A WILD MODEL OF LINEAR ARITHMETIC AND DISCRETELY ORDERED MODULES

PETR GLIVICKÝ AND PAVEL PUDLÁK

ABSTRACT. Linear arithmetics are extensions of Presburger arithmetic (Pr) by one or more unary functions, each intended as multiplication by a fixed element (scalar), and containing the full induction schemes for their respective languages.

In this paper we construct a model $\mathcal{M}$ of the 2-linear arithmetic LA_2 (linear arithmetic with two scalars) in which an infinitely long initial segment of "Peano multiplication" on $\mathcal{M}$ is $\emptyset$-definable. This shows, in particular, that LA_2 is not model complete in contrast to theories LA_1 and $\mathrm{LA}_0 = \mathrm{Pr}$ that are known to satisfy quantifier elimination up to disjunctions of primitive positive formulas.

As an application, we show that $\mathcal{M}$, as a discretely ordered module over the discretely ordered ring generated by the two scalars, is not NIP, answering negatively a question of Chernikov and Hils.

1. INTRODUCTION

There is longstanding interest in definability and related properties of various extensions of Presburger arithmetic ($\mathrm{Pr} = Th(\langle \mathbb{N}, 0, 1, +, \leq \rangle)$) by fragments of multiplication (see [Bès02] for a good survey). One class of such extensions are linear arithmetics, introduced in [Gli13]. For any cardinal number κ, the κ-linear arithmetic LA_κ is an arithmetical theory containing the full induction scheme for its language $\langle 0, 1, +, \leq, a_\alpha \rangle_{\alpha \in \kappa}$, where each a_α is a unary function symbol intended (and axiomatized) as multiplication by one fixed element (for the precise definition, see Section 2.1).

The theory LA_0 is just Pr. Its definability properties are well understood. In particular, every formula is in Pr equivalent to a disjunction of bounded primitive positive formulas (bounded pp-formulas; i.e. formulas of the form $(\exists \overline{x} < \overline{t})\chi(\overline{x}, \overline{y})$, where χ is a conjunction of atomic formulas), hence it is model complete. The same properties – bounded pp-elimination and, consequently, model completeness – have been be shown also for LA_1 ([Gli13] or [Glib]). For $\kappa \geq 2$, nevertheless, LA_κ was only known to satisfy quantifier elimination up to bounded formulas [Glia]. For more results on model theory of linear arithmetics, see [Glib] and [Glia].

In this paper, we prove that the theories LA_κ with $\kappa \geq 2$ are not model complete. We do this by constructing a model $\mathcal{M} = \langle M, 0, 1, +, \leq, a, b \rangle \models \mathrm{LA}_2$ such that for some $L \in M$ nonstandard, an operation of partial Peano multiplication $\cdot : [0, L]^2 \to M$ is $\emptyset$-definable in $\mathcal{M}$ (see Theorem 3.1). Here, $\emptyset$-definable means definable without parameters and partial

Peano multiplication is an operation $\cdot$ that can be extended to the whole M^2 in such a way that $\langle M, 0, 1, +, \cdot, \leq \rangle$ is a model of Peano arithmetic (PA).

Note that, due to the bounded quantifier elimination in LA_κ, in no model $\mathcal{M}$ of LA_κ Peano multiplication is definable on the whole M^2.

As an application of the above result, we show in section 4 that the constructed model $\mathcal{M} \models \mathrm{LA}_2$ endowed with a natural structure of a (discretely) ordered module has the independence property. This answers negatively the question of Chernikov and Hils [CH14, Question 5.9.1] whether all ordered modules are NIP.

Let us note that LA_1 (as well as $\mathrm{LA}_0 = \mathrm{Pr}$) is NIP, which follows easily from the quantifier elimination results in [Gli13], see [Glib].

