Mathematical Institute
Slovak Academy of Sciences, Bratislava

Preprint 12/1997

Ivan Korec

Arithmetical operations strongest with respect to the first order definability

August 22, 1997

PREPRINT SERIES

ARITHMETICAL OPERATIONS STRONGEST WITH RESPECT TO THE FIRST ORDER DEFINABILITY

Ivan KOREC

Abstract. An operation (or a relation) on the set $\mathbb{N}$ of nonnegative integers is called arithmetical if it is first order definable in the structure $\langle \mathbb{N}; +, \times \rangle$. An arithmetical operation f will be called strongest with respect to the first order definability if addition and multiplication are first order definable in the structure $\langle \mathbb{N}, f \rangle$. Examples of such operations are presented, including polynomials of several variables (e.g. $xy+1$, $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2$, x^7+y) functions related to divisibility and successor (e.g. $\gcd(x+1,y)$, $\mathrm{lcm}(x+3,y+3)$) and pairing functions (i.e., bijections $\mathbb{N}^2 \to \mathbb{N}$). Further, uniform definability of binary relations from pairing functions is proved.

1. Introduction and basic definitions

This paper is a contribution to the investigation of elementary definability of $+$, $\times$ in first order structures. A classical paper in this direction is [Ro49]. One reason for such investigation is to obtain undecidability results for elementary theories. The structures presented here will contain a unique basic operation. It will be a polynomial, a function related to divisibility and successor or a pairing function. A wide list of structures where $+$, $\times$ are definable is contained in [Ko96] (without complete proofs). Related results are collected also in [Ce95] and [Gr91].

In the present paper some def-strongest operations will be presented, in particular some def-strongest polynomials. A wide list of def-strongest structures is contained in [Ko96]. Related results are collected also in [Ce95] and [Gr91]. A classical paper about definability of $+$, $\times$ is [Ro49].

We shall use usual first order predicate calculus with equality. The formulas will be simplified by omitting parenthesis using usual priority of symbols; e.g., the logical connectives sorted by their priority will be $\neg$, $\wedge$, $\vee$, $\Longrightarrow$, and $\Longleftrightarrow$. The base set of considered structures will be $\mathbb{N}$, the set of nonnegative integers. The symbols like $+$, $\times$, $<$, etc. will be used in their usual meaning (and, as usual, $\times$ will be often replaced by dot or omitted). The symbol $\mathbf{s}$ will denote successor and $|$ divisibility; gcd and lcm will be greatest common divisor and least common multiple. The meaning of some symbols will be explained when they are used. We shall sometimes use lambda notation to describe some operations. The notation $\lambda_{\ldots}(T)$, where ... states instead of k (pairwise distinct) variables and T is a term, denotes the k-ary operation on the set $\mathbb{N}$ of nonnegative integers whose values are determined by the term T.

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

Key words and phrases. Elementary definability, Arithmetical structures, Undecidable theories.

This work was supported by Grant 2/1224 of Slovak Academy of Sciences. It was presented at 14th Days of Weak Arithmetics, St. Peterburg, May 22–24, 1997.

Typeset by $\mathcal{AMS}$-TEX

We shall deal with the arithmetical structures defined as follows:

Definition 1.1. *A structure $\langle \mathbb{N}; X_1, \ldots, X_k \rangle$ will be called arithmetical if all $X_1, \ldots, X_k$ are arithmetical (i.e., first order definable in $\langle \mathbb{N}; +, \times \rangle$).*

Hence the word "arithmetical" is used in the sense of mathematical logic, not in the sense of number theory. We do not consider structures with infinite signature. Notice that every recursive structure (on $\mathbb{N}$) is arithmetical; almost all structures below will be recursive.

Definition 1.2. *An arithmetical structure $\langle \mathbb{N}; X_1, \ldots, X_k \rangle$ will be called strongest with respect to the first order definability (or shortly def-strongest) if the usual operations $+$, $\times$ are definable in it.*

Definition 1.3. *An operation or relation X on $\mathbb{N}$ will be called strongest with respect to the first order definability (or shortly def-strongest) if the structure $\langle \mathbb{N}; X \rangle$ is def-strongest.*

If we consider the set of all arithmetical operations with the quasiorder "to be first order definable from" then the def-strongest operations form the greatest element of the associated partially ordered set (obtained by factorization). This fact explains the term def-strongest. Notice that the def-strongest structures have in some sense "most undecidable" theories. Of course, there are stronger operations (and harder theories), but only outside the class of arithmetical ones.

