

# Arithmetic, First-Order Logic, and Counting Quantifiers

NICOLE SCHWEIKARDT

Humboldt-Universität Berlin, Germany

---

This paper gives a thorough overview of what is known about first-order logic with counting quantifiers and with arithmetic predicates. As a main theorem we show that Presburger arithmetic is closed under unary counting quantifiers. Precisely, this means that for every first-order formula  $\varphi(y, \vec{z})$  over the signature  $\{<, +\}$  there is a first-order formula  $\psi(x, \vec{z})$  which expresses over the structure  $\langle \mathbb{N}, <, + \rangle$  (respectively, over initial segments of this structure) that the variable  $x$  is interpreted exactly by the number of possible interpretations of the variable  $y$  for which the formula  $\varphi(y, \vec{z})$  is satisfied. Applying this theorem, we obtain an easy proof of Ruhl's result that reachability (and similarly, connectivity) in finite graphs is not expressible in first-order logic with unary counting quantifiers and addition. Furthermore, the above result on Presburger arithmetic helps to show the failure of a particular version of the Crane Beach conjecture.

Categories and Subject Descriptors: F.4.1 [Mathematical Logic and Formal Languages]: Mathematical Logic

General Terms: Theory, Languages

Additional Key Words and Phrases: counting quantifiers, first-order logic, Presburger arithmetic, quantifier elimination

---

## 1. INTRODUCTION

In computational complexity theory the complexity of a problem is measured by the amount of time or space resources that are necessary for solving a problem on an (idealized) computational device such as a Turing machine. Fagin's seminal work tied this computational complexity to the descriptive complexity, i.e., to the complexity (or, the richness) of a logic that is capable of describing the problem. Until now most computational complexity classes have been characterized in such a descriptive way by logics that are certain extensions of first-order logic (cf., the textbooks [Immerman 1999; Ebbinghaus and Flum 1999]). One thing that most of these logics have in common is that they are powerful enough to express arithmetic predicates such as  $+$ ,  $\times$ , or *Bit*.

In [Barrington et al. 1990] it was shown that, on finite ordered structures, first-order logic with varying arithmetic predicates corresponds to the circuit complexity class  $AC^0$  with varying uniformity conditions. However, there are computationally easy problems such as

---

Author's address: Institut für Informatik, Humboldt-Universität Berlin, Unter den Linden 6, D-10099 Berlin, Germany. Email: [schweika@informatik.hu-berlin.de](mailto:schweika@informatik.hu-berlin.de); URL: <http://www.informatik.hu-berlin.de/~schweika>; Phone: +49 30 2093 3086; Fax: +49 30 2093 3081.

This research was performed while the author was employed at the Johannes Gutenberg-Universität Mainz, Germany.

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

© 2004 ACM 1529-3785/04/0200-0001 \$5.00

the PARITY-problem (asking whether the number of 1's in the input string is even), that do not belong to  $AC^0$ , i.e., that are not definable in first-order logic with arbitrary arithmetic predicates. In fact, an important feature that first-order logic lacks is the ability to *count*.

Various different ways of enriching first-order logic with the ability to count have been examined in the literature. A usual approach (cf., [Immerman 1999; Etessami 1997; Benedikt and Keisler 1997]) is to consider two-sorted structures that consist of a so-called “vertex domain” for the actual structure and an additional “number domain” for the counting results (usually of the same cardinality as the vertex domain) which may or may not be equipped with arithmetic predicates. However, if the actual structure is itself equipped with a linear ordering, the additional number domain does not give any additional expressivity (since the number  $i$  can be identified with the  $i$ -th largest element in the vertex domain; and the arithmetic predicates on the number domain can be translated into the corresponding predicates on the vertex domain and vice versa). In the present paper we will therefore avoid two-sorted structures. Instead, we will use the following approach, restricting attention to structures whose universe is either the set  $\mathbb{N}$  of natural numbers or an initial segment of  $\mathbb{N}$ . We enrich first-order logic by counting quantifiers of the form  $\exists^{=x}y$ . For an interpretation  $a$  of the variable  $x$ , the formula  $\exists^{=x}y \varphi(y)$  expresses that there are exactly  $a$  different interpretations of the variable  $y$  such that the formula  $\varphi(y)$  is satisfied. This leads to the logic called *FOunC*, first-order logic with unary counting quantifiers. Similarly, by adding quantifiers that allow to count the number of  $k$ -tuples that satisfy a formula, one obtains the logic *FOk-aryC*, first-order logic with  $k$ -ary counting quantifiers. In [Barrington et al. 1990] it was shown that, on finite ordered structures, *FOunC* with varying arithmetic predicates corresponds to the circuit complexity class  $TC^0$  with varying uniformity conditions.