2. Preliminaries

2.1. **Linear arithmetics.** For any cardinal number κ, κ-*linear arithmetic* LA_κ is the theory in the language $L_\kappa^{lin} = \langle 0, 1, +, \leq, a_\alpha \rangle_{\alpha \in \kappa}$ (where a_α are unary function symbols) with the following axioms:

(A1) $0 \neq z + 1$,   (A2) $x + 1 = y + 1 \to x = y$,

(A3) $x + 0 = x$,   (A4) $x + (y + 1) = (x + y) + 1$,

(D$_\leq$) $x \leq y \leftrightarrow (\exists z)(x + z = y)$,

(L1) $a_\alpha(x + 1) = a_\alpha x + a_\alpha 1$,   (L2) $a_\alpha(a_\beta x) = a_\beta(a_\alpha x)$,

(Ind) $\varphi(0, \overline{y}) \,\&\, (\varphi(x, \overline{y}) \to \varphi(x + 1, \overline{y})) \to (\forall x)\varphi(x, \overline{y})$ for all formulas $\varphi(x, \overline{y})$.

Strictly κ-linear arithmetic $\mathrm{LA}_\kappa^\#$ is the extension of LA_κ by the axiomatic scheme

(L$^\#$) "a_α is not definable by any formula not containing a_α".

2.2. **Models of LA_κ as discretely ordered modules.** Every $\mathcal{M} \models \mathrm{LA}_\kappa$ naturally corresponds to a discretely ordered module over a ring R given by $\{a_\alpha; \alpha \in \kappa\}$. Thus models of linear arithmetics can be understood as certain (in particular satisfying induction) discretely ordered modules. When $\mathcal{M}$ is viewed in this way, we call the elements of the ring R scalars. Below we describe this correspondence in more detail.

LA_κ proves that all elements are non-negative, but given a model $\mathcal{M} \models \mathrm{LA}_\kappa$, it is often useful to formally add negative elements to $\mathcal{M}$ and to work with this extension rather than with $\mathcal{M}$ itself. In the rest of this paper we will not explicitly distinguish between these two structures and denote both simply by $\mathcal{M}$. This should not cause any confusion as the correct interpretation will always be clear from the context.

In every $\mathcal{M} \models \mathrm{LA}_\kappa$, multiplication by any polynomial $p \in \mathbb{Z}[a_\alpha]_{\alpha \in \kappa}$ can be naturally defined. Thus $\mathcal{M}$ can be equipped with a structure of an (unordered) $\mathbb{Z}[a_\alpha]_{\alpha \in \kappa}$-module. It can be also viewed as an ordered module over the ordered ring

$$\mathbb{Z}(\mathcal{M}) := \mathbb{Z}[a_\alpha]_{\alpha \in \kappa} / Ann_{\mathbb{Z}[a_\alpha]_{\alpha \in \kappa}}(M),$$

where *Ann* denotes annihilator and the ordering of $\mathbb{Z}(\mathcal{M})$ is induced by the ordering of $\mathcal{M}$ via the map $[p] \mapsto p1$.

Let us note that, by induction in $\mathcal{M}$, $Ann_{\mathbb{Z}[a_\alpha]_{\alpha \in \kappa}}(M) = Ann_{\mathbb{Z}[a_\alpha]_{\alpha \in \kappa}}(\{1\})$. Therefore $\mathbb{Z}(\mathcal{M}) = \mathbb{Z}[a_\alpha]_{\alpha \in \kappa}$ (i.e. $\mathcal{M}$ is a faithful $\mathbb{Z}[a_\alpha]_{\alpha \in \kappa}$-module) if and only if all a_α are algebraically independent over $\mathbb{Z}$ in $\mathcal{M}$.

Notice that if $\mathcal{M}$ has the structure of an R-module (for any ring R), then the map $r \mapsto r1$ is a homomorphism from R (as a module over itself) to $\mathcal{M}$. We will often identify the scalar r with the element $r1 \in M$.

2.3. Euclidean algorithm and continued fractions.
The proof of our main result is based on certain elementary properties of continued fractions that are provable in Peano arithmetic. We review all what is necessary here.