2. Auxiliary results

At first we shall extend the formula $xy = \mathrm{lcm}(x, y)$ which holds for x, y relatively prime. To formulate the result, let us denote

$$\mathrm{ExTo}_k(z) \iff z = 0 \vee \neg\exists u \big(u \neq 1 \wedge u^{k+1} \mid z\big). \tag{2.1}$$

$\mathrm{ExTo}_k(z)$ expresses that the exponents which occur in the factorization of z do not exceed k; e.g., for $k = 1$ we obtain square-free integers. (The integer $z = 0$ is exceptional; it is suitable to join it.)

Theorem 2.1. *For every $k > 0$ the relation*

$$\mathrm{Mult}_k = \big\{(x, y, z) \in \mathbb{N}^3 \mid z = xy \wedge \mathrm{ExTo}_k(\gcd(x, y))\big\} \tag{2.2}$$

is definable in the structure $\langle \mathbb{N}; \mid \rangle$.

Proof. Let us denote by $\#(p, x, y)$ the number of powers of p which divide y and do not divide x. Let $\mathbb{P}$ denote the set of primes. For x, y, z positive we have

$$\begin{aligned}\mathrm{Mult}_k(x, y, z) \iff{}& \mathrm{ExTo}_k(\gcd(x, y) \wedge \\ & \wedge (\forall p \in \mathbb{P}) \bigwedge_{i=0}^{k} \Big(\#(p, 1, \gcd(x, y)) = i \iff \#(p, \mathrm{lcm}(x, y), z) = i\Big).\end{aligned}$$

This is not a first order formula but we can transform it into a first order definition of Mult_k. The functions gcd, lcm, the set $\mathbb{P}$ of primes and the set Π of prime powers are first order definable in the structure $\langle \mathbb{N}; \mid \rangle$ (the sets as unary relations). The constant 0 is definable, too, which enables us to consider the cases $x = 0$, $y = 0$, or $z = 0$. It remain to express the parts $\#(x, y, z) = i$, and it is not difficult. The number of quantifiers will depend on i. We omit further technical details. $\square$

Corollary 2.2. *For every $k > 0$ the multiplication by k (i.e., the function $\lambda_x(kx)$) is first order definable in the structure $\langle \mathbb{N}; |, k \rangle$.*

Let Mult be the grapf of multiplication on $\mathbb{N}$. We can easily see that the relations Mult_k, $k \in \mathbb{N}$ form a chain under $\subseteq$, and that the union of this chain (or also its limit) is equal to Mult.

Conjecture 2.3. *If $X \subseteq \mathrm{Mult}$ is first definable in a structure $\langle \mathbb{N}; |, a_1, \dots, a_n \rangle$ for some constants a_i (or, in other words, if X is parametrically definable in $\langle \mathbb{N}; | \rangle$) then $X \subseteq \mathrm{Mult}_k$ for some $k > 0$.*

The following theorem collects some results about def-strongest structures with more than one operations and/or relations. It contains only the results which are used below in the proofs for one-operation structures.

Theorem 2.4. *The following structures are def-strongest:*

(1) $\langle \mathbb{N}; \mathbf{s}, \times \rangle$, *where* $\mathbf{s}$ *denotes the successor operation;*
(2) $\langle \mathbb{N}; \mathbf{s}^k, \times \rangle$, *where* $k > 0$ *and* $\mathbf{s}^k(x) = x + k$;
(3) $\langle \mathbb{N}; \mathbf{s}^k, | \rangle$, *where* $k > 0$;
(4) $\langle \mathbb{N}; \mathbf{s}^k, \lambda_{xy}(xy + x + y) \rangle$, *where* $k > 0$;

Proof. (1) This is a classical result from [Ro49]. We only remember the classical Tarski–Robinson formula (valid for $z > 0$):

$$z = x + y \iff (1 + xz) \cdot (1 + yz) = 1 + z^2 \cdot (1 + xy).$$

(2) We can define the constant 0 in the usual way, and then

$$k = \mathbf{s}^k(0), \qquad y = \mathbf{s}(x) \iff ky = \mathbf{s}^k(kx).$$

Then we can apply (1).

(3) We can define $x = 0 \iff \mathbf{s}^k(x) \mid \mathbf{s}^k(\mathbf{s}^k(x))$ and $k = \mathbf{s}^k(0)$. Then by Corollary 2.2 we can multiply by k, and use the idea from the previous item.

(4) If $\bullet$ denotes the operation then we have $x \bullet y + 1 = (x + 1)(y + 1)$. We can prove the following generalization of 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 0, $\mathbf{s}$, and then $+$, $\times$. $\square$

In the next theorem the symbol MOD denotes the remainder by integer division.

Theorem 2.5. *The structure* $\langle \mathbb{N}; \in \rangle$, *where*

$$x \in y \iff y \,\mathrm{MOD}\, 2^{x+1} \geq 2^x$$

is def-strongest.

