Acta Mathematica et Informatica Universitatis Ostraviensis

Ivan Korec

Definability of arithmetical operations from binary quadratic forms

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 6 (1998), No. 1, 135--144

Persistent URL: http://dml.cz/dmlcz/120525

Definability of arithmetical operations from binary quadratic forms

Ivan Korec

Abstract: It will be shown that some binary quadratic forms $F_{a,b,c}(x,y) = ax^2 + bxy + cy^2$ are def-complete, i.e. they suffice to define addition and multiplication on the set $\mathbb{N}$ of nonnegative integers. Therefore elementary theories of the corresponding structures are undecidable. For example, the operations +, × are first order definable in the structure $\langle \mathbb{N}; F_{1,0,1} \rangle$, where $F_{1,0,1}(x,y) = x^2 + y^2$ for all $x, y \in \mathbb{N}$. The same holds for the quadratic forms $F_{6,0,1}$, $F_{15,0,1}$, for every of the operations $F_{a,-b,c}$ provided $a, b, c \in \mathbb{N}$ and $0 < b^2 \leq 4ac$, and for some further quadratic forms.

Key Words: Elementary definability. Undecidable theories. Quadratic forms

Mathematics Subject Classification: Primary 03B10. Secondary 11C99

1. Introduction

Elementary definability of +, × on the set of positive or nonnegative integers in various structures was studied for a long time. It is a frequent method of proving undecidability of the corresponding first order theories. A classical paper in this direction is [Ro49], where, e.g., definability of +, × from the successor and the divisibility is proved. A wide list of def-complete structures is contained in [Ko96]. Related results are collected also in [Ce95] and [Gr91].

We shall deal with arithmetical structures on the set $\mathbb{N}$ of nonnegative integers. They are 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. All structures considered below are obviously arithmetical.

This work is supported by Grant 5125 of Slovak Academy of Sciences.

Editorial board announces with sorrow that Professor Ivan Korec died unexpectedly on 4 August 1998.

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

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

If we consider the set of all arithmetical operations with the quasiorder "to be first order definable from" then the def-complete operations form the greatest element of the associated partially ordered set (obtained by factorization). The corresponding def-complete 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 def-completeness of some binary quadratic forms will be proved. The following theorem summarizes the results proved here and the related results of [Ko97]. The parameters a, b, c runs over $\mathbb{N}$.

Theorem 1.3. *The following operations are def-complete:*

(1) $F_{a,-b,c}(x,y) = ax^2 - bxy + cy^2$ *provided* $0 < b^2 \leq 4ac$;
(2) $F_{a,1,0}(x,y) = ax^2 + xy$ *provided* $a > 0$;
(3) $F_{a,b,c}(x,y) = ax^2 + bxy + cy^2$ *provided* $0 < b^2 = 4ac$;
(4) $F_{a,0,1}(x,y) = ax^2 + y^2$ *for* $a \in \{1, 6, 15\}$.

The items (2) and (3) and a special case of (1) are contained in [Ko97]. Therefore (2) and (3) are not proved here; (1) is proved because the additional assumption $b \mid a$ (which occurs in [Ko97]) is now removed. The case $a = 1$ of (4) is the main result of the present paper. The other two cases can be considered rather as examples, and are proved by reduction to the first one.

The quadratic form $F_{a,b,c}$ is a total binary operation in $\mathbb{N}$ if and only if

(1) a, b, c are integers and $a \geq 0$, $c \geq 0$;
(2) if $b < 0$ then $b^2 \leq 4ac$.

Further, a necessary condition for its def-completeness is that at most one coefficient is equal to 0. (Otherwise $+$ is not definable.) Hence the item (1) of Theorem 1.3 completely answers the question of def-completeness of binary quadratic forms with a negative coefficient. The items (2)–(4) give only partial answer for the binary quadratic forms with nonnegative (integer) coefficients. Maybe, the above necessary condition is sufficient also in this case, but this question remains open.