Let $\mathcal{M}$ be a model of Peano arithmetic (PA). In this subsection, we will work in $\mathcal{M}$. This means that all quantifications, unless explicitly stated otherwise, are restricted to M. In the calculations, however, we will use negative elements and fractions freely.

Let us fix $0 < b < a \in M$. The Euclidean algorithm starting from (a, b) produces the division chain

$$r_{i-2} = r_{i-1}a_i + r_i, \tag{1}$$

for $i = 0, \dots, n$, $n \in M$, where $r_{-2} = a$, $r_{-1} = b > r_0 > r_1 > \cdots > r_n = 0$, where $r_{n-1} = \gcd(a, b)$, and

$$[a_0; a_1, \dots, a_n] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \frac{1}{a_n}}} = \frac{a}{b}$$

is the continued fraction of $\frac{a}{b}$.

The numerators and denominators of the convergents $\frac{v_i}{u_i} = [a_0; \dots, a_i]$ (in the lowest terms) satisfy the recursive relations

$$u_i = u_{i-1}a_i + u_{i-2}; \quad v_i = v_{i-1}a_i + v_{i-2}, \tag{2}$$

for $i = 0, \dots, n$, where we set $u_{-1} = v_{-2} = 0$ and $u_{-2} = v_{-1} = 1$. Clearly, $0 < u_0 < u_1 < \cdots < u_n = b$ and $0 \leq v_0 < v_1 < \cdots < v_n = a$.

From (1) and (2) it follows

$$r_i = (-1)^i(au_i - bv_i), \tag{3}$$

for $i = -2, \dots, n$.

It is well known that the convergents are exactly all the "best rational approximations of $\frac{a}{b}$ of the second kind", i.e. the following holds true (provably in PA):

Proposition 2.1. *(see e.g. [Khi97, Theorems 16 and 17])*
For $u, v \in M$, $u > 0$, the following are equivalent:

1) $|au - bv| < |au' - bv'|$ for all $\frac{v'}{u'} \neq \frac{v}{u}$ with $0 < u' \leq u$.
2) There is $0 \leq i \leq n$ such that $\frac{v}{u} = \frac{v_i}{u_i}$.

with the exception of $\frac{a}{b} = a_0 + \frac{1}{2}$, for which only 1) $\Rightarrow$ 2).

3

The above proposition gives a definition of the set of all convergents $\frac{v_i}{u_i}$ of $\frac{a}{b}$ by a bounded formula that uses multiplications only by a and b. We want a similar definition of the set of pairs (u_i, v_i). Therefore we prove:

Corollary 2.2. *Assume $\frac{a}{b} \neq a_0 + \frac{1}{2}$. Then for $u, v \in M$, $u > 0$, the following are equivalent:*

0*) $|au - bv| < |au' - bv'|$ for all $(v', u') \neq (v, u)$ with $0 < u' \leq u, b$ and $0 \leq v' \leq a$.
1*) $|au - bv| < |au' - bv'|$ for all $(v', u') \neq (v, u)$ with $0 < u' \leq u$.
2*) There is $0 \leq i \leq n$ such that $v = v_i$ and $u = u_i$.

Proof. "1*)$\Leftrightarrow$ 2*)": We have the following chain of equivalences

$$1^* \Leftrightarrow 1 \ \& \ u, v \text{ are coprime} \Leftrightarrow 2 \ \& \ u, v \text{ are coprime} \Leftrightarrow 2^*,$$

where the second equivalence is from Proposition 2.1, and the other two are trivial.

"1*)$\Rightarrow$ 0*)" is obvious.

