Multi-Dimensional Interpretations of Presburger Arithmetic in Itself

Fedor Pakhomov[12] and Alexander Zapryagaev[3]

[1]Institute of Mathematics of the Czech Academy of Sciences, Žitná 25, 115 67, Praha 1, Czech Republic
[2]Steklov Mathematical Institute of Russian Academy of Sciences, 8, Gubkina Str., Moscow, 119991, Russian Federation
[3]National Research University Higher School of Economics, 6, Usacheva Str., Moscow, 119048, Russian Federation

Abstract. Presburger Arithmetic is the true theory of natural numbers with addition. We study interpretations of Presburger Arithmetic in itself. The main result of this paper is that all self-interpretations are definably isomorphic to the trivial one. Here we consider interpretations that might be multi-dimensional. We note that this resolves a conjecture by A. Visser. In order to prove the result we show that all linear orderings that are interpretable in $(\mathbb{N}, +)$ are scattered orders with the finite Hausdorff rank and that the ranks are bounded in the terms of the dimensions of the respective interpretations.

1 Introduction

Presburger Arithmetic **PrA** is the true theory of natural numbers with addition. Unlike Peano Arithmetic **PA**, it is complete, decidable and admits quantifier elimination in an extension of its language[11].

The method of interpretations is a standard tool in model theory and in the study of decidability of first-order theories [17,8]. An interpretation of a theory **T** in a theory **U** is essentially a uniform first-order definition of models of **T** in models of **U** (see details in Section 2). In the paper we study certain questions about interpretability for Presburger Arithmetic that were well-studied in the case of stronger theories like Peano Arithmetic **PA**. Although from technical point of view the study of interpretability for Presburger Arithmetic uses completely different methods than the study of interpretability for **PA** (see, for example, [19]), we show that from interpretation-theoretic point of view, **PrA** has certain similarities to strong theories that prove all the instances of mathematical induction in their own language, i.e. **PA**, Zermelo-Fraenkel set theory **ZF**, etc.

A *reflexive* arithmetical theory ([19, p. 13]) is a theory that can prove the consistency of all its finitely axiomatizable subtheories. Peano Arithmetic **PA** and Zermelo-Fraenkel set theory **ZF** are among well-known reflexive theories. In fact, all sequential theories (very general class of theories similar to **PA**, see [6, III.1(b)]) that prove all instances of induction scheme in their language are reflexive. For sequential theories reflexivity implies that the theory cannot be interpreted in any of its finite subtheories. A. Visser have conjectured that this purely interpretational-theoretic property holds for **PrA** as well. Note that **PrA** satisfies full-induction scheme in its own language but cannot formalize the statements about consistency of formal theories.

We note that Presburger Arithmetic, unlike sequential theories, cannot encode tuples of natural numbers by single natural numbers. And thus, for interpretations in Presburger Arithmetic it is important whether individual objects are interpreted by individual objects (one-dimensional interpretations) or by tuples of objects of some fixed length m (m-dimensional interpretations).

J. Zoethout [21] considered the case of one-dimensional interpretations and proved that if any one-dimensional interpretation of **PrA** in $(\mathbb{N},+)$ gives a model that is definably isomorphic to $(\mathbb{N},+)$, then Visser's conjecture holds for one-dimensional interpretations, i.e. there are no one-dimensional interpretations of **PrA** in its finite subtheories. Moreover, he proved that any interpretation of **PrA** in $(\mathbb{N},+)$ is isomorphic to $(\mathbb{N},+)$, however he hadn't proved that the isomorphism is definable. We improve the latter result and show that the isomorphism is definable.

Theorem 1.1. *The following holds for any model $\mathfrak{A}$ of* **PrA** *that is one-dimensionally interpreted in the model $(\mathbb{N},+)$:*

(a) $\mathfrak{A}$ is isomorphic to $(\mathbb{N},+)$,
(b) the isomorphism is definable in $(\mathbb{N},+)$.

Then, by a more sophisticated technique, we establish Visser's conjecture for multi-dimensional interpretations.

Theorem 1.2. *The following holds for any model $\mathfrak{A}$ of* **PrA** *that is interpreted in $(\mathbb{N},+)$:*

(a) $\mathfrak{A}$ is isomorphic to $(\mathbb{N},+)$,
(b) the isomorphism is definable in $(\mathbb{N},+)$.

In the present paper we obtain both Theorem 1.1 (a) and Theorem 1.2 (a) as a corollary of a single fact about linear orderings interpretable in $(\mathbb{N},+)$. Recall that any non-standard model of Presburger arithmetic has the order type of the form $\mathbb{N}+\mathbb{Z}\cdot A$, where A is a dense linear ordering. In particular, it means that the order types of non-standard models of **PrA** are scattered (a linear ordering is called *scattered* if it doesn't contain a dense subordering). We show that any linear ordering that is interpretable in $(\mathbb{N},+)$ is scattered.

In fact, we establish even sharper result and estimate the ranks of the interpreted orderings. The standard notion of rank of a scattered linear ordering is the Cantor-Bendixson rank that goes back to Hausdorff [7]. However, in our case a more precise estimation is obtained using slightly different notion of VD_*-rank from [10].