Proof. It will be only sketched because the theorem is known. Notice that an alternative definition of $\in$ could be

$x \in y$ if and only if the x-th binary digit of y is equal to 1.

The coincidence between the symbol for set-theoretical membership and the symbol for the considered relation is not random. We can simply *identify* the set $\mathbb{N}$ with the set of hereditarily finite sets. (In other words: $\langle \mathbb{N}; \in \rangle$ is (isomorphic with) the standard model of *Zermelo-Fraenkel theory of finite sets.* This theory is obtained if we replace the axiom of infinity by its negation and the axiom "there is a set". Axiom of choice and axiom of constructivity become provable.) We can define new "natural numbers" (or "ordinals"; now these notions coincide); in the theory of finite sets they will form a proper class ω. Then we have to define addition and multiplication on ω, and the natural bijection between ω and $\mathbb{N}$. Using them, we can easily define $+$, $\times$ on the set $\mathbb{N}$. $\square$

3. Polynomial operations

A def-strongest polynomial must have at least two variables, and its degree must be at least two. (It follows from the decidability results about one unary function and about Presburger arithmetic.) These bounds are achieved in some items of the next theorem. Notice that the parameters runs over nonnegative integers; additional conditions are always explicitly mentioned.

Theorem 3.1. *The following operations are def-strongest:*

(1) $\lambda_{xy}(xy + ax + c)$, *where* $a + c > 0$;
(2) $\lambda_{xy}(xy + ax + by)$, *where* $(a, b) \notin \{(0,0), (1,1)\}$;
(3) $\lambda_{xy}(xy + ax + by + c)$, *where* $|a - b| = 1$;
(4) $\lambda_{xy}(xy + x + y + 1)$;
(5) $\lambda_{xy}(ax^2 + xy + cx + d)$, *where* $a + c + d > 0$;
(6) $\lambda_{xy}(ax^2 - bxy + cy^2)$, *where* $0 < b^2 \leq 4ac$ *and* $b \mid a$;
(7) $\lambda_{x_1x_2x_3x_4x_5}(x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2)$;
(8) $\lambda_{xy}(x^n + by)$, *where* $n \geq 2$, $b > 0$;
(9) $\lambda_{xy}(x^n + y + c)$, *where* $n \geq 2$.

Proof. In the proof of every item (except (7)) we shall use the symbol $\bullet$ for the actual operation. Hence the formulas from one item cannot be immediately transferred into another items.

(0) We shall start with the operation $x \bullet y = \lambda_{xy}(xy + x)$; it is not separately mentioned in the theorem but it is contained in more general items (1)–(3), and it is used in their proof. We can define $x = 0 \iff x \bullet x = x$ and

$$x = 1 \iff \forall u, v\big(u \bullet v = 0 \vee \exists y(u \bullet v = x \bullet y)\big).$$

Then we can define $\mathbf{s}(x) = 1 \bullet x$, and finally $\times$ by

$$z = xy \iff y = 0 \wedge z = 0 \vee \exists u\big(y = s(u) \wedge z = x \bullet u\big).$$

Now we can use the classical result about $\langle \mathbb{N}; \mathbf{s}, \times \rangle$, see Theorem 2.4, (1).

(1) For $c = 0$ we can define 0 as above, then multiplication by a as $x \bullet 0$ and $\lambda_{xy}(xy + x)$ using $a \cdot (xy + x) = x \bullet (ay)$. Then we can apply (0).

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 $\mathbf{s}^c(x) = x \bullet 1$, and using it $\times$. Now we can use the item $\langle \mathbb{N}; \mathbf{s}^k, \times \rangle$ from Theorem 2.4.

For $a > 0$, $c > 0$ we can define $\mathbf{s}^a$. Indeed, let us consider the sets $\{u \bullet y \mid u \in \mathbb{N}\}$, $\{x \bullet u \mid u \in \mathbb{N}\}$. If $x \neq y + a$ then their symmetric difference $D_{x,y}$ is infinite. For $x = y + a$ the cardinality of $D_{x,y}$ is bounded by a constant independent on x, y, which can be expressed by a first order formula. Further, we can define $\mathbf{s}^{a+c}$ (using $1 \bullet x$) and then the function $\lambda_{xy}(xy + ax)$ by $z = xy + ax \iff \mathbf{s}^{a+c}(z) = \mathbf{s}^a(x \bullet y)$. So we reduced the case $c > 0$ to the solved case $c = 0$.

(2) We may assume $a \geq b > 0$ (the case $b = 0$ is included in (1)), and therefore $a > 1$. We can define 0 by the property $0 \bullet 0 = 0$, and multiplication by a and by b. Since $(bx) \bullet y = b \cdot (xy + ax + y)$ we can define $\lambda_{xy}(xy + ax + y)$. Hence we may assume $b = 1$. Then we can define $\mathbf{s}^{a-1}$ and $\lambda_{xy}(xy + x + y)$, and apply Theorem 2.4,(3).