"0*)$\Rightarrow$ 1*)": Let $(v', u') \neq (v, u)$ and $0 < u' \leq u$. We prove $|au - bv| < |au' - bv'|$. First observe that for $(v', u') = (a_0, 1)$, we get from 0*

$$|au - bv| < |a1 - ba_0| = r_0 < b. \tag{4}$$

We may assume $v' > 0$ (otherwise $|au' - bv'| = au' \geq a > b$, and we are done due to (4)). Further, let $v' = ka + v''$, $u' = lb + u''$ with $0 < v'' \leq a$, $0 < u'' \leq b$, $k, l \in M$ (notice also that $u'' \leq u' \leq u$). Then $|au' - bv'| = |au'' - bv'' + (l - k)ab|$. We distinguish the following cases:

- $l - k = 0$: Then $|au'' - bv'' + (l - k)ab| = |au'' - bv''| > |au - bv|$ by 0*).
- $l - k \geq 1$: Then $|au'' - bv'' + (l - k)ab| \geq a > b > |au - bv|$, where the last inequality is due to (4) and the first one due to $au'' - bv'' + (l - k)ab \geq a - ba + (l - k)ab \geq a$.

□

3. Wild models of linear arithmetics

In this section we will construct a model of the arithmetic LA_2 in which an infinite initial segment of a Peano multiplication is definable without parameters. In fact, we will prove even a little bit more. Say that a *formula is b-bounded* if all quantifiers in the formula are of the form $\exists x < b1$, $\forall x < b1$. For the sake of simplicity, in this subsection we will write $x < b$ instead of $x < b1$ in the quantifier bounds.

Theorem 3.1. *Let $\mathcal{M}$ be a non-standard model of PA and $L \in M$. Let $\mathcal{M}^+$ be the additive part of $\mathcal{M}$ and $\cdot$ the operation of multiplication in $\mathcal{M}$. Then there are elements $a < b \in M$ such that $\cdot \restriction [0, L]^2$ is $\emptyset$-definable by a b-bounded formula in $\langle \mathcal{M}^+, a, b \rangle$, where a, b stand for unary functions of multiplication by elements a, b.*

Note that if L is non-standard, then $\langle \mathcal{M}^+, a, b \rangle \models \mathrm{LA}_2^{\#}$ follows automatically for any a, b which satisfy the rest of the statement. Indeed, if one of the scalars were definable from the other (say b from a) then the multiplication on $[0, L]^2$ would be definable in $\langle \mathcal{M}^+, a \rangle \models \mathrm{LA}_1$, which contradicts the pp-elimination in LA_1. (For any pp-formula $\varphi(\overline{x})$ which defines an infinite set, it is easy to find $\overline{u} \neq \overline{v}$ such that φ holds for $\overline{u}, \overline{v}$ and $\frac{\overline{u} + \overline{v}}{2}$.

4

But for $\varphi(x, y, z)$ defining the graph of multiplication over the diagonal of $[0, L]^2$, this is clearly impossible.)

We will prove Theorem 3.1 in two steps. First, in subsection 3.1, we find three elements $a, b, c \in M$ such that $\cdot \upharpoonright [0, L]^2$ is $\emptyset$-definable in $\langle \mathcal{M}^+, a, b, c \rangle \models \mathrm{LA}_3$ (a, b, c here again standing for scalar multiplication by elements a, b, c). Then, in subsection 3.2, we show that we can equivalently replace the scalars a, b, c in the definition of the multiplication by certain functions definable from only two scalars a', b', and thus obtain a $\emptyset$-definition of $\cdot \upharpoonright [0, L]^2$ in $\langle \mathcal{M}^+, a', b' \rangle \models \mathrm{LA}_2$.

3.1. **A wild model of** LA_3. Let a non-standard $\mathcal{M} = \langle \mathcal{M}^+, \cdot \rangle \models \mathrm{PA}$ and $L \in M$ be arbitrary. We will find elements $a, b, c \in M$ such that $\cdot \upharpoonright [0, L]^2$ is $\emptyset$-definable in the extension $\langle \mathcal{M}^+, a, b, c \rangle \models \mathrm{LA}_3$ of $\mathcal{M}^+$ by scalar multiplication by a, b, c. Note that any choice of a, b, c yields a model of LA_3, so we only need to take care about definability of the multiplication.