In a different line of research, *pure* arithmetic is considered. There, the underlying structure is either the set of natural numbers with certain arithmetic predicates, or initial segments of  $\mathbb{N}$  with arithmetic predicates — and the signature contains nothing else but the arithmetic predicates. The aim is to investigate and compare the expressive power of first-order logic with different arithmetic predicates. Concerning  $\mathbb{N}$ , detailed overviews can be found in [Bès 2002; Korec 2001]; concerning initial segments of  $\mathbb{N}$ , we refer to [Esbelin and More 1998] and the references therein. One important open question is whether the so-called class of *rudimentary relations* is closed under counting, i.e., whether on initial segments of  $\langle \mathbb{N}, +, \times \rangle$  first-order logic is as expressive as *FOunC*.

The aim of the present paper is to

- give an overview of what is known about the expressive power of first-order logic with different arithmetic predicates. The emphasis here lies on finite structures and initial segments of  $\mathbb{N}$  rather than  $\mathbb{N}$ .
- examine in detail the expressive power of first-order logic with counting quantifiers and with different arithmetic predicates, for finite structures as well as for pure arithmetic on  $\mathbb{N}$  and on initial segments of  $\mathbb{N}$ . In particular, we point out that on the (non-ordered) structure  $\langle \mathbb{N}, \times \rangle$  the use of the logic *FOunC* does not make sense, since this logic lacks to have the isomorphism property on  $\langle \mathbb{N}, \times \rangle$  and its initial segments. I.e., for  $\langle \mathbb{N}, \times \rangle$  and its initial segments the usual approach with two-sorted structures would be more adequate.
- give a positive answer to the analogue of the above question on rudimentary relations, for Presburger arithmetic  $\langle \mathbb{N}, + \rangle$  rather than  $\langle \mathbb{N}, +, \times \rangle$ . I.e., we show that on  $\langle \mathbb{N}, + \rangle$  and

its initial segments first-order logic is indeed as expressive as  $FOunC$ . As applications of this result we obtain the failure of a particular version of the so-called Crane Beach conjecture, and we obtain an easy proof of Ruhl's result [Ruhl 1999] that reachability in finite graphs is not expressible in  $FOunC(+)$  and, similarly, that connectivity of finite graphs is not definable in  $FOunC(+)$ .

Via communication with Leonid Libkin the author learned that the result on Presburger arithmetic was independently discovered, but not yet published, by H. J. Keisler.

Let us mention some more papers that deal with unary counting quantifiers and with  $FO(+)$ , respectively: Benedikt and Keisler [Benedikt and Keisler 1997] investigated several different kinds of unary counting quantifiers. Implicitly, they show that, under certain presumptions, such unary counting quantifiers can be eliminated (cf., Lemma 19 in the appendix of [Benedikt and Keisler 1997]). However, their result does not deal with Presburger arithmetic and its initial segments, and their proofs are non-elementary, using hyperfinite structures. Pugh [Pugh 1994] deals with Presburger arithmetic  $\langle \mathbb{Z}, <, + \rangle$  and counting quantifiers from a different point of view. He presents a way of how a symbolic math package such as *Maple* or *Mathematica* may compute symbolic sums of the form  $\sum \{p(\vec{y}, \vec{z}) : \vec{y} \in \mathbb{Z} \text{ and } \langle \mathbb{Z}, <, + \rangle \models \varphi(\vec{y}, \vec{z})\}$ , where  $p$  is a polynomial in the variables  $\vec{y}, \vec{z}$  and  $\varphi$  is a  $FO(<, +)$ -formula. The  $FOk$ -ary  $C$ -formulas considered in the present paper correspond to the simplest such sums in which the polynomial  $p$  is the constant 1.

For other related work that deals with first-order logic, counting, and/or arithmetic from different points of view see, e.g., the articles [Lee 2003; Lima 1998; Krynicki and Zdanowski 2003; Mostowski 2001] and the references therein.

The present paper contains results of the author's dissertation [Schweikardt 2001]. The paper is structured as follows: Section 2 fixes the basic notations concerning first-order logic. Section 3 summarizes important properties of first-order logic with arithmetic predicates, concentrating on its ability and its inability, respectively, to count cardinalities of certain sets. Section 4 fixes the syntax and semantics of first-order logic with counting quantifiers and exposes important properties of this logic. In Section 5 we show that Presburger arithmetic is closed under unary counting quantifiers. Section 6 points out some applications of the previous section's result: we obtain the failure of a particular version of the Crane Beach conjecture, and we show that graph properties like reachability and connectivity are not expressible in first-order logic with unary counting and addition. Finally, Section 7 points out further questions and gives a diagram that visualizes the expressive power of first-order logic with counting quantifiers and various arithmetic predicates.

#### ACKNOWLEDGMENTS

I want to thank Clemens Lautemann, Malika More, and Thomas Schwentick for helpful discussions on the subject of this paper. Especially the proof of Proposition 4.1 is partly due to them. Furthermore, I want to thank three anonymous referees for their valuable suggestions.