(3) We may assume $a = b + 1$ and by (1) also $c > 0$. The substantial part is the 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. If we have $\mathbf{s}$ we can define also $\lambda_{xy}(xy + ax + by)$ by

$$z = xy + ax + by \iff \mathbf{s}^c(z) = x \bullet y$$

($\mathbf{s}^c$ is c-times repeated $\mathbf{s}$). So we reduced this item to (1).

(4) We can define $x = 0 \iff \neg\exists u, v(x = u \bullet v)$ and $\mathbf{s}(x) = 0 \bullet x$. Then we can define $\times$ by the formula

$$\begin{aligned} z = xy \iff & x \neq 0 \wedge y \neq 0 \wedge \exists x_1, y_1\big(x = \mathbf{s}(x_1) \wedge y = \mathbf{s}(y_1) \wedge z = x_1 \bullet y_1\big) \vee \\ & \vee (x = 0 \vee y = 0) \wedge z = 0. \end{aligned}$$

So the problem is reduced to item (1) of Theorem 2.4.

(5) Here we can define divisibility by

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

Then we can define 1 and $\mathbf{s}^{a+c+d}(x) = 1 \bullet x$, and use Theorem 2.4.

(6) The condition $b^2 \leq 4ac$ is used to obtain a total operation on $\mathbb{N}$. The condition $b \mid a$ is used in the present proof; maybe, it can be avoided.

If $a - b + c \neq 1$ we can define 0 as the root of the the equation $x \bullet x = x$ (in the range $\mathbb{N}$). If $a - b + c = 1$ this equation has two roots, 0 and 1, and we have to distinguish them, but it is not difficult. (The conditions on a, b, c imply $a = b \leq 4$, $c = 1$. Hence $0 \bullet 1 = 1$ and $1 \bullet 0 \neq 0$.)

We can easily verify that

$$x \bullet z = y \bullet z \iff x = y \vee a(x + y) = bz$$

and hence (the assumption $b \mid a$ is again used)

$$x \neq y \wedge z \neq 0 \implies \bigl(z = x + y \iff \exists u(x \bullet u = y \bullet u \wedge z \bullet u = 0 \bullet u)\bigr).$$

which enables us to define addition of distinct numbers. To define $+$ in general we shall use $z = x + y \iff (v + x) + y = v + z$ with a suitable v; some trivial cases must be expressed separately. Finally, we can define $\lambda_x(ax^2)$, and then by a result of [Bü60] the operation $\times$, too.

(7) We shall use Lagrange's theorem that every $x \in \mathbb{N}$ is a sum of four squares. (We could avoid it, but the chosen method of proof will be useful also below.) Let us denote the considered operation by F. We can define

$$x = 0 \iff F(x, x, x, x, x) = x,$$

and then the operation $x * y = x + y^2$ by

$$z = x * y \iff \exists x_1, x_2, x_3, x_4\bigl(x = F(x_1, x_2, x_3, x_4, 0) \wedge z = F(x_1, x_2, x_3, x_4, y)\bigr).$$

Then we can define addition by the formula

$$\begin{aligned} z = x + y \iff \exists x_1, x_2, x_3, x_4\bigl(x = (((0 * x_1) * x_2) * x_3) * x_4 \wedge \\ \wedge z = (((y * x_1) * x_2) * x_3) * x_4\bigr). \end{aligned}$$

Further, we can define the set of squares and then $\times$, e.g., by [Pu57].

(8) By Waring-Hilbert Theorem (see e.g. [Na90]) there is k such that every $x \in \mathbb{N}$ is a sum of at most k n-th powers. For $b = 1$ we can continue similarly as in (7) with $*$. For the definition of $\times$ we can use a result of [Bü60]: it suffices to have $+$ and the range of any (unary) non-linear polynomials (x^n in our case).

The case $b > 1$ can be reduced to $b = 1$. Indeed, we can define 0 as the root of $x \bullet x = x$, then multiplication by b as $0 \bullet x$ and $\lambda_x(b^n x)$ as n-times repeated multiplication by b. Finally, we have

$$z = x^n + y \iff b^n z = (bx) \bullet (b^n y).$$

So the case $b > 1$ is reduced to the case $b = 1$.

(9) The case $c = 0$ is already solved above. If $c > 0$ we can define 0 by the formula $x = 0 \iff \forall u, v \exists y(u \bullet v = x \bullet y)$, then $\mathbf{s}^c(x) = 0 \bullet x$ and then

$$z = x^n + y \iff \mathbf{s}^c(z) = x \bullet y.$$

So the case $c > 0$ is reduced to the solved case $c = 0$; see (8). $\square$

Now we show some polynomials which are not def-strongest; the corresponding theories are decidable.