Let us explain the idea of our construction before going to the details. First, we can make things a bit easier by recalling the well-known fact that it is enough to define in $\langle \mathcal{M}^+, a, b, c \rangle$ the function $x \mapsto x^2$ on the domain $[0,2L]$. Given the squaring function, multiplication on $[0, L]^2$ is defined by

$$ x \cdot y = \frac{(x + y)^2 - x^2 - y^2}{2}. \tag{5} $$

Let $(z_i)_{i=0}^{4L-1} = (1, 1^2, 2, 2^2, \ldots, 2L, (2L)^2)$ represent the required initial segment of $x \mapsto x^2$. The idea is then to pick the scalar c as any prime number bigger than $(2L)^2$ and define a and b in such a way that the numerators v_i, $i < 4L$, of convergents of the continued fraction $[a_0; \ldots, a_{4L-1}]$ representing a/b encode the initial segment of $x \mapsto x^2$ in the following sense:

$$ z_i = v_i \bmod c, \tag{6} $$

for $i = 0, \ldots, 4L - 1$.

By Corollary 2.2, the set $\{v_i; i < 4L\}$ is $\emptyset$-definable in $\langle \mathcal{M}^+, a, b, c \rangle$ (in fact in $\langle \mathcal{M}^+, a, b \rangle$). Then combining this definition with (5) and (6) easily gives the sought definition of multiplication on $[0, L]^2$.

Now we describe the construction in detail. As mentioned above, we choose c to be any prime bigger than $(2L)^2$. In order to define a and b, we recursively choose the coefficients a_i of the continued fraction $[a_0; \ldots, a_{4L-1}]$ in such a way that (6) holds true for every $0 \le i < 4L$ with the numerators v_i computed from a_is using (2). Then we take a and b coprime such that $a/b = [a_0; \ldots, a_{4L-1}]$.

Let $0 \le i < 4L$ and suppose that we have already defined a_j for all $0 \le j < i$ in such a way that (6) holds. Notice that no v_j with $-1 \le j < i$ is divisible by c, since $v_{-1} = 1$ and for $j \ge 0$, $v_j \equiv z_j \bmod c$ and $0 < z_j \le (2L)^2 < c$. Therefore there is $a_i > 0$ such that

$$ z_i \equiv v_i = v_{i-1} a_i + v_{i-2} \pmod c, $$

i.e. (6) holds for i.

It remains to show that with a, b, c defined in this way, we can find an L_3^{lin}-formula which defines $x \mapsto x^2$ on $[0, 2L]$ in $\langle \mathcal{M}^+, a, b, c \rangle$.

Let $\gamma(u, v)$ be the L_3^{lin}-formula

$$\gamma(u, v): \quad (\forall u', 0 < u' \leq u)(\forall v', 0 \leq v' \leq a)((u, v) \neq (u', v') \to |au - bv| < |au' - bv'|).$$

(This is 0^* from Corollary 2.2 without the bound $u' \leq b$.) Then the L_3^{lin}-formulas

$$V(v): \qquad (\exists u, 0 < u \leq b)\gamma(u, v), \tag{7}$$

$$V_0(v): \qquad (\exists u, 0 < u \leq b)(\gamma(u, v) \,\&\, au - bv > 0), \tag{8}$$

$$V_1(v): \qquad (\exists u, 0 < u \leq b)(\gamma(u, v) \,\&\, au - bv \leq 0), \tag{9}$$

define the sets $V = \{v_i; 0 \leq i < 4L\}$, $V_0 = \{v_i; 0 \leq i < 4L \text{ and } i \text{ even}\}$ and $V_1 = \{v_i; 0 \leq i < 4L \text{ and } i \text{ odd}\}$ respectively in $\langle \mathcal{M}^+, a, b, c \rangle$. For V, this follows directly from Corollary 2.2. The cases of V_0 and V_1 are implied by (3) with the case $au - bv = 0$ falling into V_1, as this is only possible for $i = 4L - 1$ which is odd.