2. Notation and auxiliary results

We shall use usual first order predicate calculus with equality. The symbols like $+$, $\times$, $<$, $\mid$ (divisibility), etc. will be used in their usual meaning (it usually depends only on the base set of the considered structure, $\mathbb{N}$ in our case). We shall use the following notation for binary quadratic forms and biquadratic forms

$$F_{a,b,c}(x,y) = ax^2 + bxy + cy^2,$$
$$G_{a,b,c,d,e}(x,y) = ax^4 + bx^3y + cx^2y^2 + dxy^3 + ey^4.$$

The former notation will occur in the theorems, the later in some proofs. We shall use also the following notation for the monomials, in particular for unary linear forms:

$$M_k^n(x) = kx^n, \qquad M_k(x) = M_k^1(x) = kx.$$

Further we shall consider the following ternary relations

$$R_{a,b,c} = \{(x,y,z) \in \mathbb{N}^3 \mid ax + by = cz\}$$
$$R^0_{a,b,c} = \{(x,y,z) \in \mathbb{N}^3 \mid x \neq y \wedge ax + by = cz\}.$$

The parameters a, b, c, d, e, k, n above are nonnegative integers, only b in $F_{a,b,c}$ can be arbitrary integer. These symbols will be used also as functional, resp. relational symbols in first order formulas. Their semantics will be fixed analogously as that of $+$, $\times$, etc. Some further symbols will be explained when they are used.

Lemma 2.1. *For every pair of positive integers a, c, addition is definable in the structure $\langle \mathbb{N}; R_{a,a,c}\rangle$, and also in the structure $\langle \mathbb{N}; R^0_{a,a,c}, 0\rangle$.*

Proof. Since $R_{ka,ka,kc} = R_{a,a,c}$ for every positive integer k we may assume that a, c are relatively prime.

I. Let us consider the structure $\langle \mathbb{N}; R_{a,a,c}\rangle$ at first. If $2a \neq c$ then the constant 0 is definable by the formula $x = 0 \iff R_{a,a,c}(x,x,x)$. If $2a = c$ (i.e., $a = 1$, $c = 2$) then the constant 0 is definable by

$$x = 0 \iff \forall y, z\big(R_{a,a,c}(y,z,x) \implies y = x \wedge z = x\big).$$

Now we can define the relations

$$\mathrm{VPlus}_c = \{(x,y,z) \in \mathbb{N}^3 \mid x + y = z \wedge c \,|\, z\},$$
$$\mathrm{APlus}_a = \{(x,y,z) \in \mathbb{N}^3 \mid x + y = z \wedge a \,|\, x \wedge a \,|\, y\}.$$

They are subrelations of the graph of $+$ (the letters V, A abbreviate "values" and "arguments", respectively). They can be defined by the formulas

$$\mathrm{VPlus}_c(x,y,z) \iff \exists u\big(R_{a,a,c}(x,y,u) \wedge R_{a,a,c}(z,0,u)\big),$$
$$\mathrm{APlus}_a(x,y,z) \iff \exists u, v\big(R_{a,a,c}(u,0,x) \wedge R_{a,a,c}(v,0,y) \wedge R_{a,a,c}(u,v,z)\big).$$

The verification is almost obvious. We shall consider only $\Leftarrow$ in the second formula. The right-hand side gives

$$au = cx, \qquad av = cy, \qquad au + av = cz,$$

and then $x + y = z$. Since a, c are relatively prime the first two equalities gives $a \,|\, x$, $a \,|\, y$. Together we obtain $\mathrm{APlus}_a(x,y,z)$.

Using APlus_a we can define every ia, $i \in \mathbb{N}$, as a constant. Then we can define the operation $+$ by the formula

$$z = x + y \iff \bigvee_{i=0}^{c-1} \bigvee_{j=0}^{c-1} \exists u, v, w\Big(\mathrm{VPlus}_c(x, ia, u) \wedge \mathrm{VPlus}_c(y, ja, v) \wedge$$
$$\wedge \mathrm{VPlus}_c(u, v, w) \wedge \mathrm{VPlus}_c(z, ia + ja, w)\Big).$$

The expressions ia, ja and $ia + ja$ ought to be understand as constants. The definition of $+$ uses that always

$$z = x + y \iff (x + ia) + (y + ja) = z + (ia + ja).$$

We need here such i, j that $x + ia$, $y + ja$ are multiples of c; then all sums on the right can be expressed by VPlus_c. Since a, c are relatively prime such i, j exist and we can choose $i < c$, $j < c$.