Theorem 3.2. *The following operations are not def-strongest:*

(1) $\lambda_{xy}\big(xy + ax + ay + a^2 - a\big)$ *for any nonnegative integer* a;

(2) $\mathbf{c}$, *the Cantor's pairing function,* $\mathbf{c}(x, y) = \frac{(x+y)(x+y+1)}{2} + x$ *for all* $x, y \in \mathbb{N}$;

(3) $\overline{\mathbf{c}}$, *defined by* $\overline{\mathbf{c}}(x, y) = \mathbf{c}(x, y) + 1 = \frac{(x+y)(x+y+1)}{2} + x + 1$ *for all* $x, y \in \mathbb{N}$.

Proof. (1) Let $\bullet$ denotes the considered operation. Since $(x \bullet y) + a = (x + a)(y + a)$ the structure $\langle \mathbb{N}; \bullet \rangle$ is isomorphic with $\langle \{x \in \mathbb{N} \mid x \geq a\}, \times \rangle$. The latest structure has nontrivial automorphisms (e.g. those induced by permutations of the primes contained in it). Hence the original structure also has nontrivial automorphisms, and $+$ cannot be defined in it. (Another argument: the elementary theory is decidable.)

(2) By P. CEGIELSKI and D. RICHARD the elementary theory of $\langle \mathbb{N}; \mathbf{c} \rangle$ is decidable; the result was announced in Warszawa, December 1996.

(3) The structure $\langle \mathbb{N}; \overline{\mathbf{c}} \rangle$ is a free groupoid (with one generator 0), and hence by [Ma61] its theory is decidable. □

4. OPERATIONS AND RELATIONS RELATED TO DIVISIBILITY AND SUCCESSOR

We are mainly interested in def-strongest operations but we shall start with some results concerning structures and relations. They will be applied in Theorem 4.3.

Theorem 4.1. *Let* $k > 0$ *and let* $|^k$ *be the restriction of divisibility to the integers not less than* k, *i.e.*

$$x \,|^k\, y \iff x \geq k \wedge y \geq k \wedge x \,|\, y.$$

Then the structure $\langle \mathbb{N}; \mathbf{s}^k, |^k \rangle$ *is def-strongest.*

Proof. We may assume $k > 1$ because for $k = 1$ we obtain an easy modification of Theorem 2.4, (3). If we have the constants $0, 1, \ldots, k$ and the unary relations $\mathrm{M}_a = \{ax \mid x \in \mathbb{N}\}$ for $a < k$ we can define

$$x \,|\, y \iff x \,|^k\, y \vee x = 1 \vee y = 0 \vee \bigvee_{a=2}^{k-1} \Big(x = a \wedge \mathrm{M}_a(y)\Big).$$

If a constant $a \neq 0$ is definable, we can define $b = (k+1)a = \mathbf{s}^{ak}(a)$ and

$$\mathrm{M}_a(x) \iff b \,|^k\, \mathbf{s}^{ak}(x) \vee b \,|^k\, \mathbf{s}^{2ak}(x) \vee \cdots \vee b \,|^k\, \mathbf{s}^{(k+1)ak}(x).$$

All $\mathbf{s}^{ik}$ here and below must be expressed as repeated $\mathbf{s}^k$.

It remains to define the constants $0, 1, \ldots, k-1$. We can define

$$x = 0 \iff \mathbf{s}^k(x) \,|^k\, \mathbf{s}^{2k}(x),$$

$$x = 1 \iff x \neq 0 \wedge \bigwedge_{i=1}^{k-1} \exists y \big(\forall z (y \neq \mathbf{s}^k(z)) \wedge \mathbf{s}^k(x) \,|^k\, \mathbf{s}^{ik}(y)\big).$$

The constant 1 was defined by a property of distribution of $k-1$ multiples of $k+1$ between k and k^2. For $2 \leq a < k$ we have

$$x = a \iff \forall y \big(x \neq \mathbf{s}^k(y)\big) \wedge \mathbf{s}^k(1) \,|^k\, \mathbf{s}^{ak}(x).$$

Indeed, the first member on the right expresses $x < k$, and for $a < k$ the integer $ak + a$ is the unique multiple of $k+1$ among $ak + x$, $x = 0, 1, \ldots, k-1$. □

Theorem 4.2. *For every $k > 0$ the relations*

$$\mathrm{DivL}_k(x,y) \iff x+k \mid y \qquad \text{and} \qquad \mathrm{DivR}_k(x,y) \iff x \mid y+k$$

are def-strongest.