## 2. PRELIMINARIES

### 2.1 Basic Notations

We use  $\mathbb{Z}$  for the set of integers,  $\mathbb{N} := \{0, 1, 2, \dots\}$  for the set of natural numbers, and  $\mathbb{N}_{>0}$  for the set of positive natural numbers. For  $N \in \mathbb{N}$  we write  $\underline{N}$  to denote the initial

segment  $\{0, \dots, N\}$  of  $\mathbb{N}$ .

For  $a, b \in \mathbb{Z}$  we write  $a \mid b$  to express that  $a$  divides  $b$ . We write  $\text{lcm}\{n_1, \dots, n_k\}$  to denote the *least common multiple* of  $n_1, \dots, n_k \in \mathbb{N}_{>0}$ . For  $n \in \mathbb{N}_{>0}$  the symbol  $\equiv_n$  denotes the *congruence relation modulo  $n$* , i.e., for  $a, b \in \mathbb{Z}$  we have  $a \equiv_n b$  iff  $n \mid a-b$ . The relation  $\equiv_n$  can be extended to rational numbers  $r, s$  via  $r \equiv_n s$  iff  $r-s = z \cdot n$  for some  $z \in \mathbb{Z}$ . For a rational number  $r$  we write  $\lfloor r \rfloor$  to denote the largest integer  $\leq r$ , and  $\lceil r \rceil$  for the smallest integer  $\geq r$ . By  $\lg(r)$  we denote the logarithm of  $r$  with respect to base 2.

A set  $P \subseteq \mathbb{N}$  is called *semi-linear* iff there are  $p, N_0 \in \mathbb{N}$  such that for every  $N > N_0$  we have  $N \in P$  iff  $N+p \in P$ .

By  $\emptyset$  we denote the empty set,  $|A|$  denotes the cardinality of a set  $A$ , and  $A^m := \{(a_1, \dots, a_m) : a_1, \dots, a_m \in A\}$  is the set of all  $m$ -tuples in  $A$ . Depending on the particular context, we use  $\vec{a}$  as abbreviation for a sequence  $a_1, \dots, a_m$  or a tuple  $(a_1, \dots, a_m)$ . Accordingly, if  $f$  is a mapping defined on all elements in  $\vec{a}$ , we write  $f(\vec{a})$  to denote the sequence  $f(a_1), \dots, f(a_m)$  or the tuple  $(f(a_1), \dots, f(a_m))$ . An  $m$ -ary relation  $R$  on  $A$  is a subset of  $A^m$ . Instead of  $\vec{a} \in R$  we often write  $R(\vec{a})$ .

## 2.2 Signatures, Structures, and Isomorphisms

A *signature*  $\tau$  consists of (a possibly infinite number of) constant symbols, relation symbols, and function symbols. Each relation or function symbol  $S \in \tau$  has a fixed arity  $\text{ar}(S) \in \mathbb{N}_{>0}$ . Whenever we refer to some “ $R \in \tau$ ” we implicitly assume that  $R$  is a *relation* symbol. Analogously, “ $c \in \tau$ ” means that  $c$  is a constant symbol, and “ $f \in \tau$ ” means that  $f$  is a function symbol.

A  $\tau$ -*structure*  $\mathcal{A} = \langle A, \tau^{\mathcal{A}} \rangle$  consists of an arbitrary set  $A$  which is called the *universe* of  $\mathcal{A}$ , and a set  $\tau^{\mathcal{A}}$  that contains an interpretation  $c^{\mathcal{A}} \in A$  for each  $c \in \tau$ , an interpretation  $R^{\mathcal{A}} \subseteq A^{\text{ar}(R)}$  for each  $R \in \tau$ , and an interpretation  $f^{\mathcal{A}} : A^{\text{ar}(f)} \rightarrow A$  for each  $f \in \tau$ . The structure  $\mathcal{A}$  is called *finite* iff its universe  $A$  is finite.

An *isomorphism*  $\pi$  between two  $\tau$ -structures  $\mathcal{A} = \langle A, \tau^{\mathcal{A}} \rangle$  and  $\mathcal{B} = \langle B, \tau^{\mathcal{B}} \rangle$  is a bijective mapping  $\pi : A \rightarrow B$  such that  $\pi(c^{\mathcal{A}}) = c^{\mathcal{B}}$  (for each  $c \in \tau$ ),  $R^{\mathcal{A}}(\vec{a})$  iff  $R^{\mathcal{B}}(\pi(\vec{a}))$  (for each  $R \in \tau$  and all  $\vec{a} \in A^{\text{ar}(R)}$ ), and  $\pi(f^{\mathcal{A}}(\vec{a})) = f^{\mathcal{B}}(\pi(\vec{a}))$  (for each  $f \in \tau$  and all  $\vec{a} \in A^{\text{ar}(f)}$ ). An *automorphism* of  $\mathcal{A}$  is an isomorphism between  $\mathcal{A}$  and  $\mathcal{A}$ .

