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 $+$, $\times$ 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. $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2$, $xy+1$, x^7+y), pairing functions (i.e., bijections $\mathbb{N}^2\to\mathbb{N}$) and some further functions (e.g. $\gcd(x+1,y+1)$, $\lfloor\frac{xy}{2}\rfloor$). They are chosen from the author's (continuously actualized) list [Ko96].

1. Introduction and basic definitions

We shall use usual first order predicate calculus with equality. The symbols like $+$, $\times$, $<$, $|$ etc. will be used in their usual meaning (it usually depends only on the base set of the considered structure). The meaning of some symbols is explained when they are used. Some operations usually considered as partial ones are completed to total ones (e. g. by the value 0 for the argument 0). This is suitable from a purely technical reason: First order predicate calculus (usually) does not work with partial operations. It concerns e.g. DIV, MOD, the quotient and the rest by integer division.

We shall sometimes use lambda notation to describe some operations. The notation $\lambda_{\dots}(T)$, 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. The subscript ... also determines the order of the arguments.

We shall deal with the arithmetical structures defined as follows:

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

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.

1991 *Mathematics Subject Classification.* Primary 03B10, 03C07 Secondary 11B65, 11U07.
Key words and phrases. Elementary definability, Arithmetical structures, Undecidable theories
This work is supported by Grant 2/1224 of Slovak Academy of Sciences

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.

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].

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 1.4. *The following structures are def-strongest:*

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

Proof. (1) This is a classical result from [Ro49]. We only show the classical Tarski-Robinson formula, valid for positive x, y, z:

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

(2) We can define the constants 0 and $k = \mathrm{s}^k(0)$, and then s by the formula

$$y = \mathrm{s}(x) \iff ky = \mathrm{s}^k(kx).$$

Then we can apply (1).

(3) Multiplication by a (given or defined) constant is definable from divisibility. Therefore we can 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 the classical Tarski-Robinson formula:

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

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 $+$, $\times$.

(5) 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 $\mathbb{N}$. $\square$

2. 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 2.1. *The following operations are def-strongest:*

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

Proof. In the proof of every item of the theorem we shall use the symbol $\bullet$ for the actual operation. (Hence the formulas from one item cannot be used in 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 will be used for more general items. We can define 0 by $x = 0 \iff x \bullet x = x$ and then 1 by

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

Then we can define $\mathbf{s}(x) = 1 \bullet x$, and finally $\times$. Now we can use the classical result about $\langle \mathbb{N}; \mathbf{s}, \times \rangle$, see Theorem 1.4.

(1) We may assume $a = b + 1$. The substantial part is definition of $\mathbf{s}$. Here we use that $y = \mathbf{s}(x)$ if the sets $\{u \bullet y \mid u \in \mathbb{N}\}$, $\{x \bullet u \mid u \in \mathbb{N}\}$ differ in a unique element.

(2) For $c = 0$ we can define 0, 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 1.4.

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

(3) $\langle \mathbb{N}; \lambda_{xy}(xy + ax + by) \rangle$, where $(a, b) \notin \{(0,0), (1,1)\}$. We may assume $a > b$; then we can define $\mathbf{s}^{a-b}$. Further, we can define 0 by the property $0 \bullet 0 = 0$, multiplication by a and by b, and then $\lambda_{xy}(xy + x + y)$. Further see Theorem 1.4, the structure $\langle \mathbb{N}; \mathbf{s}^k, \lambda_{xy}(xy + x + y) \rangle$.

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

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

(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 1.4.

(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 by the property $x \bullet x = x$. In several remaining cases we have to distinguish 1 and 0, but it is not difficult. (The conditions on a, b, c imply $a = b \leq 4$, $c = 1$. Hence $0 \bullet 1 = 1$ and $1 \bullet 0 \neq 0$.) Now the substantial trick is that

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

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

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

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 $\times$, too.

(7) We have $x \bullet y = k \cdot (px + qy)^2$ for some positive integers k, p, q, $p \perp q$. We can define 0 as the idempotent and the ternary relation $px + qy = pz$ by $x \bullet y = z \bullet 0$. Therefore we can define addition on the set M of all nonnegative multiples of pq, and then (using $\bullet$ on M) all arithmetical relations on M. Finally, let us consider the mapping $\phi : x \mapsto 0 \bullet (x \bullet 0)$ of $\mathbb{N}$ into M. The ϕ-images of $+$, $\times$ are arithmetical, hence definable, and then so are $+$, $\times$, too.