Proof. For the symbol DivL_k we can define $x = 0 \iff \forall y\, \mathrm{DivL}_k(y,x)$ and then

$$\begin{aligned} y = \mathbf{s}^k(x) &\iff \mathrm{DivL}_k(x,y) \wedge \forall z\big(z \neq 0 \wedge \mathrm{DivL}_k(x,z) \implies y \mid z\big), \\ x \mid^k y &\iff \forall z\big(\mathrm{DivL}_k(z,x) \implies \mathrm{DivL}_k(z,y)\big). \end{aligned}$$

Now we can use Theorem 4.1.

For the symbol DivR_k we can define

$$x \mid y \iff \forall z\big(\mathrm{DivR}_k(y,z) \implies \mathrm{DivR}_k(x,z)\big).$$

Indeed, the right-hand side is equivalent with $(\forall z \geq k)(y \mid z \implies x \mid z)$, which is obviously equivalent with $x \mid y$. Further we can define

$$y = \mathbf{s}^k(x) \iff \mathrm{DivR}_k(y,x) \wedge \forall z\big(\mathrm{DivR}_k(z,x) \implies z \mid y\big).$$

Now we can use Theorem 2.4, (3). $\square$

Theorem 4.3. *For every $k \geq 1$ the following operations are def-strongest:*

(1) $\lambda_{xy}\big(\gcd(x,y)+k\big)$;
(2) $\lambda_{xy}\big(\gcd(x+k,y+k)\big)$;
(3) $\lambda_{xy}\big(\gcd(x+k,y)\big)$;
(4) $\lambda_{xy}\big(\mathrm{lcm}(x,y)+k\big)$;
(5) $\lambda_{xy}\big(\mathrm{lcm}(x+k,y+k)\big)$;
(6) $\lambda_{xy}\big(\mathrm{lcm}(x+k,y)\big)$.

Proof. Let us always use the symbol $\bullet$ for the actual operation.

(1) We can define $\mathbf{s}^k(x) = x \bullet x$ and $z = \gcd(x,y) \iff z \bullet z = x \bullet y$, and then $\mid$. After that we can apply item (3) of Theorem 2.4.
(2) We can define $\mathbf{s}^k(x) = x \bullet x$ and

$$x \mid^k y \iff \exists u,v\big(x = \mathbf{s}^k(u) \wedge y = \mathbf{s}^k(v) \wedge u \bullet v = x\big).$$

After that we can apply Theorem 4.1.
(3) We can define $\mathrm{DivR}_k(x,y) \iff y \bullet x = x$, and then apply Theorem 4.2.

The items (4)–(6) can be proved similarly; in the item (6) we can define $\mathrm{DivL}_k(x,y) \iff x \bullet y = y$. $\square$

5. Pairing functions

Here we define *pairing functions* as bijections from $\mathbb{N}^2$ into $\mathbb{N}$, and the set of all pairing functions will be denoted by $\mathrm{Bij}(\mathbb{N}^2, \mathbb{N})$. As we have seen in Theorem 2.2, Cantor's pairing function is not def-strongest. The same probably holds for many classical pairing functions. Therefore the following theorem is interesting.

Theorem 5.1. *There is a def-strongest pairing function.*

Proof. The constructed pairing function $\bullet$ will code the relation $\in$ from the item (5) of Theorem 1.4. (However, we can use any def-strongest binary relation instead of $\in$. Some minor technical problems could arise, but they can be solved, e.g. in the way used in the next theorem.) For every $n \in \mathbb{N}$ we define

$$(4n+1) \bullet (4n) = 4n+1 \quad \text{and} \quad (4n+2) \bullet (4n+3) = 4n+3.$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	□	■	□	■	□	■	□	■	□	■	□	■	□	■	□
1	**1**	□	■	■	□	□	■	■	□	□	■	■	□	□	■
2	□	□	□	**3**	■	■	■	■	□	□	□	□	■	■	■
3	□	□	□	□	□	□	□	□	■	■	■	■	■	■	■
4	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
5	□	□	□	□	**5**	□	□	□	□	□	□	□	□	□	□
6	□	□	□	□	□	□	□	**7**	□	□	□	□	□	□	□
7	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
8	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□
9	□	□	□	□	□	□	□	□	**9**	□	□	□	□	□	□

Figure 1. Schema of $\bullet$; multiples of 4 denoted by ■.

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 Theorem 1.4. Multiples of 4 will denote "true"; their positions are displayed in Figure 1. We obviously can arrange $x \in y \iff 4 \mid (y \bullet x)$. For example, we can fill in the even values of $\bullet$ in the order given by Cantor's pairing function, and always choose the smallest suitable value. $\square$

The previous construction can be generalized and strengthened as follows:

Claim. *Binary relations (on $\mathbb{N}$) are uniformly first order definable from pairing functions.*

The exact formulation is in the next theorem. Notice that the formula A is a definition of R from f. Strictly speaking, we ought to distinguish the relations and functions from relational and functional symbols. However, now no misunderstandness arises. $\mathcal{S} \models A$ means that the formula A is true in the structure $\mathcal{S}$.