## 2.3 First-Order Logic

Let  $\tau$  be a signature. We use  $x_1, x_2, \dots$  as variable symbols.  $\tau$ -*terms* are built from the variable symbols, the constant symbols, and the function symbols in  $\tau$  in the following way: each constant symbol in  $\tau$  and each variable symbol is a  $\tau$ -term, and if  $t_1, \dots, t_m$  are  $\tau$ -terms and  $f$  is a function symbol in  $\tau$  of arity  $m$ , then  $f(t_1, \dots, t_m)$  is a  $\tau$ -term. *Atomic  $\tau$ -formulas* are formulas of the form  $t_1=t_2$  and  $R(t_1, \dots, t_m)$ , where  $R \in \tau$  is of arity  $m$  and  $t_1, \dots, t_m$  are  $\tau$ -terms.

*First-order  $\tau$ -formulas*, for short: *FO( $\tau$ )-formulas*, are built up as usual from the atomic  $\tau$ -formulas and the logical connectives  $\vee, \neg$ , the variable symbols  $x_1, x_2, \dots$ , and the existential quantifier  $\exists$ . As usual, we use  $\forall x \varphi$  (respectively  $\varphi \wedge \psi, \varphi \rightarrow \psi, \varphi \leftrightarrow \psi$ ) as abbreviation for  $\neg \exists x \neg \varphi$  (respectively  $\neg(\neg \varphi \vee \neg \psi), \neg \varphi \vee \psi, (\varphi \wedge \psi) \vee (\neg \varphi \wedge \neg \psi)$ ).

With *free* ( $\varphi$ ) we denote the set of all variables that occur free (i.e., not in the scope of some quantifier) in  $\varphi$ . Sometimes we write  $\varphi(x_1, \dots, x_m)$  to indicate that *free* ( $\varphi$ )  $\subseteq \{x_1, \dots, x_m\}$ . We say that  $\varphi$  is a *sentence* if it has no free variable. We say that  $\varphi$  is

*quantifier free* if there is no quantifier in  $\varphi$  (i.e.,  $\varphi$  is a Boolean combination of atomic  $\tau$ -formulas). If we insert additional relation, function, or constant symbols, e.g.,  $<$  and  $+$ , into a signature  $\tau$ , we simply write  $FO(\tau, <, +)$  instead of  $FO(\tau \cup \{<, +\})$ .

For an  $FO(\tau)$ -sentence  $\varphi$  and a  $\tau$ -structure  $\mathcal{A}$  we say that  $\mathcal{A}$  models  $\varphi$  and write  $\mathcal{A} \models \varphi$  to indicate that  $\varphi$  is satisfied when interpreting each symbol in  $\tau$  by its interpretation in  $\tau^{\mathcal{A}}$ . For an  $FO(\tau)$ -formula  $\varphi(x_1, \dots, x_m)$  and for interpretations  $a_1, \dots, a_m \in A$  of the variables  $x_1, \dots, x_m$ , we write  $\mathcal{A} \models \varphi(a_1, \dots, a_m)$  (or, equivalently,  $\langle \mathcal{A}, a_1, \dots, a_m \rangle \models \varphi(x_1, \dots, x_m)$ ) to indicate that the  $(\tau \cup \{x_1, \dots, x_m\})$ -structure  $\langle \mathcal{A}, a_1, \dots, a_m \rangle$  models the  $FO(\tau, x_1, \dots, x_m)$ -sentence  $\varphi$ .

It should be obvious that  $FO(\tau)$  has the *isomorphism property*, i.e.: if  $\pi$  is an isomorphism between two  $\tau$ -structures  $\mathcal{A}$  and  $\mathcal{B}$ , if  $\varphi(\vec{x})$  is an  $FO(\tau)$ -formula, and if  $\vec{a} \in A$  is an interpretation of the variables  $\vec{x}$ , then  $\mathcal{A} \models \varphi(\vec{a})$  iff  $\pi(\mathcal{A}) \models \varphi(\pi(\vec{a}))$ .

A relation  $R \subseteq A^m$  is called  *$FO(\tau)$ -definable* in  $\mathcal{A}$  if there is an  $FO(\tau)$ -formula  $\varphi(x_1, \dots, x_m)$  such that  $R = \{(a_1, \dots, a_m) \in A^m : \mathcal{A} \models \varphi(a_1, \dots, a_m)\}$ . Accordingly, a function  $f : A^m \rightarrow A$  and an element  $a \in A$  are called  *$FO(\tau)$ -definable* in  $\mathcal{A}$  if the corresponding relations  $R_f := \{(a_1, \dots, a_m, f(a_1, \dots, a_m)) : (a_1, \dots, a_m) \in A^m\}$  and  $R_a := \{a\}$  are  *$FO(\tau)$ -definable* in  $\mathcal{A}$ .

