \mathrm{Pow}_4(z) \wedge z \neq x \wedge \mathrm{Sq}(x \sqcup y \sqcup z). \end{aligned}$$

For these two cases the inclusion $\supseteq$ in (4.2.1) can be easily verified and $\subseteq$ follows from Lemma 4.1.a and 4.1.c. Now let us define

$$\begin{aligned} \mathrm{Q}_{023456}(x_0, x_2, x_3, x_4, x_5, x_6) \iff\ & \mathrm{Q}_{034}(x_0, x_3, x_4) \wedge \mathrm{Q}_{034}(x_2, x_5, x_6) \\ & \wedge x_6 \neq x_0 \wedge x_6 \neq x_4 \\ & \wedge \mathrm{Sq}(x_0 \sqcup x_4 \sqcup x_5) \wedge \mathrm{Sq}(x_0 \sqcup x_4 \sqcup x_6); \end{aligned}$$

we have to prove

$$\mathrm{Q}_{023456} = \left\{(2^{2j}, 2^{2j+2}, 2^{2j+3}, 2^{2j+4}, 2^{2j+5}, 2^{2j+6}) \mid\ j \in \mathbb{N}\right\}. \tag{4.2.2}$$

The inclusion $\supseteq$ can be easily verified; let us prove $\subseteq$. Let $\mathrm{Q}_{023456}(x_0, x_2, x_3, x_4, x_5, x_6)$. Since $\mathrm{Q}_{034}(x_0, x_3, x_4)$ we have $x_0 = 2^{2i}$, $x_3 = 2^{2i+3}$, $x_4 = 2^{2i+4}$ for some $i \in \mathbb{N}$. Analogously $\mathrm{Q}_{034}(x_2, x_5, x_6)$ implies $x_2 = 2^{2j}$, $x_5 = 2^{2j+3}$, $x_6 = 2^{2j+4}$ for some $j \in \mathbb{N}$. The integers $x_0$, $x_4$, $x_5$, $x_6$ are pairwise distinct powers of 2, and therefore

$$x_0 \sqcup x_4 \sqcup x_5 = x_0 + x_4 + x_5 = 17 \cdot 2^{2i} + 2^{2j+3},$$
$$x_0 \sqcup x_4 \sqcup x_6 = x_0 + x_4 + x_6 = 17 \cdot 2^{2i} + 2^{2j+4}.$$

These values are squares, and hence by Lemma 4.1.d we have $j = i + 1$, and (4.2.2) is proved.

We shall also need the constants 1, 2, 4, which can be defined as follows:

$$x = 1 \iff \mathrm{Pow}_4(x) \wedge \neg\exists x_0, x_3, x_4, x_5, x_6\ \mathrm{Q}_{023456}(x_0, x, x_3, x_4, x_5, x_6);$$
$$x = 2 \iff \mathrm{OddPow}_2(x) \wedge \neg\exists y\,(\mathrm{Sq}(y) \wedge x \sqsubset y);$$
$$x = 4 \iff \mathrm{Pow}_4(x) \wedge x \neq 1 \wedge \neg\exists y, z\ \mathrm{Q}_{034}(y, z, x).$$

Finally, we can define

$$\begin{aligned}\mathrm{SPow}_2(y, z) \iff\ & y = 1 \wedge z = 2 \ \vee\ y = 2 \wedge z = 4 \\ & \vee \exists x_0, x_4, x_5, x_6\ \mathrm{Q}_{023456}(x_0, y, z, x_4, x_5, x_6) \\ & \vee \exists x_0\ \mathrm{Q}_{034}(x_0, y, z).\end{aligned}$$

□

**LEMMA 4.3.** *The operation* $\times$ *is first order definable in* $(\mathbb{N}; B_2, +, \mathrm{SqPow}_2)$, *where* $\mathrm{SqPow}_2 = \left\{(2^i, 2^{2i}) \mid\ i \in \mathbb{N}\right\}$.