II. The consideration for $\langle \mathbb{N}; R^0_{a,a,c}, 0\rangle$ are similar to those above but a little more complicated; we must avoid equal arguments. If we define the relation VPlus^0_c, APlus^0_a by the same formulas as VPlus_c, APlus_a above (up to the superscript 0) we obtain

$$\begin{aligned}\mathrm{VPlus}^0_c(x,y,z) &\iff x \neq y \wedge \mathrm{VPlus}_c(x,y,z),\\ \mathrm{APlus}^0_a(x,y,z) &\iff x \neq 0 \wedge y \neq 0 \wedge x \neq y \wedge \mathrm{APlus}_a(x,y,z).\end{aligned}$$

Now we can define

$$\begin{aligned}\mathrm{APlus}_a(x,y,z) \iff & x = 0 \wedge y = 0 \wedge z = 0 \vee\\ & \vee (x = 0 \vee y = 0) \wedge (x = z \vee y = z) \wedge \exists u, v\, \mathrm{APlus}^0_a(z,u,v) \vee\\ & \vee \exists u, v, w, x_1, y_1, z_1 \Big(\mathrm{APlus}^0_a(x,u,x_1) \wedge \mathrm{APlus}^0_a(y,v,y_1) \wedge\\ & \quad \wedge \mathrm{APlus}^0_a(z,w,z_1) \wedge \mathrm{APlus}^0_a(x_1,y_1,z_1) \wedge \mathrm{APlus}^0_a(u,v,w)\Big).\end{aligned}$$

The formula expresses that

$$(x+u) + (y+v) = z + (u+v);$$

the values of u, v must be chosen so that all partial sums are given in APlus_a, i.e. their arguments are pairwise distinct nonzero multiples of a.

Similarly we can define VPlus_c. (The defining formula can be a little simpler; we need not rewrite the second line of the definition of APlus_a.) Further we can continue as above. □

Remark. If the constant 0 can be defined in $\langle \mathbb{N}; R^0_{a,a,b}\rangle$ it can be eliminated from Lemma 2.1. However, we shall need not such statement.

The relation $R_{a,a,c}$ in Lemma 2.1 cannot be replaced by $R_{a,b,c}$ (and similarly for R^0), as the following example shows.

Example 2.2. Let us consider the relation $R_{6,10,15}$. No integers relatively prime to 30 occur in any element of $R_{6,10,15}$ (at any of three position). Hence these elements cannot be distinguished from each other, and no of them can be defined in $\langle \mathbb{N}; R_{6,10,15}\rangle$ as a constant. However, these constants are definable in $\langle \mathbb{N}; +\rangle$.

Conjecture 2.3. *For every positive integers a, b, c addition is definable in the structure $\langle \mathbb{N}; R_{a,b,c}\rangle$ if and only if* $\gcd(a,b,c) \in \{\gcd(a,b), \gcd(a,c), \gcd(b,c)\}$.

Lemma 2.4. *For every positive integers a, b, c such that $b^2 \leq 4ac$ the constant 0 is definable in $\langle \mathbb{N}; F_{a,-b,c}\rangle$.*

Proof. Let us use the $\bullet$ (as a binary operator) instead of $F_{a,-b,c}$. (Remember that $b^2 \leq 4ac$ arranges that the operation $F_{a,-b,c}$ is total.

If $a - b + c \neq 1$ we can define $x = 0 \iff x \bullet x = x$. Therefore we may assume $a - b + c = 1$ below. We may also assume $a \leq c$. Notice that $x \bullet x = x$ is satisfied by $x = 0$ and $x = 1$; therefore we only have to distinguish 0 and 1.

If $a = 1$ then we can define

$$x = 0 \iff x \bullet x = x \wedge \exists y\big(y \neq x \wedge y \bullet y = y \wedge (y \bullet x) \bullet (y \bullet x) = y \bullet x\big);$$

we can see that from the Cayley table of $\bullet$.