Theorem 1.3. *Suppose a linear ordering $(L,\prec)$ is m-dimensionally interpretable in $(\mathbb{N},+)$. Then $(L,\prec)$ is scattered and has VD_*-rank of at most m.*

In order to prove Theorem 1.1 (b), we show that the (unique) isomorphism of the interpreted model $\mathfrak{A}$ and $(\mathbb{N}, +)$ is in fact definable in $(\mathbb{N}, +)$. This isomorphism is trivially definable using counting quantifiers, while the theorem that in Presburger Arithmetic first-order formulas with counting quantifiers have the same expressive power as first-order formulas is due to H. Apelt [1] and N. Schweikardt [13].

The proof of Theorem 1.2 relies on a theory of cardinality functions $p \mapsto |A_p|$ for definable families of finite sets $\langle A_p \subseteq \mathbb{N}^m \mid p \in P \subseteq \mathbb{N}^n \rangle$.

We note that the present work essentially is an expanded version of the paper [20]. Results of Theorem 1.1(a,b), Theorem 1.2(a), Theorem 1.3, Theorem 5.1, and Corollary 5.1 were already present in [20]. Theorem 1.2(b) is new.

The work is organized in the following way. Section 2 introduces Presburger Arithmetic and interpretations. In Section 3, we define notion of dimension for Presburger-definable sets and prove Theorem 1.3. In Section 4 we prove Theorem 1.1. In Section 5 we prove Theorem 1.2.

2 Preliminaries

2.1 Presburger Arithmetic

In this section we give some general results about Presburger Arithmetic and definable sets in $(\mathbb{N}, +)$.

Definition 2.1. Presburger Arithmetic (**PrA**) *is the elementary theory of the model* $(\mathbb{N}, +)$ *of natural numbers with addition.*

It is easy to define in the model $(\mathbb{N}, +)$ the constants $0, 1$, relation $\leq$ and modulo comparison relations $\equiv_n$, for all $n \geq 1$. In the language extended by this constants and predicates, Presburger arithmetic admits quantifier elimination [11]. Furthermore, **PrA** is decidable.

PrA has non-standard models. Unlike **PA**, however, where it is impossible to produce an explicit non-standard model by defining some recursive addition and multiplication (Tennenbaum's Theorem [18]), examples of non-standard models of **PrA** can be given easily (see [14]). By a usual argument one could show that any non-standard model of **PrA** has the order type $\mathbb{N} + \mathbb{Z} \cdot L$, where L is a dense linear ordering without endpoints. In particular, any countable model of **PrA** either has the order type $\mathbb{N}$ or $\mathbb{N} + \mathbb{Z} \cdot \mathbb{Q}$.

Definition 2.2. *For vectors* $\overline{c}, \overline{p_1}, \ldots, \overline{p_n} \in \mathbb{Z}^m$ *we call the set* $\{\overline{c} + \sum k_i \overline{p_i} \mid k_i \in \mathbb{N}\} \subseteq \mathbb{Z}^m$ *a* lattice *(or a linear set) generated by* $\{\overline{p_i}\}$ *from* $\overline{c}$*. If* $\{\overline{p_i}\}$ *are linearly independent, we call this set a* fundamental lattice*.*

According to [5], definable subsets of $\mathbb{N}^m$ are exactly the unions of a finite number of (possibly intersecting, possibly non-fundamental) lattices (also called *semilinear sets* in literature). Ito in [9] has shown that any set in $\mathbb{N}^m$ which is a union of a finite number of (possibly intersecting, possibly non-fundamental) lattices (semilinear sets) can be expressed as a union of a finite number of disjoint fundamental lattices. Hence,

Theorem 2.1. *All subsets of $\mathbb{N}^k$ definable in $(\mathbb{N}, +)$ are exactly the subsets of $\mathbb{N}^k$ that are disjoint unions of finitely many fundamental lattices.*

Definition 2.3. *For a fundamental lattice J generated by $\overline{v}_1, \dots, \overline{v}_n$ from $\overline{c}$ we call a function $f\colon J \to \mathbb{N}$* piecewise linear *if it is of the form $f(\overline{c} + x_1\overline{v}_1 + \dots + x_n\overline{v}_n) = a_0 + a_1x_1 + \dots + a_nx_n$, where $a_0, \dots, a_n$ are natural.*

For an $(\mathbb{N}, +)$-definable set A we call a function $f\colon A \to \mathbb{N}$ piecewise linear *if there is a decomposition of A into disjoint fundamental lattices $J_1, \dots, J_n$ such that the restriction of f on each J_i is linear*[1]*.*

Theorem 2.2. *Functions $f\colon \mathbb{N}^n \to \mathbb{N}$ definable in $(\mathbb{N}, +)$ are exactly piecewise linear functions.*

Proof. The definability of all piecewise linear functions in Presburger Arithmetic is obvious. A function $f\colon \mathbb{N}^n \to \mathbb{N}$ is definable if and only if its graph

$$G = \{(a_1, \dots, a_n, f(a_1, \dots, a_n)) \mid (a_1, \dots, a_n) \in \mathbb{N}^n\}$$

is definable. According to Theorem 2.1, G is a finite union of fundamental lattices $J_1 \sqcup \dots \sqcup J_k$. For $1 \le i \le k$ we denote by J_i' the projections of J_i along the last coordinate, $J_i' = \{(a_1, \dots, a_n) \mid \exists a_{n+1}((a_0, a_1, \dots, a_n, a_{n+1}) \in J_i)\}$. Clearly, all J_i' are fundamental lattices. Furthermore, the restriction of the function f on each of J_i' is linear.

2.2 Interpretations

We define multi-dimensional first-order non-parametric interpretations, following [17].