P r o o f. Let us consider the following infinite table:

$$\begin{array}{ccccccc} 2^1 & 2^3 & 2^5 & 2^7 & 2^9 & 2^{11} & \ldots \\ 2^2 & 2^6 & 2^{10} & 2^{14} & 2^{18} & 2^{22} & \ldots \\ 2^4 & 2^{12} & 2^{20} & 2^{28} & 2^{36} & 2^{44} & \ldots \\ 2^8 & 2^{24} & 2^{40} & 2^{56} & 2^{72} & 2^{88} & \ldots \\ 2^{16} & 2^{48} & 2^{80} & 2^{112} & 2^{144} & 2^{176} & \ldots \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \end{array} \tag{4.1.1}$$

The element in the $i$th row and $j$th column (both enumerated from 0) is $2^{2^i\cdot(2j+1)}$. We shall define the relations

$$\mathrm{RowPr} = \{(2^{2^i\cdot(2j+1)}, 2^{2j+1}) \mid i,j \in \mathbb{N}\}, \quad \mathrm{ColPr} = \{(2^{2^i\cdot(2j+1)}, 2^{2^i}) \mid i,j \in \mathbb{N}\},$$

i.e. the projections to the initial row and initial column, respectively. We can easily verify

$$\begin{aligned} &\mathrm{RowPr}(x,y) \iff \\ \iff\ &\mathrm{Pow}_2(x) \wedge x \neq 1 \wedge \mathrm{OddPow}_2(y) \\ &\wedge \forall z \Big( x \sqsubseteq z \wedge \forall u,v \left(\mathrm{SqPow}_2(u,v) \wedge v \sqsubseteq z \implies u \sqsubseteq z\right) \implies y \sqsubseteq z \Big). \end{aligned}$$

Here $z$ represents a finite subset of $\mathrm{Pow}_2$ which contains $x$ and is closed under square roots (among powers of 2). Every such set must contain $y$. Now we can define membership to the initial column:

$$\mathrm{PowPow}_2(x) \iff \mathrm{RowPr}(x,2).$$

To define ColPr, we shall also need the following auxiliary predicate

$$\begin{aligned} &\mathrm{RNb}(x,y) \iff \\ \iff\ &\exists w \Big(\mathrm{RowPr}(x,w) \wedge \mathrm{RowPr}(y, w+w+w+w) \\ &\quad \wedge \Big( w = 2 \wedge \exists u,z_2 \left(\mathrm{SqPow}_2(x,u) \wedge \mathrm{SqPow}_2(u,v) \wedge u < y \wedge y < v\right) \\ &\qquad \vee\ w > 2 \wedge \exists z \left(\mathrm{SqPow}_2(x,z) \wedge x < y \wedge y < z\right)\Big)\Big). \end{aligned}$$

Informally, $\mathrm{RNb}(x,y)$ means that $y$ is the right neighbour of $x$ in a row of the table above. Now we can use the same idea as in the definition of RowPr:

$$\begin{aligned} \mathrm{ColPr}(x,y) \iff &\mathrm{Pow}_2(x) \wedge x \neq 1 \wedge \mathrm{PowPow}_2(y) \\ &\wedge \forall z \left(x \sqsubseteq z \wedge \forall u,v \left(\mathrm{RNb}(u,v) \wedge v \sqsubseteq z \implies u \sqsubseteq z\right) \implies y \sqsubseteq z\right). \end{aligned}$$

We shall define the function *memb* which enables us to code every sequence $S$ of nonnegative integers which contains only finitely many nonzero members by an integer $z$ (the function *memb* itself is used by decoding; its role resembles the role of Gödel's function $\Gamma$). So every finite sequence of integers can be coded by its length and suitable $z$. The code of $S$ will be constructed as follows. If the $j$th digit of the $i$th member of $S$ is 1, then the $j$th element of the $i$th row of the table above (i.e., $2^{2^i\cdot(2j+1)}$) will be marked. So the $i$th member of $S$ will be

coded in the $i$th row of the table. The integer $z$ will be the sum of all marked elements. Formally we define:

$$x = memb(z, y) \iff$$

$$\iff \neg\,\mathrm{PowPow}_2(y) \wedge x = 0 \;\vee\; \mathrm{PowPow}_2(y) \wedge \forall u, v \Big(\mathrm{SqPow}_2(u, v) \implies \big(u \sqsubseteq x \iff \exists w \,(\mathrm{ColPr}(w, y) \wedge \mathrm{RowPr}(w, v + v))\big)\Big).$$