If $a > 1$ we can define

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

To see $\implies$ we can take $z = by^2$. Indeed, $0 \bullet y = cy^2$ and

$$(cy^2) \bullet 0 = ac^2y^4 = ac^2y^4 - b^2cy^4 + b^2cy^4 = a(cy^2)^2 - b(cy^2)z + cz^2 = (cy^2) \bullet z.$$

Now assume that the right-side holds; the first member expresses $x \in \{0, 1\}$. We shall show that the second member excludes $x = 1$. Indeed, substitution $x = 1$ into its last part gives $(1 \bullet y) \bullet 1 = (1 \bullet y) \bullet z$ and then

$$b(a - by + cy^2)(z - 1) = c(z - 1).$$

Since $z \neq 1$ we can divide by $z - 1$ and then for $y = c + 1$ we obtain $c \,|\, b$, i.e. $c \,|\, a + c - 1$. Then $c \,|\, a - 1$ which contradicts $1 < a \leq c$. □

For the next theorem we shall need the neighborhood relation Neib defined as follows:

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

where s denotes the successor operation.

Theorem 2.5. *The structure $\langle \mathbb{N}; \mathrm{Neib}, \times \rangle$ is def-complete.*

This is (a reformulation of) Theorem 2.2 from [Ko96], therefore the proof will not be given. It uses the idea of definition of $+$ from s, $\times$ from [Ro49], the asymmetry of distribution of squares modulo 8 and Lagrange's Four squares theorem.

3. Def-complete quadratic forms

The main result of the present paper is that the quadratic form $F_{1,0,1}$ is def-complete. We shall formulate it in more widely used terms:

Theorem 3.1. *The operations $+$, $\times$ are first order definable in the structure $\langle \mathbb{N}; \bullet \rangle$, where $x \bullet y = x^2 + y^2$ for all $x, y \in \mathbb{N}$.*

operation.

Proof. At first we need to define multiplying by 2, i.e. the unary function $M_2(x) = 2x$. It can be done through the the following steps, in which some functions $M_k^n(x) = kx^n$ are defined.

$$\begin{array}{l}
0 \bullet 0 = 0 \\
x^2 = x \bullet 0 \\
2x^2 = x \bullet x \\
4x^4 = 2x^2 \bullet 0 \\
5x^4 = 2x^2 \bullet x^2 \\
8x^4 = 2x^2 \bullet 2x^2 \\
3x^4 \bullet 4x^4 = 5x^4 \bullet 0 \\
7x^4 \bullet x^4 = 5x^4 \bullet 5x^4 \\
9x^8 = 3x^4 \bullet 0 \\
34x^8 = 5x^4 \bullet 3x^4
\end{array}$$

$$\begin{array}{l}
12x^8 \bullet x^8 = 8x^8 \bullet 9x^8 \\
36x^8 \bullet 2x^8 = 12x^8 \bullet 34x^8 \\
6x^4 \bullet 0 = 36x^8 \\
9x^4 \bullet 2x^4 = 7x^4 \bullet 6x^4 \\
3x^2 \bullet 0 = 9x^4 \\
18x^4 = 3x^2 \bullet 3x^2 \\
17x^4 \bullet 6x^4 = 18x^4 \bullet x^4 \\
16x^4 \bullet 7x^4 = 17x^4 \bullet 4x^4 \\
4x^2 \bullet 0 = 16x^4 \\
2x \bullet 0 = 4x^2.
\end{array}$$

Every formula expresses the idea of the definition of the leftest function in it. For example, we have

$$x = 0 \iff x \bullet x = x, \qquad M_1^2(x) = x \bullet 0, \qquad M_2^2(x) = x \bullet x.$$

A middle step and the last step are

$$y = M_{36}^8(x) \iff y \bullet M_2^8(x) = M_{12}^8(x) \bullet M_{34}^8(x), \quad y = M_2(x) \iff y \bullet 0 = M_4^2(x).$$

(Of course, we could reduce the number of steps by more complex definitions.) Notice that if we have defined M_k^n we can immediately define also M_k^{2n} because it can be defined by composition of M_k^n with M_1^2; these steps are not mentioned in the list. (For example, $8x^8$ can be used because $8x^4$ was defined.) However, the converse is not true. E.g., we cannot obtain $4x^2$ immediately from $4x^4$ or $9x^4$ from $9x^8$.