Theorem 5.2. *There is a formula A of the form $R(x,y) \iff B$, where B contains the only non-logical symbol f, such that*

$$(\forall R \subseteq \mathbb{N}^2)(\exists f \in \mathrm{Bij}(\mathbb{N}^2, \mathbb{N}))(\langle \mathbb{N}; f, R\rangle \models \forall x, y\, A).$$

Proof. We shall code any binary relation R by a pairing functions f so that usually

$$\begin{aligned} R(x,y) &\iff f(x,y) \operatorname{MOD} 10 \in \{4,7\}. \\ \neg R(x,y) &\iff f(x,y) \operatorname{MOD} 10 \in \{0,2\}. \end{aligned} \tag{5.1}$$

However, modification for some special pairs (x,y) are necessary because the condition on the right must be expressed by f only. (All special pairs will satisfy $|x-y| = 1$.) The choice from two values on the right in the formulas (5.1) will be used to code some additional information. Also finite and co-finite relations R force us to a special modification, see (5.4).

In the construction of the pairing function f to a given relation R we shall start with the conditions independent on R. For every $k \in \mathbb{N}$ we define

$$\begin{aligned} f(10n+1, 10n) &= 10n+1, & f(10n+2, 10n+3) &= 10n+3, \\ f(10n+5, 10n+4) &= 10n+5, & f(10n+6, 10n+5) &= 10n+6, \\ f(10n+7, 10n+8) &= 10n+8, & f(10n+8, 10n+9) &= 10n+9. \end{aligned} \tag{5.2}$$

In all other cases we shall arrange

$$f(x,y) \notin \{x,y\}. \tag{5.3}$$

This enables us to define the residue classes modulo 10 as unary relations; we shall use the notation $x \equiv_{10} i$ for them. For example, we can define

$$\begin{aligned} x \equiv_{10} 0 &\iff \exists y\big(f(y,x) = y \wedge \neg\exists z(f(z,y) = z) \wedge \neg\exists u(f(x,u) = x)\big), \\ x \equiv_{10} 2 &\iff \exists y\big(f(x,y) = y \wedge \neg\exists z(f(y,z) = z) \wedge \neg\exists u(f(u,x) = x)\big), \\ x \equiv_{10} 4 &\iff \exists y,z\big(f(y,x) = y \wedge f(z,y) = z\big), \\ x \equiv_{10} 7 &\iff \exists y,z\big(f(x,y) = y \wedge f(y,z) = z\big). \end{aligned}$$

Further conditions on f will be

$$\begin{aligned} f(40n, 40n+1) &\equiv_{10} 0, & f(40n+10, 40n+11) &\equiv_{10} 2, \\ f(40n+20, 40n+21) &\equiv_{10} 4, & f(40n+30, 40n+31) &\equiv_{10} 7. \end{aligned} \tag{5.4}$$

The performed steps of the construction of f are schematically expressed in Figure 2. The rows and columns correspond to (the same) ten values $10n+i$, $i = 0,1,\dots,9$. The digits inside correspond to the formulas (5.2), and the letter X to the formulas (5.4); for the corresponding pairs (x,y) the values $f(x,y) \operatorname{MOD} 10$ cannot code the (boolean) value $R(x,y)$ because they are determined independently on R. These boolean values will be coded in the same row at the main diagonal. Hence $f(x,x) \operatorname{MOD} 10$ at the positions denoted by arrows will code R for both pairs (x,x) and $(x, x\pm 1)$; the sign is given by the direction of the arrow. The values

	0	1	2	3	4	5	6	7	8	9
0	$\rightarrow$	X	.	.	.	.	.	.	.	.
1	1	$\leftarrow$	.	.	.	.	.	.	.	.
2	.	.	$\rightarrow$	3	.	.	.	.	.	.
3	.	.	.	.	.	.	.	.	.	.
4	.	.	.	.	.	.	.	.	.	.
5	.	.	.	.	5	$\leftarrow$	.	.	.	.
6	.	.	.	.	.	6	$\leftarrow$	.	.	.
7	.	.	.	.	.	.	.	$\rightarrow$	8	.
8	.	.	.	.	.	.	.	.	$\rightarrow$	9
9	.	.	.	.	.	.	.	.	.	.

Figure 2. Schema of f.

2 and 7 will correspond to "true" for the second pair, and 0, 4 will correspond to "false". This condition together with (5.1) uniquely determines $f(x,x) \operatorname{MOD} 10$. For all positions denoted by dots (as well as for all non-displayed positions) we have to obey (5.1) only; for example, we can use the values 0 and 4 in all cases.