Now we can define the set Sq as follows:

$$\mathrm{Sq}(x) \iff \exists z, y \Big(memb(z, y) = x \wedge memb(z, 2) = 0 \wedge memb(z, 4) = 1 \wedge \forall u, v, w \Big(\mathrm{PowPow}_2(u) \wedge \mathrm{SqPow}_2(u, v) \wedge \mathrm{SqPow}_2(v, w) \implies \Big(\big(memb(z, v) = 0 \implies memb(z, w) = 0\big) \wedge \big(memb(z, w) \neq 0 \implies memb(z, u) + memb(z, w) = memb(z, v) + memb(z, v) + 2\big)\Big)\Big)\Big).$$

In this definition $z$ is the code of an initial segment of the sequence of squares (followed by infinitely many zeros). Now we can define $\times$ from Sq, $+$ by the formulae given in the introduction. □

R e m a r k 4.4. The structures $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{SqPow}_2)$ and $(\mathbb{N}; B_2, \mathrm{SqPow}_2)$ have nontrivial automorphisms which are given by permutations of the set of columns of table (4.4.1) in essence (for the later structure the initial column must remain fixed). More formally, let $\alpha$ be arbitrary permutation of the set of odd positive integers, and let $\varphi$ be the permutation of $\mathrm{Pow}_2$ defined by

$$\varphi\big(2^{2^i \cdot (2j+1)}\big) = 2^{2^i \cdot \alpha(2j+1)} \qquad \text{for all} \quad i, j \in \mathbb{N}.$$

Then $\overline{\varphi}$ defined by (2.5.1) is an automorphism of the structure $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{SqPow}_2)$; if $\alpha(1) = 1$, then $\overline{\varphi}$ is an automorphism of $(\mathbb{N}; B_2, \mathrm{SqPow}_2)$, too. Since the structures in Lemma 4.3 have no nontrivial automorphisms it is impossible to replace $(\mathbb{N}; \mathrm{EqB}_2, +, \mathrm{SqPow}_2)$ by $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{SqPow}_2)$ in the lemma. (The operation $+$ is substantially used in the definition of RNb.)

**LEMMA 4.5.** *Let* $\mathrm{Sq}_3 = \big\{x \in \mathrm{Sq} \mid \mathrm{card}\big\{i \in \mathbb{N} \mid 2^i \sqsubseteq x\big\} = 3\big\}$. *Then for every set* X, $\mathrm{Sq}_3 \subseteq \mathrm{X} \subseteq \mathrm{Sq}$, *the operations* $+$, $\times$ *are first order definable in* $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{X})$.

P r o o f. The set $\mathrm{Sq}_3$ is definable in $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{X})$ by the formula

$$\mathrm{Sq}_3(x) \iff \mathrm{X}(x) \wedge \exists y, z, w \,\big(y \neq z \wedge y \neq w \wedge z \neq w \wedge \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \mathrm{Pow}_2(z) \wedge x = y \sqcup z \sqcup w\big).$$

Therefore it suffices to consider the structure $(\mathbb{N}; \mathrm{EqB}_2, \mathrm{Sq}_3)$ in what follows. Further, in the proof of Theorem 4.3 (including Lemma 4.2) the set Sq can be replaced by the set

$$\mathrm{Sq}_3' = \Big\{ x \in \mathrm{Sq} \mid \ \mathrm{card}\big\{ i \in \mathbb{N} \mid \ 2^i \sqsubseteq x \big\} \leq 3 \Big\};$$

only such squares occur in the considerations. However, we cannot immediately replace Sq by $\mathrm{Sq}_3$ because squares with one or two nonzero digits were also substantially used in the proof. We shall show how to avoid them.