We say that two  $FO(\tau)$ -formulas  $\varphi(\vec{x})$  and  $\psi(\vec{x})$  are *equivalent over  $\mathcal{A}$*  if, for all interpretations  $\vec{a} \in A$  of the variables  $\vec{x}$ , we have  $\mathcal{A} \models \varphi(\vec{a})$  iff  $\mathcal{A} \models \psi(\vec{a})$ . Accordingly, if  $\mathcal{K}$  is a class of  $\tau$ -structures, we say that  $\varphi(\vec{x})$  and  $\psi(\vec{x})$  are *equivalent over  $\mathcal{K}$* , if they are equivalent over every structure  $\mathcal{A} \in \mathcal{K}$ .

### 3. FIRST-ORDER LOGIC WITH ARITHMETIC

In this section we summarize important properties of first-order logic with arithmetic, and we point out the correspondence between first-order logic with arithmetic and *circuit complexity* on the one hand and *rudimentary relations* on the other hand.

#### 3.1 Arithmetic

In this paper we consider the following *arithmetic predicates* on  $\mathbb{N}$  and on initial segments  $\underline{N}$  of  $\mathbb{N}$ :

- the binary *linear ordering* predicate  $<$ ,
- the ternary *addition* predicate  $+$ , consisting of all triples  $(x, y, z)$  such that  $x + y = z$ ,
- the ternary *multiplication* predicate  $\times$ , consisting of all triples  $(x, y, z)$  such that  $x \cdot y = z$ ,
- the ternary *exponentiation* predicate *Exp*, consisting of all triples  $(x, y, z)$  such that  $x^y = z$ ,
- the binary *Bit* predicate *Bit*, consisting of all tuples  $(x, y)$  such that the  $y$ -th bit in the binary representation of  $x$  is 1, i.e.,  $\lfloor \frac{x}{2^y} \rfloor$  is odd,
- the unary *square numbers* predicate *Squares*, consisting of all numbers  $n^2$ , for all  $n \in \mathbb{N}$ .

When speaking of *arithmetic on finite structures* we consider a set  $\mathfrak{A}$  of arithmetic predicates. Furthermore, we consider arbitrary signatures  $\tau$  and all  $\tau$ -structures whose universe is an initial segment of  $\mathbb{N}$ . Given such a  $\tau$ -structure  $\mathcal{A} = \langle \underline{N}, \tau^{\mathcal{A}} \rangle$  we enrich  $\mathcal{A}$  by the arithmetic predicates in  $\mathfrak{A}$ . I.e., we move over to the  $(\tau \cup \mathfrak{A})$ -structure  $\langle \mathcal{A}, \mathfrak{A} \rangle := \langle \underline{N}, \tau^{\mathcal{A}}, \mathfrak{A}^{\mathcal{A}} \rangle$ , where  $\mathfrak{A}^{\mathcal{A}}$  is the collection of the relations  $P^{\mathcal{A}} := P \cap \underline{N}^{ar(P)}$ , for all  $P \in \mathfrak{A}$ . Usually we

will suppress the superscript  $N$  and simply write  $\mathfrak{A}$  instead of  $\mathfrak{A}^N$  and  $P$  instead of  $P^N$ . In contrast to arithmetic on finite structures, *pure arithmetic* means that we restrict our attention to structures where the signature  $\tau$  is *empty*. I.e., we only consider the structure  $\langle \mathbb{N}, \mathfrak{A} \rangle$  and the structures  $\langle \underline{N}, \mathfrak{A}^N \rangle$ , for all  $N \in \mathbb{N}$ .

To compare the expressive power of different sets of arithmetic predicates, we fix the following notation.

**DEFINITION 3.1.** Let  $\mathfrak{A}_1$  and  $\mathfrak{A}_2$  be classes of arithmetic predicates, i.e., subsets of  $\{<, +, \times, \text{Exp}, \text{Bit}, \text{Squares}\}$ .