When $f(x,y) \operatorname{MOD} 10$ is chosen for all pair (x,y) we can completely determine $f(x,y)$ (on the positions not covered by (5.2)). A simple possibility is to consider all positions in the order given by Cantor's pairing function, and fill in the smallest suitable value in every case. (So we arrange that f is not too complicate with respect to R. For example, if R is /primitive/ recursive then so is f, and if R is arithmetical then f is arithmetical.) Notice that by (5.4) every of the rests 0, 2, 4, 7 is prescribed for infinitely many positions, and the other residue classes modulo 10 are completely exhausted by (5.2). Therefore we can arrange that f is a pairing function.

It remains to write the formula A; we shall use auxiliary defined symbols. Let us define

$$\operatorname{Special}(x,y) \iff f(x,y)=x \vee f(x,y)=y \vee \bigl(x \equiv_{10} 0 \wedge f(y,x)=y\bigr).$$

Then we have

$$\begin{aligned} R(x,y) \iff & \neg \operatorname{Special}(x,y) \wedge \bigl(f(x,y) \equiv_{10} 4 \vee f(x,y) \equiv_{10} 7)\bigr) \vee \\ & \vee \operatorname{Special}(x,y) \wedge \bigl(f(x,x) \equiv_{10} 2 \vee f(x,y) \equiv_{10} 7)\bigr). \end{aligned}$$

After replacing defined symbols we obtain the requested formula A. $\square$

It would be very nice if the constructed function f be (uniformly) definable from the relation R. However, it is impossible in general, even without the word "uniformly". Some relations do not suffice to define any pairing function.

The pairing functions constructed above satisfy $f(x,y) \in \{x,y\}$ for infinitely many pairs x, y; a weaker similar property is existence of infinitely many cycles in the relation $\bigl\{(x,z) \in \mathbb{N}^2 \mid \exists y\bigl(f(x,y)=z \vee f(y,x)=z\bigr)\bigr\}$. Similar rather pathological property probably cannot be avoided.

Conjecture 5.3. *If a pairing function $\bullet$ satisfy the condition $x \bullet y > \max(x,y)$ for all sufficiently large x, y then the elementary theory of $\langle \mathbb{N}; \bullet \rangle$ is decidable.*

REFERENCES

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

[Ce96] P. Cegielski, *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.

[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. 7–97.

[Ko93] I. Korec, *Definability of arithmetic operations in Pascal triangle modulo an integer divisible by two primes*, Grazer Matematische Berichte **318** (1993), 53–62.

[Ko96] ———, *List of structures strongest with respect to the first order definability*, Preprint 33/1996 of Math. Institute SAV Bratislava, 32 pages, (latest revision: April 1997).

[Ko96a] ———, *Definability of addition from multiplication and neighborhood relation and some related results*, Proceedings of the Conference on Analytic and Elementary Number Theory, Vienna, July 18-20, 1996 (W. G. Nowak and J. Schoissengeier, eds.), Universität für Bodenkultur and Universität Wien, 1996, pp. 137-148, also Preprint 23/1996 of Math. Institute SAV Bratislava.

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

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

[Na90] W. Narkiewicz, *Number Theory* (in Polish), PWN, Warszawa, 1990.

[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.

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

[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.

[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.

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

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

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:

12/1997 *Ivan Korec*: Arithmetical operations strongest with respect to the first order definability

11/1997 *Otokar Grošek, Karol Nemoga, Marcel Zanechal*: Why use bijective S-boxes in GOST-algorithm

10/1997 *Beloslav Riečan*: On the L^p space of observables

9/1997 *Ladislav Mišík Jr., Tibor Žáčik*: A formula for calculation of metric dimension of converging sequences

8/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Commutative BCK-algebras and lattice ordered groups

7/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: On representations of commutative BCK-algebras

6/1997 *Sylvia Pulmannová, Karl Svozil*: Ideals in ortholattices, Bell inequalities and simultaneously definite properties

5/1997 *Camille Debiève, Miloslav Duchoň, Beloslav Riečan*: Moment problem in some ordered vector spaces

4/1997 *Miloslav Duchoň, Beloslav Riečan*: On the Kurzweil–Stieltjes integral in ordered spaces

3/1997 *Anatolij Dvurečenskij, Maria Gabriella Graziano*: Remarks on representations of minimal clans

2/1997 *Ivan Korec*: Elementary definability from Pascal's triangle modulo p and the set of e-th powers

1/1997 *Ján Jakubík*: Lexicographic products of half linearly ordered groups

34/1996 *Emília Halušková*: Direct limits of monounary algebras

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

(continued on inside back cover)

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

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