(8) We shall use Lagrange's theorem that every $x \in \mathbb{N}$ is a sum of four squares. We can easily define 0, and then the function $x * y = x + y^2$ by

$$z = x * y \iff \exists x_1, x_2, x_3, x_4\big(x = x_1^2 + x_2^2 + x_3^2 + x_4^2 + 0^2 \wedge \\ \wedge z = x_1^2 + x_2^2 + x_3^2 + x_4^2 + y^2\big).$$

Then we can define addition by the formula

$$z = x + y \iff \exists x_1, x_2, x_3, x_4\big(y = (((0 * x_1) * x_2) * x_3) * x_4 \wedge \\ \wedge z = (((x * x_1) * x_2) * x_3) * x_4\big).$$

When $+$ is defined we can easily define $\times$. (Conjecture: Four squares suffice here.)

(9) Connected with Waring's problem. 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. So for $b = 1$ we can continue similarly as in (8) with $*$. The case $b > 1$ can be reduced to $b = 1$. Indeed, we can define 0, then the unary function $\lambda_x(bx)$, and then also $\lambda_x(b^n x)$. Finally, we have

$$x^n + y = \frac{b^n x^n + b^n y}{b^n} = \frac{(bx) \bullet (b^n y)}{b^n}$$

We shall not rewrite the latest formula into a strict form.

(10) 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 finally

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

So the general case is reduced to the solved one, $c = 0$; see (9). $\square$

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

Theorem 2.2. *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 (induced by permutations of big primes). 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. $\square$

3. NON-POLYNOMIAL OPERATIONS

The following theorem collects some known examples. The last item is interesting as an example of def-strongest operation which is strictly modular in the sense of [CG86].

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

(1) DIV*, the quotient by integer division;*
(2) MOD*, the rest by integer division;*
(3) exp*, the exponential function,* $\exp(x, y) = x^y$*;*
(4) β *defined by* $\beta(x, y, t) = x \operatorname{MOD}(1 + (y+1)t)$ *(the ternary Gödel coding function);*
(5) B_n *defined by* $B_n(x, y) = \binom{x+y}{x} \operatorname{MOD} n$ *provided* $n > 1$ *is divisible by two distinct primes;*
(6) C_n *defined by* $C_n(x, y) = \binom{x}{y} \operatorname{MOD} n$ *for* $x \geq y$ *and* 0 *otherwise, provided* $n > 1$ *is divisible by two distinct primes;*
(7) C_0*, defined by* $C_0(x, y) = \binom{x}{y}$ *for* $x \geq y$ *and* 0 *otherwise;*
(8) *the binary operation* H *defined by*

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

Proof. (1) We can define

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

Now we can define $\mathbf{s}$ $(= \mathbf{s}^1)$, and use the result about $\langle \mathbb{N}; \mathbf{s}^1, | \rangle$ from Theorem 1.4.

(2) We can define

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

and continue as above. (Remark: These results are contained in [Ko96]. However, later I was informed by D. RICHARD that they are contained also in his thesis.)

(3) The result is known, see e.g. [Ce96] where J.-P. Pabion & D. Richard, 1981 are mentioned. Nevertheless, we repeat the defining formulas:

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

(4) The result is mentioned in [Ce96], where [PR81], [Ri81], [Ri85] are cited.

(5) The result is proved in [Ko93].

(6) The proof is similar to that of (5). We can define the functions C_p, C_q for two prime divisors of n and the corresponding masking relations $\sqsubseteq_p$, $\sqsubseteq_q$ (where $x \sqsubseteq_p y$ means that the every p-adic digit of x is less or equal to the corresponding p-adic digit of y). Lucas' theorem is applied.

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

(8) The result is proved in [Ko94]. When displayed (in the way usual for Pascal's triangle) the function H resembles B_2 near the left margin and B_3 near the right margin. The crucial step in the proof is to define the masking relations $\sqsubseteq_2$ and $\sqsubseteq_3$. Then method of [Ko93] is used. □

Theorem 3.2. *The following operations are def-strongest:*

(1) $\lambda_{xy}\big(\gcd(x+1, y+1)\big)$;
(2) $\lambda_{xy}\big(\gcd(x+1, y)\big)$;
(3) $\lambda_{xy}\big(\gcd(x, y)+1\big)$;
(4) $\lambda_{xy}\big(\operatorname{lcm}(x+1, y+1)\big)$;
(5) $\lambda_{xy}\big(\operatorname{lcm}(x+1, y)\big)$;
(6) $\lambda_{xy}\big(\operatorname{lcm}(x, y)+1\big)$;
(7) $\lambda_{xy}\big(\lfloor \frac{xy}{k} \rfloor\big)$ *for every* $k > 1$.