If we have multiplication by two then the functions $|x^2 - y^2|$ and × can be defined by

$$z = |x^2 - y^2| \iff z \bullet (x \bullet y) = 2 \cdot ((x \bullet 0) \bullet (y \bullet 0)),$$
$$z = xy \iff |x^2 - y^2| \bullet (2z) = (x \bullet y) \bullet 0.$$

Now we can define 1 (using × only) and then the neighborhood relation Neib by

$$\mathrm{Neib}(x, y) \iff \exists z \big(x \bullet z = 2 \cdot (y \bullet 1) \wedge xz = |y^2 - 1|\big).$$

We show only reverse implication. The right-hand side gives $x^2 + z^2 = 2y^2 + 2$ and $x^2 z^2 = (y^2 - 1)^2$. Hence x^2, z^2 are the roots of the quadratic equation

$$X^2 - (2y^2 + 2)X + (y^2 - 1)^2 = 0.$$

Its rots are $(y \pm 1)^2$, and hence $x^2 = (y \pm 1)^2$ which (together with $x \in \mathbb{N}$) gives $x = y \pm 1$ for $y > 0$, and $x = 1$ for $y = 0$.

By [Ko96] Neib and × suffice to define addition. □

Remark. [Ko97] contains a similar result with the sum of five squares (and the conjecture that four squares suffice). Since no unary function suffices to define +, × Theorem 3.1 is definitive in the sense that the number of squares cannot be further diminished.

Theorem 3.2. *The quadratic forms* $6x^2 + y^2$ *and* $15x^2 + y^2$ *are def-complete.*

Proof. **I.** We shall reduce the first case to the previous theorem, i.e., we shall prove that $F_{1,0,1}$ is definable from $F_{6,0,1}$. In the first stage of the proof we shall freely use all suitable M_k, and we shall define $F_{1,0,1}$ through some quadratic and biquadratic forms. Then in the second stage we shall eliminate the used linear forms, i.e., we shall show that they are definable in $\langle \mathbb{N}; F_{6,0,1} \rangle$.

Analogously as in the previous proof we shall write only the ideas of the definitions; the leftest innermost form is defined. Let us notice that $F_{c,b,a}(x, y) =$

$F_{a,b,c}(y,x)$; such steps will not be mentioned below.

$$\begin{aligned}
F_{1,0,0}(x,y) &= F_{6,0,1}(0,x)\\
2\cdot F_{3,0,2}(x,y) &= F_{6,0,1}(x,2y)\\
G_{15,0,12,0,4}(x,y) &= F_{6,0,1}\left(F_{1,0,0}(x,y),F_{3,0,2}(x,y)\right)\\
F_{6,0,1}(F_{11,0,8}(x,y),F_{3,0,2}(3x,y)) &= 97\cdot G_{15,0,12,0,4}(x,y)\\
4\cdot F_{11,0,2}(x,y) &= F_{11,0,8}(2x,y)\\
F_{2,0,3}(F_{9,0,8}(x,y),F_{11,0,2}(x,y)) &= 35\cdot G_{15,0,12,0,4}(x,y)\\
4\cdot F_{9,0,2}(x,y) &= F_{9,0,8}(2x,y)\\
F_{1,0,6}(12\cdot F_{1,0,1}(x,y),F_{9,0,2}(x,y)) &= 42\cdot G_{15,0,12,0,4}(x,y)
\end{aligned}$$

So the first stage is finished. If we take factorize the coefficients used above into prime factors we obtain that $F_{1,0,1}$ is definable in $\langle\mathbb{N}; F_{6,0,1}, M_2, M_3, M_5, M_7, M_{97}\rangle$.

In the second stage we have to prove that M_2, M_3, M_5, M_7, M_{97} are definable in $\langle\mathbb{N}; F_{6,0,1}\rangle$. We shall continue as we did in the previous proof with M_2. However, now we denote $x \bullet y = 6x^2 + y^2$; this operation is not commutative, and hence the defined function cannot be always the first argument on the left.

$x^2 = 0 \bullet x$
$6x^2 = x \bullet 0$
$7x^2 = x \bullet x$
$3x^2 \bullet x^2 = x^2 \bullet 7x^2$
$x^2 \bullet 17x^2 = 7x^2 \bullet x^2$
$3x^2 \bullet 41x^2 = 17x^2 \bullet x^2$
$x^2 \bullet 42x^2 = 17x^2 \bullet 6x^2$
$x \bullet 6x = 42x^2$
$0 \bullet 15x^2 = 6x^2 \bullet 3x^2$

$x \bullet 3x = 15x^2$
$3 \cdot 2x = 6x$
$13x^2 \bullet 49x^2 = 17x^2 \bullet 41x^2$
$0 \bullet 7x = 49x^2$
$0 \bullet 15x = 6x \bullet 3x$
$3 \cdot 5x = 15x$
$x \bullet 17x = 7x \bullet x$
$3x \bullet 39x = 7 \cdot (0 \bullet 15x)$
$x \bullet 97x = 39x \bullet 17x.$

So all necessary M_k were defined.