Definition 2.4. *An m-*dimensional interpretation *ι of some first-order language $\mathcal{K}$ in a model $\mathfrak{A}$ consists of first-order formulas of language of $\mathfrak{A}$:*

1. *$D_\iota(\overline{y})$ defining the set $\mathbf{D}_\iota \subseteq \mathfrak{A}^m$ (domain of interpreted model);*
2. *$P_\iota(\overline{x}_1, \dots, \overline{x}_n)$, for predicate symbols $P(x_1, \dots, x_n)$ of $\mathcal{K}$ including equality;*
3. *$f_\iota(\overline{x}_1, \dots, \overline{x}_n, \overline{y})$, for functional symbols $f(x_1, \dots, x_n)$ of $\mathcal{K}$.*

Here all vectors of variables $\overline{x}$ are of length m, and f_ι's should define graphs of some functions (modulo interpretation of equality).

Naturally, ι and $\mathfrak{A}$ give a model $\mathfrak{B}$ of the language $\mathcal{K}$ on the domain $\mathbf{D}_\iota/{\sim_\iota}$, where equivalence relation $\sim_\iota$ is given by $=_\iota (\overline{x}_1, \overline{x}_2)$. We will call $\mathfrak{B}$ the *internal model.* If $\mathfrak{B} \models \mathbf{T}$, then ι is an *interpretation of the theory* $\mathbf{T}$ in $\mathfrak{A}$. If for a first-order theory $\mathbf{U}$ an interpetaion ι is an iterpretation of $\mathbf{T}$, for any $\mathfrak{A} \models \mathbf{U}$, then ι is an interpretation of $\mathbf{T}$ in $\mathbf{U}$.

Interpretations are very natural concept, appearing in mathematics when, for example, Euclidean geometry is interpreted in the theory of real numbers $\mathbb{R}$ (two-dimensionally, by defining points as pairs of real numbers) in analytic

[1] In our work, we use the word 'piecewise' only in the sense defined here.

geometry, or the field $\mathbb{C}$ of complex numbers is two-dimensionally interpreted in $\mathbb{R}$ by defining $a + bi \leftrightarrow (a, b)$ and declaring addition and multiplication. We note that in $(\mathbb{N}, +)$ itself, the field $(\mathbb{Z}, +)$ can be interpreted. This is achieved by mapping the negative numbers to odd, positive to even and 0 to 0 and defining the addition case-by-case (through non-negative subtraction, which is definable).

We will be interested in interpretations of theories in the standard model of Presburger Arithmetic, that is, $(\mathbb{N}, +)$.

Definition 2.5. *It is said that an m-dimensional interpretation ι in a model $\mathfrak{A}$* has absolute equality *if the symbol $= \in \mathcal{K}$ is interpreted as the coincidence of two m-tuples.*

Definition 2.6. *It is said that an interpretation ι, κ in a model $\mathfrak{A}$ are definably isomorphic, if there is a first-order formula $F(\overline{x}, \overline{y})$. of the language of $\mathfrak{A}$ defining an isomorphism between the respective internal models.*

The following theorem is a version of [21, Lemma 3.2.2] extended to multi-dimensional interpretations. It shows that it is enough to consider only interpretations with absolute equality.

Theorem 2.3. *Suppose ι is an interpretation of some theory $\mathbf{U}$ in $(\mathbb{N}, +)$. Then there is an interpretation with absolute equality κ of $\mathbf{U}$ in $(\mathbb{N}, +)$ which is definably isomorphic to ι.*

Proof. Indeed there is a definable in $(\mathbb{N}, +)$ well-ordering $\prec$ of $\mathbb{N}^m$:

$$(a_0, \dots, a_{m-1}) \prec (b_0, \dots, b_{m-1}) \overset{\text{def}}{\iff} \exists i < m(\forall j < i\ (a_j = b_j) \wedge a_i < b_i).$$

Now we could define κ by taking the definition of $+$ from ι, taking the trivial interpretation of equality, and taking the domain of interpretation to be the part of the domain of ι that consists of the $\prec$-least elements of equivalence classes with respect to ι-interpretation of equality. It is easy to see that this κ is definably isomorphic to ι.

3 Ranks of Interpreted Orders

3.1 Presburger Dimension

Further we will talk only about the definability in the model $(\mathbb{N}, +)$. By a definable set we always mean a set $A \subseteq \mathbb{N}^n$ definable in $(\mathbb{N}, +)$. And by a definable function $f \colon A \to B$ we mean a function between definable sets A, B that itself is definable in $(\mathbb{N}, +)$.

Definition 3.1. *The* dimension $\dim(A)$ *of an* infinite *definable set $A \subseteq \mathbb{N}^m$ is such $k \geq 1$ that there is a definable bijection between A and $\mathbb{N}^k$.*

The following theorem shows that the definition indeed gives the unique dimension for each definable set.

Theorem 3.1. *Suppose $A \subseteq \mathbb{N}^n$ is an infinite definable set. Then there is a unique $m \in \mathbb{N}$ such that there is a Presburger definable bijection between A and $\mathbb{N}^m$, $1 \leq m \leq k$.*

Proof. First let us show that there is some m with the property. According to Theorem 2.1, all sets definable in $(\mathbb{N}, +)$ are disjoint unions of fundamental lattices $J_1, \ldots, J_n$ of the dimensions $k_1, \ldots, k_n$, respectively (the dimension of a fundamental lattice is the number of generating vectors). It is easy to see that for each J_i there is a linear bijection with $\mathbb{N}^{k_i}$, which is obviously definable. Let us put m to be the maximum of k_i's.