Notice also that since the sequence (v_i) is increasing, we can define the set of all pairs (v_{2i}, v_{2i+1}) with $i < 2L$ by:

$$\pi(v, v'): \quad V_0(v) \,\&\, V_1(v') \,\&\, \neg(\exists w, v < w < v')V(w).$$

Finally, we define $x \mapsto x^2$ on $[0, 2L]$ by:

$$x^2 = y \leftrightarrow x = y = 0 \lor (\exists v, v')(0 \leq v, v' \leq a \,\&\, \pi(v, v') \,\&\, x = v \bmod c \,\&\, y = v' \bmod c),$$

where, of course, $z = w \bmod c$ stands for $0 \leq z < c \,\&\, (\exists m)(0 \leq m \leq w \,\&\, w = z + cm)$.

We denote the formula on the right hand side of the previous equivalence by $\sigma(x, y)$. Notice that this is a bounded formula (even bounded by constant terms) and does not contain parameters from M. The same holds true about the formula which defines multiplication on $[0, L]^2$ using (5), as it is equivalent to

$$\mu(x, y, z): \quad (\exists p, q, r)(0 \leq p, q, r < c \,\&\, \sigma(x, p) \,\&\, \sigma(y, q) \,\&\, \sigma(x + y, r) \,\&\, 2z + p + q = r),$$

where all three numbers $r = (x+y)^2$, $p = x^2$, $q = y^2$ can be bounded by $(2L)^2$ and therefore by c.

3.2. A wild model of LA_2.

Let $\langle \mathcal{M}^+, a, b, c \rangle$ be the model from the previous subsection. We will show that the multiplication on $[0, L]^2$ is $\emptyset$-definable in the structure $\langle \mathcal{M}^+, ac, abc^2 + c \rangle \models \mathrm{LA}_2$ (where again ac and $abc^2 + c$ stand for the functions of scalar multiplication by these two elements). If we could prove that scalar multiplication by a, b and c is definable using scalar multiplication by ac and $abc^2 + c$, we would be done, but this is not the case. We are only able to define the elements $a1$, $b1$ and $c1$. We would also be done, if we could define scalar multiplication by ac, bc and c, because the formula defining partial multiplication is homogeneous in a and b. We do have ac, but we are not able to define bc and c. However, what we can do is to define scalar multiplication by bc and c *restricted to the interval* $[0, a1]$, which suffices for our purpose.

Let $\alpha^* x := acx$ for all x, $\beta^* x = bcx$ for $0 \leq x \leq a$, $\gamma^* x = cx$ for $0 \leq x \leq a$ and let $\gamma^* x = \beta^* x = 0$ for $x > a$. We will modify the formula μ defined above as follows. We keep $a1$, $b1$ and $c1$ in the inequalities that determine the range of quantification. (In the

formula we used just letters a, b and c for the sake of brevity; now we have to be more careful.) We replace the other occurrences of scalar multiplication by a, b and c by the functions α^*, β^* and γ^* respectively. We will denote the resulting formula by $\mu'(x, y, z)$.

First we prove that $\mu(x, y, z) \Leftrightarrow \mu'(x, y, z)$ for all $x, y, z \in M$. In what follows, for a subformula φ of μ, we denote by φ' the corresponding subformula of μ'.

We observe that during the evaluation of $\mu(x, y, z)$, the subformulas $V(v)$, $V_0(v)$ and $V_1(v)$ are only evaluated for $0 \leq v \leq a$. For $0 \leq v, v' \leq a$ (and any u, u'), we have

$$|au - bv| < |au' - bv'| \Leftrightarrow |\alpha^* u - \beta^* v| < |\alpha^* u' - \beta^* v'|$$

and similarly for $au - bv > 0$ and $au - bv \leq 0$. Therefore, for $0 \leq v \leq a$, we get

$$V(v) \Leftrightarrow V'(v)$$

and the same for V_0', V_1'. Consequently, for $0 \leq u, v \leq a$,

$$\pi(u, v) \Leftrightarrow \pi'(u, v).$$

Further, for $0 \leq w \leq a$ and any z, we get that

$$z = w \mod c \Leftrightarrow (z = w \mod c)'.$$

(Note that $z = w \mod c$ means $z \equiv w \mod c \,\&\, 0 \leq z < c1$.) From this, it is easy to see that the same equivalence holds true also for $\sigma(x, y)$ and consequently for $\mu(x, y, z)$.