We shall construct (i.e., define) a graph whose vertices will be powers of 2. At first we define

$$\mathrm{Edge}(x,y) \iff \mathrm{Pow}_2(x) \wedge \mathrm{Pow}_2(y) \wedge \exists z \left(\mathrm{Pow}_2(z) \wedge \mathrm{Sq}_3(x \sqcup y \sqcup z)\right).$$

By Lemma 4.1.b the odd powers of 2 are never adjacent. Therefore if an odd power of 2 is adjacent with three (distinct) vertices, these vertices are (distinct) even powers of 2, and at least two of them are adjacent. On the other hand, if $x$ is a power of 4, then it is adjacent with all sufficiently large odd powers of 2 (beginning from $8x$), and no two of them are adjacent. Therefore we can define:

$$\begin{aligned} \mathrm{Pow}_4(x) \iff \exists y,z,w \big( & y \neq z \wedge y \neq w \wedge z \neq w \\ & \wedge \mathrm{Edge}(x,y) \wedge \mathrm{Edge}(x,z) \wedge \mathrm{Edge}(x,w) \\ & \wedge \neg\, \mathrm{Edge}(y,z) \wedge \neg\, \mathrm{Edge}(y,w) \wedge \neg\, \mathrm{Edge}(z,w) \big) \end{aligned}$$

$$\mathrm{OddPow}_2(x) \iff \mathrm{Pow}_2(x) \wedge \neg\, \mathrm{Pow}_4(x).$$

Let us remember the mnemonics (4.2.1) and define

$$\begin{aligned} \mathrm{Q}_{046}(x,y,z) \iff & \mathrm{Pow}_4(x) \wedge \mathrm{Pow}_4(y) \wedge \mathrm{Pow}_4(z) \wedge \mathrm{Sq}_3(x \sqcup y \sqcup z) \\ & \wedge \forall u \left(\mathrm{Pow}_2(u) \wedge \mathrm{Sq}_3(u \sqcup y \sqcup z) \implies u = x\right) \\ & \wedge \neg \exists v \left(\mathrm{OddPow}_2(v) \wedge \mathrm{Sq}_3(x \sqcup v \sqcup z)\right). \end{aligned} \tag{4.5.1}$$

We have to prove $\mathrm{Q}_{046} = \big\{(2^{2i}, 2^{2i+4}, 2^{2i+6}) \mid \ i \in \mathbb{N}\big\}$. We shall start with the inclusion $\supseteq$; let $i \in \mathbb{N}$ and $(x,y,z) = (2^{2i}, 2^{2i+4}, 2^{2i+6})$. We have to verify six members of the conjunction in the definition of $\mathrm{Q}_{046}$; only the last two are nontrivial. For the fifth one, let $u = 2^n$. Then $u \sqcup y \sqcup z = u + y + z = 2^n + 5 \cdot 2^{2i+4}$ is a square and $n \neq 2i+2$ (because $u \neq z$). Therefore $n = 2i$ by Lemma 4.1.e, i. e. $u = x$, and the fifth member is proved. The sixth one immediately follows

from Lemma 4.1.f. Now we shall prove the inclusion $\subseteq$. If $\mathrm{Q}_{046}(x,y,z)$, then obviously $x = 2^{2i}$, $y = 2^{2j}$, $z = 2^{2k}$ for some $i,j,k \in \mathbb{N}$. Since $\mathrm{Sq}_3(x,y,z)$, the integers $i,j,k$ are pairwise distinct. Let $d = |j-k|$ and $m = \max(j,k)$; then $\{2j,2k\} = \{2m, 2m-2d\}$. If $d \geq 2$, we have

$$2m-2d < 2m-d+1 < 2m < 2m+2d-2 \qquad \text{and}$$

$$\left(2^{m-d}+2^{m}\right)^2 = 2^{2m}+2^{2m-d+1}+2^{2m-2d} = 2^{2m-d+1} \sqcup y \sqcup z\,,$$

$$\left(2^{m-d}+2^{m+d-1}\right)^2 = 2^{2m-2d}+2^{2m}+2^{2m+2d-2} = 2^{2m+2d-2} \sqcup y \sqcup z\,.$$

We have obtained two distinct squares (which belong to $\mathrm{Sq}_3$), and this contradicts the part $\forall u\,(\ldots)$ of (4.5.1). Therefore $|j-k| = 1$, and $y \sqcup z = y+z = 5 \cdot 2^{2m-2}$. Hence, by Lemma 4.1.e, we have $2i = 2m-6$ and $\{2j,2k\} = \{2i+4, 2i+6\}$. However, $2k = 2i+4$ is impossible because for $v = 2^{2i+3}$ we would obtain a square $x \sqcup v \sqcup z = 25 \cdot 2^{2i}$, which contradicts the part $\neg\exists v\,(\ldots)$ of (4.5.1). Therefore $2k = 2i+6$ and $2j = 2i+4$, and the inclusion $\subseteq$ is proved.