Now we just need to notice that for each sequence $r_1, \ldots, r_m \in \mathbb{N}$ and $u = \max(r_1, \ldots, r_m)$, if $u \geq 1$, then we could split $\mathbb{N}^u$ into disjoint union of definable sets $B_1, \ldots, B_m$, for which we have definable bijections with $\mathbb{N}^{r_1}, \ldots, \mathbb{N}^{r_m}$, respectively. We prove the latter by induction on m.

Let us show that there is no other m with this property. Assume the contrary. Then, for some $m_1 > m_2$, there is a definable bijection $f\colon \mathbb{N}^{m_1} \to \mathbb{N}^{m_2}$. Let us consider a sequence of expanding cubes

$$I_s^{m_1} \stackrel{\text{def}}{=} \{(x_1, \ldots, x_k) \mid 0 \leq x_1, \ldots, x_n \leq s\}.$$

We define function $g\colon \mathbb{N} \to \mathbb{N}$ to be the function which maps a natural number x to the least y such that $f(I_x^{m_1}) \subseteq I_y^{l_2}$. Clearly, g is a definable function. Then there should be some linear function $h\colon \mathbb{N} \to \mathbb{N}$ such that $g(x) \leq h(x)$, for all $x \in \mathbb{N}$. But since for each $x \in \mathbb{N}$ and $y < x^{m_1/m_2}$ the cube $I_x^{m_1}$ contains more points than the cube $I_y^{m_2}$, from the definition of g we see that $g(x) \geq x^{m_1/m_2}$. This contradicts the linearity of the function h.

As far as we know, this definition of dimension for Presburger definable sets was first introduced in [4] and restated in [20]. It can be seen that the dimension of a set $A \subseteq \mathbb{N}^n$ is equal to the maximal m such that there exists an m-dimensional fundamental lattice which is a subset of A.

Definition 3.2. *For a set $A \subseteq \mathbb{N}^{n+m}$ and $a \in \mathbb{N}^n$ we define the section*

$$A \restriction a = \{b \in \mathbb{N}^m \mid a \frown b\},$$

where $a \frown b$ is the concatenation of the tuples a and b.

Definition 3.3. *For a definable set $P \subseteq \mathbb{N}^n$ a family of sets $\langle A_p \subseteq \mathbb{N}^m \mid p \in P\rangle$ is called* definable *if there is a definable set $A \subseteq P \times \mathbb{N}^m$ such that $A_p = A \restriction p$, for any $p \in P$.*

Lemma 3.1. *Suppose $\langle A_p \subseteq \mathbb{N}^n \mid p \in P\rangle$ is a definable family of sets, and the set $P' \subset P$ (possibly undefinable) is such that for $p \in P'$ the sets A_p are n-dimensional and pairwise disjoint. Then P' is finite.*

Proof. Let us consider the set $A = \{p \frown a \mid p \in P \text{ and } a \in A_p\}$. By Theorem 2.1, the set A is a disjoint union of finitely many fundamental lattices $J_i \subseteq \mathbb{N}^{k+n}$.

It is easy to see that if some set A_p is n-dimensional, then for some i the section $J_i \upharpoonright p = \{a \mid p \frown a \in J_i\}$ is an n-dimensional set. Thus it is enough to show that for each J_i there are only finitely many $p \in P'$ for which the section $J_i \upharpoonright p$ is an n-dimensional set.

Let us now assume for a contradiction that for some J_i there are infinitely many $p \in P'$ for which $J_i \upharpoonright p$ are n-dimensional sets. Let us consider some $p \in P'$ such that the section $J_i \upharpoonright p$ is an n-dimensional set. Then there exists an n-dimensional fundamental lattice $K \subseteq J_i \upharpoonright p$. Suppose the generating vectors of K are $\overline{v}_1, \dots, \overline{v}_n \in \mathbb{N}^n$ and initial vector of K is $\overline{u} \in \mathbb{N}^n$. It is easy to see that each vector $\overline{v}_j$ is a non-negative linear combination of generating vectors of J_i, since otherwise for large enough $h \in \mathbb{N}$ we would have $\overline{c} + h\overline{v}_j \notin J_i$. Now notice that for any $p \in P$ and $\overline{a} \in J_i \upharpoonright p$ the n-dimensional lattice with generating vectors $\overline{v}_1, \dots, \overline{v}_n$ and initial vector $\overline{a}$ is a subset of $J_i \upharpoonright p$.

Thus infinitely many of the sets A_p, for $p \in P'$, contain some shifts of the same n-dimensional fundamental lattice K. It is easy to see that the latter contradicts the assumption that all the sets A_p, for $p \in P'$, are disjoint.

3.2 Ranks of Linear Orderings

Definition 3.4. *A linear ordering $(L, \prec)$ is called* scattered *([12, pp. 32–33]) if it does not have an infinite dense subordering.*

Definition 3.5. *Let $(L, \prec)$ be a linear ordering. We define a family of equivalence relations $\simeq_\alpha$, for ordinals $\alpha \in \mathbf{Ord}$ by transfinite recursion:*

- $\simeq_0$ *is just equality;*
- $\simeq_\lambda = \bigcup\limits_{\beta<\lambda} \simeq_\alpha$*, for limit ordinals λ;*
- $a \simeq_{\alpha+1} b \overset{\text{def}}{\iff} |\{c \in L \mid (a \prec c \prec b) \text{ or } (b \prec c \prec a)\}/{\simeq_\alpha}| < \aleph_0$.