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

(1) We can define $\mathbf{s}(x) = x \bullet x$, then gcd and $|$. After that we can apply item (3) of Theorem 1.4.

(2) – (6) can be proved similarly. Notice that the common idea of (1) – (6) is to compose the successor with some functions derived from $|$.

(7) We can define 1 counting repetitions in the row of Cayley's table of $\bullet$, then k^2 by the property $(x \bullet k^2) \bullet 1 = x$ and multiplication by $x \times y = (k^2 \bullet x) \bullet y$. Further, we can define successors for multiples of k. Finally, we can use a modified Tarski-Robinson formula to define addition: for positive x, y, z we have

$$z = x + y \iff (1 + kxz) \cdot (1 + kyz) = 1 + kz^2 \cdot (1 + kxy).$$

□

We shall finish the section with an open problem:

Problem 3.3. *Is the function* $B_0(x, y) = \binom{x+y}{x}$ *def-strongest?*

4. 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 4.1. *There is a def-strongest pairing function.*

Proof. The constructed pairing function $\bullet$ will code the relation $\in$ from the item (5) ot 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

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

	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 $\blacksquare$.

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.

Theorem 4.2. *There is a formula A of the form $R(x,y) \iff B$, where B contains the only non-logical symbol f, such that*

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

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

$$\begin{aligned} R(x,y) &\iff f(x,y)\,\mathrm{MOD}\,10 \in \{4,7\}. \\ \neg R(x,y) &\iff f(x,y)\,\mathrm{MOD}\,10 \in \{0,2\}. \end{aligned} \tag{4.1}$$

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 (4.1) will be used to code some additional information. Also finite and co-finite relations R force us to a special modification, see (4.4).

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

$$\begin{aligned} f(10n+1, 10n) &= 10n+1, & f(10n+2, 10n+3) &= 10n+3, \\ f(10n+5, 10n+4) &= 10n+5, & f(10n+6, 10n+5) &= 10n+6, \\ f(10n+7, 10n+8) &= 10n+8, & f(10n+8, 10n+9) &= 10n+9. \end{aligned} \tag{4.2}$$

In all other cases we shall arrange

$$f(x,y) \notin \{x,y\}. \tag{4.3}$$

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

$$\begin{aligned} f(40n, 40n+1) &\equiv_{10} 0, & f(40n+10, 40n+11) &\equiv_{10} 2, \\ f(40n+20, 40n+21) &\equiv_{10} 4, & f(40n+30, 40n+31) &\equiv_{10} 7. \end{aligned} \tag{4.4}$$

The performed steps of the construction of f are schematically expressed in Figure 2. The rows and columns correspond to (the same) ten values $10n+i$, $i = 0, 1, \ldots, 9$. The digits inside correspond to the formulas (4.2), and the letter X to the formulas (4.4); for the corresponding pairs (x,y) the values $f(x,y)\,\mathrm{MOD}\,10$ 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 $f(x,x)\,\mathrm{MOD}\,10$ at the positions denoted by arrows will code R for both pairs

	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.

(x, x) and $(x, x \pm 1)$; the sign is given by the direction of the arrow. The values 2 and 7 will correspond to "true" for the second pair, and 0, 4 will correspond to "false". This condition together with (4.1) uniquely determines $f(x, x)\,\mathrm{MOD}\,10$. For all positions denoted by dots (as well as for all non-displayed positions) we have to obey (4.1) only; for example, we can use the values 0 and 4 in all cases.

When $f(x, y)\,\mathrm{MOD}\,10$ is chosen for all pair (x, y) we can completely determine $f(x, y)$ (on the positions not covered by (4.2)). 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 (4.4) 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 (4.2). 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

$$\mathrm{Special}(x, y) \iff f(x, y) = x \vee f(x, y) = y \vee \big(x \equiv_{10} 0 \wedge f(y, x) = y\big).$$

Then we have

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

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 $\big\{(x, z) \in \mathbb{N}^2 \mid \exists y\big(f(x, y) = z \vee f(y, x) = z\big)\big\}$. Similar rather pathological property probably cannot be avoided.

Conjecture 4.3. *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

[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.

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

[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.

[Ko94] ———, *Substantially different theories of two structures associated to the same generalized Pascal triangle*, Summer School on General Algebra and Ordered Sets, Horní Lipová, September 1994 (I. Chajda, F. Halaš, F. Krutský, eds.), Palacký University, Olomouc, 1994, pp. 63–78.

[Ko94a] ———, *Theories of generalized Pascal triangles* (Proceedings of the Logic Colloquium'94, Clermont-Ferrand, July 21–30, 1994), Annals of Pure and Applied Logic (submitted July 1994), 1-7.

[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