We continue with definition of some constants and the predicates $\mathrm{Q}_{02}$, $\mathrm{Q}_{02456}$ (where always (4.2.1) is assumed):

$$\begin{aligned}
x = 2 &\iff \mathrm{OddPow}_2(x) \wedge \neg\exists y\,\big(x \sqsubseteq y \wedge \mathrm{Sq}_3(y)\big)\,;\\
x = 8 &\iff \mathrm{OddPow}_2(x) \wedge \exists!\, y\,\big(x \sqsubseteq y \wedge \mathrm{Sq}_3(y)\big)\,;\\
x = 16 &\iff \mathrm{Pow}_4(x) \wedge \exists u,v\ \mathrm{Q}_{046}(u,x,v) \wedge \exists y\,\big(\mathrm{Pow}_4(y) \wedge \mathrm{Sq}_3(y \sqcup 8 \sqcup x)\big);\\
x = 1 &\iff \mathrm{Pow}_4(x) \wedge \exists u\,\big(x \sqcup 8 \sqsubseteq u \wedge \mathrm{Sq}_3(u)\big)\,;\\
x = 4 &\iff \mathrm{Pow}_4(x) \wedge x \neq 1 \wedge \neg\exists u,v\ \mathrm{Q}_{046}(u,x,v)\,;\\
\mathrm{Q}_{02}(x,y) &\iff x = 1 \wedge y = 4 \ \vee\ x = 4 \wedge y = 16 \ \vee\ \exists z\ \mathrm{Q}_{046}(z,x,y)\,;\\
\mathrm{Q}_{02456}(x_0,x_2,x_4,x_5,x_6) &\iff \mathrm{Q}_{046}(x_0,x_4,x_6) \wedge Q_{02}(x_0,x_2) \wedge \mathrm{OddPow}_2(x_5)\\
&\qquad \wedge \mathrm{Sq}_3(x_0 \sqcup x_4 \sqcup x_5) \wedge \mathrm{Sq}_3(x_2 \sqcup x_5 \sqcup x_6)\,.
\end{aligned}$$

The correctness of all definitions except the last one is easily seen. For the last predicate, the inclusion $\supseteq$ in (4.2.1) can be immediately verified. To prove the inclusion $\subseteq$, assume that

$$x_0 = 2^{2i}\,, \quad x_2 = 2^{2i+2}\,, \quad x_4 = 2^{2i+4}\,, \quad x_6 = 2^{2i+6}\,, \quad \text{and} \quad x_5 = 2^{2j+1}$$

for some $i,j \in \mathbb{N}$. Further, $x_0 + x_4 + x_5 = 17 \cdot 2^{2i} + 2^{2j+1}$ and $x_2 + x_5 + x_6 = 17 \cdot 2^{2i+2} + 2^{2j+1}$ are squares. Therefore by Lemma 4.1.g we have $j = i+2$, and the inclusion is proved.

Now we can define

$$\begin{aligned}\mathrm{SPow}_2(x,y) \iff & x=1\wedge y=2 \ \vee \ x=2\wedge y=4\\ & \vee \ x=4\wedge y=8 \ \vee \ x=8\wedge y=16\\ & \vee \exists z_0,z_2,z_6\, \mathrm{Q}_{02456}(z_0,z_2,x,y,z_6)\\ & \vee \exists z_0,z_2,z_5\, \mathrm{Q}_{02456}(z_0,z_2,z_4,x,y)\,,\end{aligned}$$

and by Theorem 3.5, the operation $+$ is definable. We may use $+$ (and also $\leq$, $<$ etc.) in what follows.