*Now we define VD_*-*rank[2] $\mathrm{rk}(L, \prec) \in \mathbf{Ord} \cup \{\infty\}$ *of the ordering $(L, \prec)$. The VD_*-rank $\mathrm{rk}(L, \prec)$ is the least α such that $L/{\simeq_\alpha}$ is finite. If, furthermore, for all $\alpha \in \mathbf{Ord}$ the factor-set $L/{\simeq_\alpha}$ is infinite, we put* $\mathrm{rk}(L, \prec) = \infty$.

By definition we put $\alpha < \infty$, for all $\alpha \in \mathbf{Ord}$.

The definition given above corresponds to the procedure of *condensation* that glues the points at finite distance from each other. The VD_*-rank is now the minimal number of iterated condensations required to reach some finite ordering.

Remark 3.1. Linear orderings $(L, \prec)$ such that $\mathrm{rk}(L, \prec) < \infty$ are exactly the scattered linear orderings.

The orderings with the VD_*-rank equal to 0 are exactly finite orderings, and the orderings with VD_*-rank ≤ 1 are exactly the order sums of finitely many copies of $\mathbb{N}$, $-\mathbb{N}$ and 1 (one-element linear ordering).

[2] *VD* stand for *very discrete*; see [12, p. 84-89].

Remark 3.2. Each scattered linear ordering of VD_*-rank 1 is 1-dimensionally interpretable in $(\mathbb{N}, +)$. There are scattered linear orderings of VD_*-rank 2 that are not interpretable in $(\mathbb{N}, +)$.

Proof. The interpretability of linear orderings with rank 0 and rank 1 follows from the description above.

Since there are uncountably many non-isomorphic scattered linear orderings of VD_*-rank 2 and only countably many linear orderings interpretable in $(\mathbb{N}, +)$, there is some scattered linear ordering of VD_*-rank 2 that is not interpretable in $(\mathbb{N}, +)$.

Now we prove the rank condition.

Theorem 1.3. *Suppose a linear ordering $(L, \prec)$ is m-dimensionally interpretable in $(\mathbb{N}, +)$. Then $(L, \prec)$ is scattered and has VD_*-rank of at most m.*

Proof. We prove the theorem by induction on $m \geq 1$.

Assume for a contradiction that there is an m-dimensionally interpretable ordering $(L, \prec)$ with $\mathrm{rk}(L, \prec) > m$. By the definition of VD_*-rank, there are infinitely many distinct $\simeq_m$-equivalence classes in L. Hence, either there is an infinite ascending $a_0 \prec a_1 \prec \ldots$ or descending $a_0 \succ a_1 \succ \ldots$ chain of elements of L such that $a_i \not\simeq_m a_{i+1}$, for each i. Let L_i be the intervals (a_i, a_{i+1}) in the order $\prec$, if we had an ascending chain, or the intervals (a_{i+1}, a_i) in the order $\prec$, if we had a descending chain. Since $a_i \not\simeq_m a_{i+1}$, the set $L_i/{\simeq_{m-1}}$ is infinite and $\mathrm{rk}(L_i, \prec) > m - 1$.

Clearly, all the intervals L_i are definable. Let us show that $\dim(L_i) \geq m$, for each i. If $m = 1$ then it follows from the fact that L_i is infinite. If $m > 1$ then we assume for a contradiction that $\dim(L_i) < m$. Also notice that in this case $(L_i, \prec)$ would be $(m-1)$-dimensionally interpretable in $(N, +)$, which contradicts the induction hypothesis and the fact that $\mathrm{rk}(L_i, \prec) > m - 1$. Since $L_i \subseteq \mathbb{N}^m$, we conclude that $\dim(L_i) = m$, for all i.

Now consider the definable family of sets $\{(a, b) \mid a, b \in L^2\}$. We see that all L_i are in this family. Thus we have infinitely many disjoint sets of the dimension m in the family and hence there is a contradiction with Lemma 3.1.

4 Visser's conjecture in one-dimensional case

Let us now consider the extension of the first-order predicate language with an additional quantifier $\exists^{=y}x$, called a *counting quantifier* (notion introduced in [2]). It is used as follows: if $f(\overline{x}, z)$ is an $\mathcal{L}$-formula with the free variables $\overline{x}, z$, then $F = \exists^{=y}z\, G(\overline{x}, z)$ is also a formula with the free variables $\overline{x}, y$.

We extend the standard assignment of truth values to first-order formulas in the model $(\mathbb{N}, +)$ to formulas with counting quantifiers. For a formula $F(\overline{x}, y)$ of the form $\exists^{=y}zG(\overline{x}, z)$, a vector of natural numbers $\overline{a}$, and a natural number n we say that $F(\overline{a}, n)$ is true if and only if there are exactly n distinct natural numbers b such that $G(\overline{a}, b)$ is true. H. Apelt [1] and N. Schweikardt [13] have established that such an extension does not extend the expressive power of **PrA** :

Theorem 4.1. *([13, Corollary 5.10]) Every formula $F(\overline{x})$ in the language of Presburger arithmetic with counting quantifiers is equivalent in $(\mathbb{N}, +)$ to a quantifier-free formula.*

Theorem 1.1. *The following holds for any model $\mathfrak{A}$ of* **PrA** *that is one-dimensionally interpreted in the model $(\mathbb{N}, +)$:*

(a) $\mathfrak{A}$ is isomorphic to $(\mathbb{N}, +)$,
(b) the isomorphism is definable in $(\mathbb{N}, +)$.