- (a) The statement “ **$\mathbf{FO}(\mathfrak{A}_1) \subseteq \mathbf{FO}(\mathfrak{A}_2)$  on  $\mathbb{N}$** ” has the following precise meaning: For every  $\mathbf{FO}(\mathfrak{A}_1)$ -formula  $\varphi_1(\vec{x})$  there is an  $\mathbf{FO}(\mathfrak{A}_2)$ -formula  $\varphi_2(\vec{x})$  such that “ $\langle \mathbb{N}, \mathfrak{A}_1 \rangle \models \varphi_1(\vec{a})$  iff  $\langle \mathbb{N}, \mathfrak{A}_2 \rangle \models \varphi_2(\vec{a})$ ” is true for all interpretations  $\vec{a} \in \mathbb{N}$  of the variables  $\vec{x}$ .
- (b) The statement “ **$\mathbf{FO}(\mathfrak{A}_1) \subseteq \mathbf{FO}(\mathfrak{A}_2)$  on initial segments of  $\mathbb{N}$** ” has the following precise meaning: For every  $\mathbf{FO}(\mathfrak{A}_1)$ -formula  $\varphi_1(\vec{x})$  there is an  $\mathbf{FO}(\mathfrak{A}_2)$ -formula  $\varphi_2(\vec{x})$  such that “ $\langle \underline{N}, \mathfrak{A}_1 \rangle \models \varphi_1(\vec{a})$  iff  $\langle \underline{N}, \mathfrak{A}_2 \rangle \models \varphi_2(\vec{a})$ ” is true for all  $N \in \mathbb{N}_{>0}$  and all interpretations  $\vec{a} \in \underline{N}$  of the variables  $\vec{x}$ .
- (c) The statement “ **$\mathbf{FO}(\mathfrak{A}_1) \subseteq \mathbf{FO}(\mathfrak{A}_2)$  on finite structures**” has the following precise meaning: For every signature  $\tau$  and every  $\mathbf{FO}(\mathfrak{A}_1, \tau)$ -formula  $\varphi_1(\vec{x})$  there is an  $\mathbf{FO}(\mathfrak{A}_2, \tau)$ -formula  $\varphi_2(\vec{x})$  such that “ $\langle \underline{N}, \mathfrak{A}_1, \tau^A \rangle \models \varphi_1(\vec{a})$  iff  $\langle \underline{N}, \mathfrak{A}_2, \tau^A \rangle \models \varphi_2(\vec{a})$ ” is true for all  $N \in \mathbb{N}_{>0}$ , all  $\tau$ -structures  $\mathcal{A} = \langle \underline{N}, \tau^A \rangle$ , and all interpretations  $\vec{a} \in \underline{N}$  of the variables  $\vec{x}$ .  $\square$

Instead of the notion introduced in (c), one could also consider the notion “ **$\mathbf{FO}(\mathfrak{A}_1) \subseteq \mathbf{FO}(\mathfrak{A}_2)$  on finite structures with arbitrary universe**”, which has the following precise meaning: For every signature  $\tau$  and every  $\mathbf{FO}(\mathfrak{A}_1, \tau)$ -formula  $\varphi_1(\vec{x})$  there is an  $\mathbf{FO}(\mathfrak{A}_2, \tau)$ -formula  $\varphi_2(\vec{x})$  such that “ $\langle A, \mathfrak{A}_1, \tau^A \rangle \models \varphi_1(\vec{a})$  iff  $\langle A, \mathfrak{A}_2, \tau^A \rangle \models \varphi_2(\vec{a})$ ” is true for all finite, non-empty subsets  $A$  of  $\mathbb{N}$ , all  $\tau$ -structures  $\mathcal{A} = \langle A, \tau^A \rangle$ , and all interpretations  $\vec{a} \in A$  of the variables  $\vec{x}$ .

This notion has the unpleasant property that seemingly weaker arithmetic predicates cannot be replaced by seemingly stronger predicates without losing some of the expressive power. For example, the  $\mathbf{FO}(<)$ -formula “ $x < y$ ” cannot be expressed by an  $\mathbf{FO}(+, \times)$ -formula. To see this, consider the universe  $A = \{2, 7\}$ . Clearly, the formula “ $x < y$ ” is satisfied when interpreting  $x$  with 2 and  $y$  with 7, but not when interpreting  $x$  with 7 and  $y$  with 2. On the other hand, when restricted to  $A$ , the relations  $+$  and  $\times$  are empty, and therefore no  $\mathbf{FO}(+, \times)$ -formula  $\varphi(x, y)$  can distinguish between the numbers 2 and 7.

In fact, it is not difficult to see that none of the equivalences mentioned in the following Section 3.2 is valid for the notion “on finite structures with arbitrary universe”. Therefore, this notion will not be further considered in the present paper.

### 3.2 Expressive Power

The expressive power of first-order logic with arithmetic predicates  $<, +, \times$ , etc. is by now well understood:

$$\begin{aligned} \mathbf{FO}(<) &\subsetneq \mathbf{FO}(+) \subsetneq \mathbf{FO}(+, \times) \quad \text{and} \\ \mathbf{FO}(+, \times) &= \mathbf{FO}(<, \times) = \mathbf{FO}(\text{Bit}) = \mathbf{FO}(+, \text{Squares}) \\ &= \mathbf{FO}(<, +, \times, \text{Exp}, \text{Bit}, \text{Squares}) \end{aligned}$$

**on initial segments of  $\mathbb{N}$  (and on finite structures and on  $\mathbb{N}$ ).**

More precisely:

- $\mathbf{FO}(<) \subsetneq \mathbf{FO}(+)$  is true, because, on the one hand, “ $<$ ” can be expressed using “ $+$ ”, and on the other hand, there is an  $\mathbf{FO}(+)$ -formula, but no  $\mathbf{FO}(<)$ -formula which expresses that the cardinality of the underlying universe is even (cf., e.g., the textbook [Ebbinghaus and Flum 1999, Example 2.3.6]).
- $\mathbf{FO}(+) \subsetneq \mathbf{FO}(+, \times)$  is true, because, there is an  $\mathbf{FO}(+, \times)$ -formula, but no  $\mathbf{FO}(+)$ -formula which expresses that the cardinality of the underlying universe is a prime number. This is a direct consequence of the Theorem of Ginsburg and Spanier which states that the  $\mathbf{FO}(+)$ -definable subsets of  $\mathbb{N}$  are *semi-linear*, i.e., for every  $\mathbf{FO}(+)$ -formula  $\varphi(x)$  there are numbers  $p, N_0 \in \mathbb{N}$  such that for every  $N > N_0$  we have  $\langle \mathbb{N}, + \rangle \models \varphi(N)$  iff  $\langle \mathbb{N}, + \rangle \models \varphi(N+p)$ . A proof of the Theorem of Ginsburg and Spanier, based on Presburger’s quantifier elimination, can be found in the textbook [Smoryński 1991, Theorem 4.10]; an Ehrenfeucht-Fraïssé game proof is given in [Schweikardt 2001, Corollary 8.5].
- $\mathbf{FO}(+, \times) = \dots = \mathbf{FO}(<, +, \times, \mathbf{Exp}, \mathbf{Bit}, \mathbf{Squares})$  is true because of the following:

**THEOREM 3.2.** *There is*

- (a) an  $\mathbf{FO}(\mathbf{Bit})$ -formula  $\varphi_{<}(x, y)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y} \in \underline{N}$  of the variables  $x, y$ , we have  $\langle \underline{N}, \mathbf{Bit} \rangle \models \varphi_{<}(\mathbf{x}, \mathbf{y})$  iff  $\mathbf{x} < \mathbf{y}$ .
- (b) an  $\mathbf{FO}(\mathbf{Bit})$ -formula  $\varphi_{+}(x, y, z)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \underline{N}$  of  $x, y, z$ , we have  $\langle \underline{N}, \mathbf{Bit} \rangle \models \varphi_{+}(\mathbf{x}, \mathbf{y}, \mathbf{z})$  iff  $\mathbf{x} + \mathbf{y} = \mathbf{z}$ .
- (c) an  $\mathbf{FO}(\mathbf{Bit})$ -formula  $\varphi_{\times}(x, y, z)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \underline{N}$  of  $x, y, z$ , we have  $\langle \underline{N}, \mathbf{Bit} \rangle \models \varphi_{\times}(\mathbf{x}, \mathbf{y}, \mathbf{z})$  iff  $\mathbf{x} \times \mathbf{y} = \mathbf{z}$ .
- (d) an  $\mathbf{FO}(<, \times)$ -formula  $\varphi_{\mathbf{Bit}}(x, y)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y} \in \underline{N}$  of the variables  $x, y$ , we have  $\langle \underline{N}, <, \times \rangle \models \varphi_{\mathbf{Bit}}(\mathbf{x}, \mathbf{y})$  iff  $\mathbf{Bit}(\mathbf{x}, \mathbf{y})$ .
- (e) an  $\mathbf{FO}(+, \times)$ -formula  $\varphi_{\mathbf{Exp}}(x, y, z)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \underline{N}$  of  $x, y, z$ , we have  $\langle \underline{N}, +, \times \rangle \models \varphi_{\mathbf{Exp}}(\mathbf{x}, \mathbf{y}, \mathbf{z})$  iff  $\mathbf{x} = \mathbf{y}^{\mathbf{z}}$ .
- (f) an  $\mathbf{FO}(+, \mathbf{Squares})$ -formula  $\varphi_{\times}(x, y, z)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\mathbf{x}, \mathbf{y}, \mathbf{z} \in \underline{N}$  of  $x, y, z$ , we have  $\langle \underline{N}, +, \mathbf{Squares} \rangle \models \varphi_{\times}(\mathbf{x}, \mathbf{y}, \mathbf{z})$  iff  $\mathbf{x} \times \mathbf{y} = \mathbf{z}$ .  $\square$

**PROOF.** The proofs of the parts (a)–(e) are very involved. Part (a) is shown in [Dawar et al. 1998].  $\mathbf{FO}(<, \mathbf{Bit})$ -formulas for (b) and (c) are outlined in the textbook [Immerman 1999]. (d) is shown in [Lee 2003]. (e) is shown in [Bennett 1962] (see also Lindell’s email note [Lindell 1995]).

The proof of part (f) is not so difficult:

*Step 1* is to construct an  $\mathbf{FO}(+, \mathbf{Squares})$ -formula  $\psi(u, v)$  expressing that  $u^2 = v$ . Here, one can make use of the equation  $(u - 1)^2 = u^2 - 2u + 1$  which gives us that  $u^2 = v$  is valid if and only if

- $v$  is a square number, i.e.,  $\mathbf{Squares}(v)$ , and
- $(u = 0$  and  $v = 0)$  or  $(u = 1$  and  $v = 1)$  or
- for the number  $w$  that is the predecessor of  $v$  in the set  $\mathbf{Squares}$  we have that  $w = v - 2u + 1$ .