Since the set Sq of all squares is not defined, we cannot use the formulae from Section 1 to define $\times$. However, we can define $\mathrm{SqPow}_2$ (see Lemma 4.3 for the definition), and then we can apply Lemma 4.3. Therefore the proof will be finished if we prove that the formula

$$\begin{aligned}\mathrm{SqPow}_2(x,y) \iff & x=1\wedge y=1 \ \vee \ x=2\wedge y=4\\ & \vee\, x>2\wedge y>x+x\wedge \mathrm{Pow}_2(x)\wedge \mathrm{Pow}_4(y)\wedge \mathrm{Sq}_3\big(1\sqcup(x+x)\sqcup y\big)\end{aligned}$$

is true (in the appropriate structure, e.g. $(\mathbb{N};B_2,+,\mathrm{Sq}_3,\mathrm{SqPow}_2)$). The implication $\Longrightarrow$ can be easily verified. For the converse, assume that the right side of the above formula holds; we shall only consider the nontrivial case $x>2$. Then $x=2^j$, $y=2^{2i}$ for some $i,j\in\mathbb{N}$, $j+1<2i$ and $1+2^{j+1}+2^{2i}$ is a square. Therefore by Lemma 4.1.h we have $j=i$ and hence $\mathrm{SqPow}_2(x,y)$. □

R e m a r k 4.6. The set $\mathrm{Sq}_3$ in Lemma 4.5 can be replaced neither by the set $\mathrm{Sq}_2=\{x\in\mathrm{Sq}\mid \mathrm{card}\{i\in\mathbb{N}\mid 2^i\sqsubseteq x\}\leq 2\}$ nor by the set $\mathrm{BiSq}=\{x^4\mid x\in\mathbb{N}\}$.

**THEOREM 4.7.** *The following structures are d-equivalent to* $(\mathbb{N};+,\times)$*:*

$(\mathbb{N};\mathrm{EqB}_2,\times)$*;*

$(\mathbb{N};\mathrm{EqB}_2,sqr)$*, where* $sqr$ *is the operation of squaring;*

$(\mathbb{N};\mathrm{EqB}_2,\mathrm{Sq})$*, where* Sq *is the set of squares;*

$(\mathbb{N};\mathrm{EqB}_2,\mathrm{Sq}_3)$*,*

*where* $\mathrm{Sq}_3$ *is the set of squares with (exactly) three nonzero binary digits;*

$(\mathbb{N};\mathrm{EqB}_2,\mathrm{X})$*, where* X *is any arithmetical set such that* $\mathrm{Sq}_3\subseteq \mathrm{X}\subseteq \mathrm{Sq}$*;*

$(\mathbb{N};\mathrm{EqB}_2,+,\mathrm{SqPow}_2)$*, where* $\mathrm{SqPow}_2=\{(2^i,2^{2i})\mid i\in\mathbb{N}\}$*;*

*and also the structures obtained from the above if* $\mathrm{EqB}_2$ *is replaced be* $B_2$ *or* $+$ *is replaced by* $\leq$ *or* $\mathbf{s}$*.*

P r o o f. All basic relations and operations of the structures listed in the theorem are arithmetical and therefore these structures are d-weaker than

$(\mathbb{N}; +, \times)$. The third structure, the fourth and the fifth one, and the sixth structure are d-stronger than $(\mathbb{N}; +, \times)$ by Lemma 4.2, 4.3 and 4.5, respectively. The first two structures are d-stronger than the third one. By transitivity, all mentioned structures are d-equivalent. □

We shall finish with a relationship between the structures above and the theory of finite sets.

**THEOREM 4.8.** *The following structures are d-equivalent to* $(\mathbb{N}; +, \times)$*:*
$(\mathbb{N}; \mathrm{EqB}_2, pow_2)$, *where* $pow_2(x) = 2^x$ *for every* $x \in \mathbb{N}$;
$(\mathbb{N}; \in)$, *where* $x \in y \iff pow_2(x) \sqsubseteq y$.