Proof. From Theorem 2.3 it follows that it is enough to consider the case when the interpretation that gives us $\mathfrak{A}$ has absolute equality.

Let us denote the relation given by the **PrA** definition of $<$ within $\mathfrak{A}$ by $<^{\mathfrak{A}}$. Clearly, $<^{\mathfrak{A}}$ is definable in $(\mathbb{N}, +)$. Hence, by Theorem 1.3, the order type of $\mathfrak{A}$ is scattered. But since any non-standard model of **PrA** is not scattered, the model $\mathfrak{A}$ is isomorphic to $(\mathbb{N}, +)$.

It is easy to see that the isomorphism f from $\mathfrak{A}$ to $(\mathbb{N}, +)$ is the function $f\colon x \mapsto |\{y \in \mathbb{N} \mid y <^{\mathfrak{A}} x\}|$. Now we use a counting quantifier to express the function:

$$f(a) = b \iff (\mathbb{N}, +) \models \exists^{=b} z\ (z <^{\mathfrak{A}} a).$$

Now apply Theorem 4.1 and see that f is definable in $(\mathbb{N}, +)$.

This implies Visser's Conjecture for one-dimensional interpretations.

Theorem 4.3. *Theory* **PrA** *is not one-dimensionally interpretable in any of its finitely axiomatizable subtheories.*

Proof. Assume ι is an one-dimensional interpretation of **PrA** in some finitely axiomatizable subtheory $\mathbf{T}$ of **PrA**. In the standard model $(\mathbb{N}, +)$ the interpretation ι will give us a model $\mathfrak{A}$ for which there is a definable isomorphism f with $(\mathbb{N}, +)$. Now let us consider theory $\mathbf{T}'$ that consists of $\mathbf{T}$ and the statement that the definition of f gives an isomorphism between (internal) natural numbers and the structure given by ι. Clearly $\mathbf{T}'$ is finitely axiomatizable and true in $(\mathbb{N}, +)$, and hence is subtheory of **PrA**. But now note that $\mathbf{T}'$ proves that if something was true in the internal structure given by ι, it is true. And since $\mathbf{T}'$ proved any axiom of **PrA** in the internal structure given by ι, the theory $\mathbf{T}'$ proves every axiom of **PrA**. Thus $\mathbf{T}'$ coincides with **PrA**. But it is known that **PrA** is not finitely axiomatizable, contradiction.

5 Visser's Conjecture in multi-dimensional case

Our goal is to prove Theorem 1.2. In order to prove that all multi-dimensional interpretations of **PrA** in $(\mathbb{N}, +)$ are isomorphic to $(\mathbb{N}, +)$, we use the same argument as in one-dimensional case: an interpretation of a non-standard model would entail an interpretation of a non-scattered order, which is impossible by Theorem 1.3.

However, in order to show that the isomorphism is definable, we first need to develop theory of cardinality functions for definable families of finite sets.

Definition 5.1. *Let $J \subseteq \mathbb{Z}^n$ be a fundamental lattice generated by vectors $\overline{p}_1, \ldots, \overline{p}_m$ from $\overline{c}$. We say that $f\colon J \to \mathbb{N}$ is* polynomial *if there is a polynomial with rational coefficients $P_f(x_1, \ldots, x_m)$ such that $f(\overline{c} + \overline{p}_1 x_1 + \ldots + \overline{p}_m x_m) = P_f(x_1, \ldots, x_m)$, for all $x_1, \ldots, x_m \in \mathbb{N}$.*

We note that if f is a polynomial function on J, then the polynomial P_f is uniquely determined.

Definition 5.2. *Let $A \subseteq \mathbb{Z}^n$ be a definable set. We call a function $f\colon A \to \mathbb{N}$* piecewise polynomial *if there is a decomposition of A into finitely many fundamental lattices $J_1, \ldots, J_k$ such that the restriction of f on each J_i is a polynomial. The degree of f is the maximum of the degrees of the restrictions.*

We note that our definition of the degree is independent of the choice of the decomposition $J_1, \ldots, J_k$. Indeed, for a piecewise polynomial function $f\colon A \to \mathbb{N}$ consider the function $h_f\colon \mathbb{N} \to \mathbb{N}$ that maps $x \in \mathbb{N}$ to $\max\{f(a_1, \ldots, a_n)) \mid (a_1, \ldots, a_n) \in A \text{ and } a_1, \ldots, a_n \leq x\}$. Observe that if f has degree m (according to a particular decomposition) then h_f has the asymptotic growth rate of m-th degree polynomial. Thus the degree is independent of the choice of decomposition.

By the same argument as above we get the following

Lemma 5.1. *Suppose piecewise polynomial functions $f, g\colon A \to \mathbb{N}$ are such that $g(\overline{x}) \leq f(\overline{x})$, then the degree of g is less than or equal than the degree of f.*

The following theorem is a slight modification of the theorem by G.R. Blakley [3].

Theorem 5.1. *Let M be a $m \times n$ matrix of integer numbers, the function $\varphi_M\colon \mathbb{Z}^m \to \mathbb{N} \cup \{\aleph_0\}$ is defined as follows:*

$$\varphi_M(\overline{u}) \stackrel{\text{def}}{=} |\{\overline{\lambda} \in \mathbb{N}^n \mid M\overline{\lambda} = \overline{u}\}|.$$

Then, if the values of φ_M are always finite, the function φ_M is a piecewise polynomial function of degree $\leq n - \mathrm{rk}(M)$.