It remains to find definitions of $\beta^*, \gamma^*, a1, b1, c1$ in $\langle \mathcal{M}^+, ac, abc^2 + c \rangle$. Let us denote by $\alpha = ac$, $\beta = bc$. Then $abc^2 + c = \alpha\beta + c$.

To define γ^*, we first define an auxiliary function γ° by

$$\gamma^\circ x = ((\alpha\beta + c)x) \mod \alpha.$$

Notice that for $0 \leq x < a1$, $\gamma^\circ x = cx = \gamma^* x$, but $\gamma^\circ a = 0 \neq \gamma^* a$. This enables us to write down parameter-free definitions of $a1, c1$ and γ^* in $\langle \mathcal{M}^+, \alpha, \alpha\beta + c \rangle$:

$$
\begin{aligned}
a1 &= \min\{x > 0; \gamma^\circ x = 0\}, \\
c1 &= \gamma^\circ 1,
\end{aligned}
$$

and

$$
\gamma^* x = \begin{cases}
\gamma^\circ x & \text{for } 0 \leq x < a1, \\
\alpha 1 & \text{for } x = a1, \\
0 & \text{otherwise.}
\end{cases}
$$

To define β^*, we again start with a definition of an auxiliary function β°

$$\beta^\circ x = ((\alpha\beta + c)x) \text{ div } \alpha,$$

where the function u div α is defined by $w = u$ div $\alpha \leftrightarrow \alpha w \leq u < \alpha(w + 1)$. Again, it is not difficult to see that $\beta^\circ x = bcx = \beta^* x$ for $0 \leq x < a$, but $\beta^\circ a = abc + 1 \neq \beta^* a$, which we can use to $\emptyset$-define $b1$ and β^* in $\langle \mathcal{M}^+, \alpha, \alpha\beta + c \rangle$ as follows:

$$b1 = (\beta^\circ a) \text{ div } \alpha,$$

and

$$\beta^* x = \begin{cases} \beta^\circ x & \text{for } 0 \leq x < a1, \\ \beta^\circ x - 1 & \text{for } x = a1, \\ 0 & \text{otherwise.} \end{cases}$$

Finally note that the L_2^{lin}-definition $\mu''(x, y, z)$ of multiplication on $[0, L]^2$ in $\langle \mathcal{M}^+, \alpha, \alpha\beta + c \rangle$ that we just constructed is a bounded formula, because it was constructed from μ' by substituting definitions of functions $\alpha^*, \beta^*, \gamma^*$ and constants $a1, b1, c1$ to appropriate places. It can easily be seen that during the evaluation of μ' in $\langle \mathcal{M}^+, \alpha^*, \beta^*, \gamma^* \rangle$ the function $\alpha^* x$ is evaluated only for $0 \leq x \leq b$ and $\beta^* x, \gamma^* x$ only for $0 \leq x \leq a$. Therefore, always $0 \leq \alpha^* x, \beta^* x, \gamma^* x < abc1 < (\alpha\beta + c)1$. Clearly also $0 \leq a1, b1, c1 < (\alpha\beta + c)1$ and thus the existentially quantified variables in μ'' can be bounded by $(\alpha\beta + c)1$.