II. To prove that $F_{15,0,1}$ is def-complete it suffices to define $F_{6,0,1}$ in the structure $\langle\mathbb{N}; F_{15,0,1}\rangle$. The proof is similar to that above, therefore we shall write it more briefly. From the formulas

$$\begin{aligned}
F_{1,0,0}(x,y) &= F_{15,0,1}(0,x)\\
3\cdot F_{5,0,3}(x,y) &= F_{15,0,1}(x,3y)\\
G_{40,0,30,0,9}(x,y) &= F_{15,0,1}\left(F_{1,0,0}(x,y),F_{5,0,3}(x,y)\right)\\
F_{5,0,3}(F_{8,0,3}(x,y),F_{5,0,3}(0,y)) &= 8\cdot G_{40,0,30,0,9}(x,y)\\
8\cdot F_{1,0,6}(x,y) &= F_{8,0,3}(x,4y).
\end{aligned}$$

we see that $F_{6,0,1}$ is definable in $\langle\mathbb{N}; F_{15,0,1}, M_2, M_3\rangle$. It remains to show that M_2, M_3 are definable in $\langle\mathbb{N}; F_{15,0,1}\rangle$, and this is clear from the formulas

$x^2 = 0 \bullet x$
$0 \bullet 4x^2 = x^2 \bullet x^2$
$0 \bullet 2x = 4x^2$
$4x = 2 \cdot 2x$

$8x = 2 \cdot 4x$
$x \bullet 7x = 2x \bullet 2x$
$0 \bullet 17x = 4x \bullet 7x$
$3x \bullet x = 8 \cdot 17x.$ □

Theorem 3.3. *For every $a, b, c \in \mathbb{N}$ such that $0 < b^2 \leq 4ac$ the quadratic form $F_{a,-b,c}(x, y) = ax^2 - bxy + cy^2$ is def-complete.*

Proof. We shall use the symbol $\bullet$ for $F_{a,-b,c}$. Since $b^2 \leq 4ac$ the symbol $\bullet$ denotes a total operation on $\mathbb{N}$. By Lemma 2.2 we can define 0. Now we shall prove that for all x, y, z

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

Indeed, by equivalent transformations we obtain:

$$\begin{aligned} x \bullet z &= y \bullet z \\ ax^2 - bxz + cz^2 &= ay^2 - byz + cz^2 \\ ax^2 - ay^2 &= bxz - byz \\ a(x + y)(x - y) &= bz(x - y) \\ x = y \quad &\vee \quad a(x + y) = bz. \end{aligned}$$

Hence we can define the relation $R^0_{a,a,b}$ by the formula

$$R^0_{a,a,b}(x, y, z) \iff x \neq y \wedge x \bullet z = y \bullet z.$$

Now by Lemma 2.1 we can define $+$. Finally, since $xy = \frac{(x+y)^2 - |x-y|^2}{4}$ we can define $\times$ by the formula

$$z = xy \iff \exists u\big((x + u = y \vee y + u = x) \wedge (u \bullet 0) + 4a \times z = (x + y) \bullet 0\big).$$

The expression $4a \times z$ must be understood as repeated addition $z + z + \cdots + z$. □

References

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

[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.

[Ko96] I. Korec, *List of structures strongest with respect to the first order definability*, Preprint 33/1996 of Math. Institute SAV Bratislava, 32pp, latest revision: November 1997, 34pp.

[Ko96a] I. Korec, *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.

[Ko97] I. Korec, *Arithmetical operations strongest with respect to the first order definability*, Preprint 12/1997 of Math. Institute SAV Bratislava, 12pp.

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

Author's address: Mathematical Institute, Slovak Academy of Sciences,
Štefánikova 49, 81473 Bratislava, Slovakia

E-mail: korec@savba.sk

Received: February 24, 1998