Proof. Since $\varphi_M(u)$ is always finite, there could be no non-zero $\overline{\lambda} \in \mathbb{N}^n$ such that $M\overline{\lambda} = 0$. Hence there are no non-zero $\overline{\lambda} \in (\mathbb{Q}^+)^n$ such that $M\overline{\lambda} = 0$. Furthermore, since M was a matrix with integer coefficients, there are no non-zero $\overline{\lambda} \in (\mathbb{R}^+)^n$ such that $M\overline{\lambda} = 0$. Thus there exists a rational $\varepsilon > 0$ such that for any $\overline{\lambda} \in \mathbb{R}^+$ with $|\overline{\lambda}|_\infty = 1$ we have $|M\overline{\lambda}|_\infty \geq \varepsilon$; here $|(a_1, \ldots, a_k)|_\infty = \max(a_1, \ldots, a_k)$.

The value $\varphi_M(u)$ is the number of points with natural coordinates in the hyperplanes $H_u = \{\overline{\lambda} \in \mathbb{R} \mid M\lambda = u\}$. From what we proved above those natural coordinates should be bounded by $|u|_\infty/\varepsilon$. It is easy to see that intersection of a k-dimensional plane with the cube $[0,N]^n$ always contains at most $((N+1)n)^k$ integer points. Given that the planes H_u are $n-\mathsf{rk}(M)$-dimensional, we see that $\varphi_M(u) \leq ((\lceil |u|_\infty/\varepsilon\rceil + 1)n)^{n-\mathsf{rk}(M)}$. The function $u \mapsto ((\lceil |u|_\infty/\varepsilon\rceil + 1)n)^{n-\mathsf{rk}(M)}$ on $\mathbb{N}^n$ clearly is piecewise polynomial of degree $n-\mathsf{rk}(M)$. Thus, by Lemma 5.1, the function φ_M is piecewise polynomial of degree $\leq n-\mathsf{rk}(M)$.

Corollary 5.1. *For any definable family of finite sets $\langle A_p \subseteq \mathbb{N}^n \mid p \in P\rangle$, the function $p \mapsto |A_p|$ is piecewise polynomial of degree $\leq n$.*

Proof. Let $A = \bigcup\limits_{p\in P} \{p \frown a \mid a \in A_p\} \subseteq \mathbb{N}^{m+n}$. We have a decomposition of A into a disjoint union of fundamental lattices $J_1,\ldots,J_n$. A sum of piecewise polynomial functions of degree $\leq n$ is piecewise polynomial of degree $\leq n$. Hence, it is enough to show that for all J_i the function $f_i\colon p \mapsto |J_i \upharpoonright p|$ is a piecewise polynomial function on on P.

Suppose J_i is generated by vectors $v_1,\ldots,v_k$ from c. Let $v_1',\ldots,v_k',c'$ be the vectors consisting of first m coordinates of $v_1,\ldots,v_k,c$, respectively. Let M be the $m\times k$-dimensional matrix corresponding to the function that maps $(x_1,\ldots,x_k)$ to $v_1'x_1 + \ldots v_k'x_k$. It is clear that $\mathsf{rk}(M) \geq k-n$. Now we see that $|J_i \upharpoonright p| = \varphi_M(p-c')$ and thus f_i is piecewise polynomial of degree $\leq n$.

Lemma 5.2. *Each monotone piecewise polynomial function $f\colon \mathbb{N}\to\mathbb{N}$ of degree $n+1$ is of the form $Cx^{n+1}+g(x)$, where $C>0$ is rational and $g\colon\mathbb{N}\to\mathbb{N}$, is piecewise polynomial of degree n.*

Proof. Since f is piecewise linear, there is a splitting of $\mathbb{N}$ into infinite arithmetical progressions and one-element sets $A_1,\ldots,A_n$ such that on each of them f is given by a polynomial $P_1,\ldots,P_n$. From monotonicity of f, it is easy to see that for all infinite A_i the corresponding P_i should have the same highest degree term Cx^{n+1}. This determines g. On infinite A_i, we see that $g(x) = P_i(x) - Cx^{n+1}$ (which is n-th degree polynomial). Thus, g is piecewise polynomial of degree n.

Theorem 1.2. *The following holds for any model $\mathfrak{A}$ of* **PrA** *that is interpreted in $(\mathbb{N},+)$:*

(a) $\mathfrak{A}$ is isomorphic to $(\mathbb{N},+)$,
(b) the isomorphism is definable in $(\mathbb{N},+)$.

Proof. As in the proof of Theorem 1.1 we may assume that the interpretation of $\mathfrak{A}$ has absolute equality. And we show that $\mathfrak{A} \simeq (\mathbb{N},+)$ by the same method. So further we just prove that the isomorphism is definable.

For $i\in\mathbb{N}$, let $S_i \subseteq \mathfrak{A}$ be the maximal initial fragment of $\mathfrak{A}$ such that all elements in it are tuples $(a_1,\ldots,a_n)$ with $a_1,\ldots,a_n \leq i$. Clearly, $\langle S_i \mid i\in\mathbb{N}\rangle$ is a definable family of finite sets. Let $h\colon\mathbb{N}\to\mathbb{N}$ be the function $x\mapsto |S_x|$. From Corollary 5.1, it follows that the function h is piecewise polynomial.