4. A NON-NIP DISCRETELY ORDERED MODULE

A structure $\mathcal{A}$ is NIP (not independence property; see [Sim15] for an extensive introduction to NIP structures and theories) if there is no formula $\varphi(\overline{x}, \overline{y})$ such that for every $n \in \omega$, there are $\overline{a_i} \in A^{l(\overline{x})}$, with $i < n$, and $\overline{b_J} \in A^{l(\overline{y})}$, with $J \subseteq n$, such that

$$\varphi(\overline{a_i}, \overline{b_J}) \Leftrightarrow i \in J.$$

Chernikov and Hils [CH14, Question 5.9.1] asked whether all ordered modules are NIP. We answer their question negatively:

Let $\langle \mathcal{M}^+, a, b \rangle \models \text{LA}_2$ be a model in which a multiplication (function $\cdot$ satisfying $x \cdot 0 = 0$ and $x(y + 1) = xy + x$) is definable on $[0, L]^2$ for some non-standard L (such models exist by Theorem 3.1) and let $\mathcal{A} = \langle M, 0, +, -, \leq, r \rangle_{r \in R}$ be the discretely ordered module corresponding to $\langle \mathcal{M}^+, a, b \rangle$ (see subsection 2.2).

Proposition 4.1. *The discretely ordered module $\mathcal{A}$ is not NIP.*

Proof. Let ψ define multiplication $\cdot$ on $[0, L]^2$ in $\langle \mathcal{M}^+, a, b \rangle$. We construct a formula ψ' by replacing possible occurrences of the constant 1 in ψ by the definition of 1 in $\mathcal{A}$ (the least positive element), replacing every quantifier (Qx) by $(Qx, 0 \leq x)$ and replacing scalars a, b by scalars $q, r \in R$ representing the same functions on M as a, b do. Then the formula $x, y, z \geq 0 \& \psi'(x, y, z)$ defines $\cdot$ on $[0, L]^2$ in $\mathcal{A}$.

Clearly $\cdot \upharpoonright \mathbb{N}^2$ is the usual multiplication on $\mathbb{N}$ and the formula $\varphi(x, y) \colon (\exists z, 0 \leq z \leq y)z \cdot x = y$ when restricted to $\mathbb{N}^2$ defines the usual divisibility relation.

It is now easy to prove that the φ has the independence property: Let $n \in \omega$ be given. For $i < n$ take a_i the i-th prime number in $\mathbb{N}$ and for $J \subseteq n$ take $b_J = \prod_{i \in J} a_i$. $\qquad \square$

5. Open problems

What is the strongest possible quantifier elimination result for LA_κ with $\kappa \geq 2$? Can definable sets in models of LA_κ be precisely characterized?

Is there a model of $\mathrm{LA}_\kappa^\#$ with $\kappa \geq 2$ whose first-order theory is model complete/NIP? Can those models be characterized?

References

[Bès02] A. Bès, *A survey of arithmetical definability*, A tribute to Maurice Boffa, Soc. Math. Belgique, 2002, pp. 1–54.

[CH14] A. Chernikov and M. Hils, *Valued difference fields and NTP2*, Israel Journal of Mathematics (2014), 1–29.

[Glia] P. Glivický, *Bounded quantifier elimination for ordered modules with integral division*, forthcoming.

[Glib] ———, *Model theory of linear arithmetics*, forthcoming.

[Gli13] ———, *Study of arithmetical structures and theories with regard to representative and descriptive analysis*, Ph.D. thesis, Charles University in Prague, 2013.

[Khi97] A. Khinchin, *Continued fractions*, Dover books on Mathematics, Dover Publications, Mineola, New York, 1997.

[Sim15] P. Simon, *A guide to NIP theories*, Lecture notes in logic, Cambridge University Press, Cambridge, 2015.

: Academy of Sciences of the Czech Republic, Institute of Mathematics, Žitná 25, 115 67 Praha 1, Czech Republic

: University of Economics, Department of Mathematics, Ekonomická 957, 148 00 Praha 4, Czech Republic

E-mail address: glivicky@math.cas.cz

E-mail address: petrglivicky@gmail.com

: Academy of Sciences of the Czech Republic, Institute of Mathematics, Žitná 25, 115 67 Praha 1, Czech Republic

E-mail address: pudlak@math.cas.cz