P r o o f. The structure $(\mathbb{N}; +, \times)$ is obviously d-stronger than the other two structures. The last two structures are d-equivalent because $\in$ is definable in $(\mathbb{N}; \mathrm{EqB}_2, pow_2)$ (by the formula in the theorem) and $\mathrm{EqB}_2$, $pow_2$ are definable in the last structure by the formulae:

$$\mathrm{EqB}_2(x_1, y_1, x_2, y_2) \iff \big(\exists z\,(z \in x_1 \wedge z \in y_1) \iff \exists z\,(z \in x_2 \wedge z \in y_2)\big),$$
$$y = pow_2(x) \iff \forall z\,(z \in y \iff z = x).$$

It remains to show that $+$, $\times$ are definable in the third structure; this result is well known in essence. All axioms of ZFC (Zermelo-Fraenkel set theory with the axiom of choice) but the axiom of infinity are true in $(\mathbb{N}; \in)$. (Or: this structure is (the standard) model of the theory of finite sets.) Usual notions of set theory including ordinal numbers and transfinite induction can be developed. For example, we can define

$$\mathrm{Ord}(x) \iff \forall z\,\big(0 \in z \wedge \forall y\,\big(y \in z \wedge y \neq x \implies y \sqcup pow_2(y) \in z\big) \implies x \in z\big).$$

(No infinite ordinal numbers exists, and so ordinal numbers coincide with natural numbers and transfinite induction reduces to the usual mathematical induction. Remember that "natural numbers" do not coincide with the elements of $\mathbb{N}$.) The relation $<$ satisfies the formula

$$x < y \iff \exists z\,\big(z \in y \wedge z \notin x \wedge \forall w\,(w \in x \implies w < z \vee w \in y)\big).$$

It cannot be immediately used to define $<$ because $<$ is contained in its right-hand part, too. However, the right-hand part uses $<$ only between *elements* of $x$, $y$. Therefore the expressed idea can be used as a base for the definition by transfinite induction. As soon as $<$ (and hence $\leq$, too) is defined we can define $+$ by Theorem 3.2, and also $\mathrm{SqPow}_2$ by the formula

$$\mathrm{SqPow}_2(x, y) \iff \exists z\,\big(x = pow_2(z) \wedge y = pow_2(z + z)\big).$$

Now Lemma 4.3 can be used to define $\times$. (Of course, the desired result can be obtained also in another way if the theory of finite sets is sufficiently developed.) □

## REFERENCES

[Bo] BONDARENKO, B. A.: *Generalized Pascal Triangles and Pyramids, Their Fractals, Graphs and Applications* (Russian), Fan, Tashkent, 1990.

[K1] KOREC, I.: *Generalized Pascal triangles. Decidability results*, Acta Math. Univ. Comenian. **46-47** (1985), 93–130.

[K2] KOREC, I.: *Generalized Pascal triangles.* In: Proceedings of the V. Universal Algebra Symposium, Turawa, Poland, May 1988 (K. Halkowska and S. Stawski, eds.), World Scientific, Singapore, 1989, pp. 198–218.

[K3] KOREC, I.: *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Math. Ber. **318** (1993), 53–61.

[Le] LE, M.: *On the number of solutions of the generalized Ramanjuan-Nagell equation* $x^2 - D = 2^{n+2}$, Acta Arith. **60** (1991), 149–167.

[Mo] MONK, J. D.: *Mathematical Logic*, Springer Verlag, New York, 1976.

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

[Ro] ROBINSON, J.: *Definability and decision problems in arithmetic*, J. Symbolic Logic **14** (1949), 98–114.

[Se] SEMENOV, A. L.: *On definability of arithmetic in their fragments* (Russian), Dokl. Akad. Nauk SSSR **263** (1982), 44–47.

[Sh] SHOENFIELD, J. R.: *Mathematical Logic*, Addison — Wesley, Reading, 1967.

[Si] SINGMASTER, D.: *Notes on binomial coefficients III – Any integer divides almost all binomial coefficients*, J. London Math. Soc. (2) **8** (1974), 555–560.

[Wo] WOODS, A.: *Some Problems in Logic and Number Theory, and Their Connection.* Ph.D. Thesis, University of Manchester, Manchester, 1981.

[Ye] YERSHOW, JU. L.: *Decidability Problems and Constructive Models* (Russian), Nauka, Moscow, 1980.

Received October 22, 1993

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