Clearly, the degree of h is non-zero. First assume that h has the degree 1. In this case, since h is monotone, from Lemma 5.2 it follows that $h(x+1)-h(x)$

is piecewise polynomial of degree 0 and hence bounded by some constant C. This allows us to create a first-order definition of the required isomorphism $f\colon \mathfrak{A} \to (\mathbb{N}, +)$ as follows. We explicitly define values of f for $a \in S_0$. For all other $a \in \mathfrak{A}$, we first find l such that $a \in S_{l+1} \setminus S_l$. Next, we explicitly consider cases for number $s < C$ of elements in $S_{l+1} \setminus S_l$ that are $<^{\mathfrak{A}}$-smaller than a. Finally, we define $f(a)$ to be $h(l) + s$.

Now assume that h has the degree $k \geq 2$. Our goal will be to show that this is in fact impossible. Let us use $\mathfrak{A}$-addition to define the following function $g\colon \mathbb{N} \to \mathbb{N}$: given $x \in \mathbb{N}$ we find the $<^{\mathfrak{A}}$-least element $a \in \mathfrak{A} \setminus S_x$. Next, we calculate $b = a +_{\mathfrak{A}} a$. We define $g(x)$ as the least y such that $b \in \mathfrak{A} \setminus S_y$. From the definition it is clear that g is a definable function.

However, there is an alternative definition of g in terms of h. Let $h'\colon \mathbb{N} \to \mathbb{N}$ be the "inverse" for h: we put $h'(x)$ to be the greatest y such that $h(y) \leq x$. Notice that $g(x) = h'(2h(x))$. By Lemma 5.2, since h is monotone, in fact, it is of the form $h(x) = Cx^k(1+o(1))$, where C is rational. Hence, $h'(x) = \frac{\sqrt[k]{x}}{C}(1+o(1))$. Thus, $g(x) = x\sqrt[k]{2}(1 + o(1))$. From the definition it is clear that g is monotone. Thus, since $\sqrt[k]{2}$ is irrational, by Lemma 5.2 the function g cannot be piecewise linear: contradiction with definability of g.

In the same manner as Theorem 4.3 (but using Theorem 1.2 instead of Theorem 1.1) we prove

Theorem 5.3. *Theory* **PrA** *is not interpretable in any of its finitely axiomatizable subtheories.*

Acknowledgments

The authors thank Lev Beklemishev for suggesting to study Visser's conjecture, a number of fruitful discussions of the subject, and his useful comments.

Work of Fedor Pakhomov is supported by grant 19-05497S of GA ČR.

References

1. Apelt, H.: Axiomatische Untersuchungen über einige mit der Presburgerschen Arithmetik verwandte Systeme. MLQ Math. Log. Q. 12.1, 131-168 (1966)
2. Barrington, D., Immerman, N., Straubing, H.: On uniformity within NC1. §J. Comput. System Sci. 41.3, 274-306 (1990)
3. Blakley, G. R.: Combinatorial remarks on partitions of a multipartite number. Duke Math. J. 31.2, 335-340 (1964)
4. Cluckers, R.: Presburger sets and p-minimal fields. J. Symbolic Logic, 68(1), 153-162 (2003)
5. Ginsburg, S., Spanier, E.: Semigroups, Presburger formulas, and languages. Pacific J. Math. 16.2, 285-296 (1966)
6. Hájek, P., Pudlák, P.: Metamathematics of first-order arithmetic. Springer-Verlag (1993)

7. Hausdorff, F.: Grundzüge einer Theorie der geordneten Mengen. Math. Ann. 65.4, 435-505 (1908)
8. Hodges, W.: Model theory. Vol. 42. Cambridge University Press (1993)
9. Ito, R.: Every semilinear set is a finite union of disjoint linear sets. J. Comput. System Sci. 3.2, 221-231 (1969)
10. Khoussainov, B., Rubin, S., Stephan, F.: Automatic linear orders and trees. ACM Trans. Comput. Log. 6.4, 675-700 (2005)
11. Presburger M.: Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt. Comptes Rendus du I congrès de Mathématiciens des Pays Slaves 92–101 (1929) – English translation in [15]
12. Rosenstein, J.: Linear orderings. Vol. 98. Academic press (1982)
13. Schweikardt, N.: Arithmetic, first-order logic, and counting quantifiers. ACM Trans. Comput. Log. 6.3, 634-671 (2005)
14. Smorynski, C.: Logical number theory I: An introduction. Springer Science & Business Media (2012)
15. Stansifer, R.: Presburger's Article on Integer Arithmetic: Remarks and Translation (Technical Report). Cornell University (1984)
16. Sturmfels, B.: On vector partition functions. J. Combin. Theory Ser. A 72.2, 302-309 (1995)
17. Tarski A., Mostowski A., Robinson R.M.: Undecidable Theories. Studies in logic and the foundations of mathematics. North-Holland (1953)
18. Tennenbaum, S.: Non-archimedean models for arithmetic. Not. Am. Math. Soc., 6(270), 44 (1959)
19. Visser, A.: An overview of interpretability logic. In Kracht M., de Rijke M., Wansing H., Zakharyaschev M., ed., Advances in Modal Logic. CSLI Lecture Notes 1.87, 307-359 (1998)
20. Zapryagaev, A., Pakhomov F.: Interpretations of Presburger arithmetic in itself. International Symposium on Logical Foundations of Computer Science. Springer, Cham (2018)
21. Zoethout, J.: Interpretations in Presburger Arithmetic. BS thesis. Utrecht University (2015)