It is straightforward to express this by an  $FO(+, \text{Squares})$ -formula  $\psi(x, y)$ .

*Step 2* is to construct an  $FO(+, \text{Squares})$ -formula  $\varphi'_\times(x, y, z)$  expressing that  $x \times y = z$  for numbers  $x, y$  of size at most  $\sqrt{N}$  (when considering the universe  $\{0, \dots, N\}$ ). Here, one can make use of the equation  $(x-y)^2 = x^2 - 2xy + y^2$  which gives us that  $x \times y = z$  if and only if the equation  $w = u - 2z + v$  is true for the numbers  $u := x^2$ ,  $v := y^2$ , and  $w := (x-y)^2$ . Using the formula  $\psi$  from Step 1, it is straightforward to express this by an  $FO(+, \text{Squares})$ -formula  $\varphi'_\times(x, y, z)$ . Note that this formula defines the multiplication  $\times$  only for numbers  $x, y$  of size at most  $\sqrt{N}$ , where  $N$  is the maximum element in the universe.

*Step 3* is to lift the multiplication from numbers of size up to  $\sqrt{N}$  to numbers of size up to  $N$ . Such a lifting is proved in [Lynch 1982, Lemma 1 (ii)]. The details are similar to the details in Step 2 of the proof of Theorem 3.4 (d) in the appendix of the present paper. The basic idea is the following:

1. For numbers  $x \in \{0, \dots, N\}$  use the  $(M+1)$ -ary decomposition  $x = x_1 \cdot (M+1) + x_0$ , where  $x_1, x_0 \leq M$  and  $M := \lfloor \sqrt{N} \rfloor$ .
2. Show that this decomposition is definable via an  $FO(+, \text{Squares})$ -formula  $\chi(x, x_1, x_0)$ .
3. Use  $\varphi'_\times$  to construct a formula  $\varphi''_\times(x_1, x_0, y_1, y_0, z_1, z_0)$  that defines the multiplication for the  $(M+1)$ -ary decompositions of numbers  $x, y, z$ .

Finally this leads to the desired  $FO(+, \text{Squares})$ -formula that defines multiplication of numbers of size up to  $N$ . Hence, the proof sketch for part (f) of Theorem 3.2 is complete. ■

It is easy to see that “ $<$ ” cannot be expressed using “ $\times$ ” alone, i.e.,

**$FO(\times) \subsetneq FO(<, \times)$  on initial segments of  $\mathbb{N}$  (and also on finite structures and on  $\mathbb{N}$ ).**

To see this, let  $\mathcal{A}$  be either the structure  $\langle \mathbb{N}, \times \rangle$  or some initial segment  $\langle \underline{N}, \times \rangle$ . For the sake of contradiction, assume that there is an  $FO(\times)$ -formula  $\varphi_{<}(x, y)$  expressing that  $a < b$ , for all interpretations  $a, b \in A$  of the variables  $x, y$ . The *isomorphism property* of  $FO(\times)$  thus implies, for every automorphism  $\pi$  of  $\mathcal{A}$ , that  $\pi(a) < \pi(b)$  iff  $a < b$ . Hence, the identity function on  $A$  is the only automorphism of  $\mathcal{A}$ .

The contradiction now follows from the fact that  $\langle \mathbb{N}, \times \rangle$  and also most initial segments  $\langle \underline{N}, \times \rangle$  do have automorphisms different from the identity function: indeed, over  $\mathbb{N}$ , the role of any two different prime numbers  $p$  and  $q$  is interchangeable. I.e., the following mapping  $\pi_{p \leftrightarrow q}$  is an automorphism of  $\langle \mathbb{N}, \times \rangle$ :  $\pi_{p \leftrightarrow q}$  is determined via  $\pi_{p \leftrightarrow q}(a \times b) = \pi_{p \leftrightarrow q}(a) \times \pi_{p \leftrightarrow q}(b)$  for all  $a, b \in \mathbb{N}_{>0}$ , and, for all prime numbers  $r$ ,

$$\pi_{p \leftrightarrow q}(r) := \begin{cases} q & \text{if } r = p \\ p & \text{if } r = q \\ r & \text{if } r \neq p, q \text{ is a prime.} \end{cases}$$

Moreover, if  $p$  and  $q$  are prime numbers  $> \frac{N}{2}$ , then  $\pi_{p \leftrightarrow q}$  can even be viewed as an automorphism of the initial segment  $\langle \underline{N}, \times \rangle$ . In fact,  $\pi_{p \leftrightarrow q}$  leaves all elements in  $\underline{N}$  fixed except for  $p$  and  $q$ . For example,  $\pi_{2 \leftrightarrow 3}$  is an automorphism of  $\langle \underline{3}, \times \rangle$ , and  $\pi_{5 \leftrightarrow 7}$  is an automorphism of  $\langle \underline{8}, \times \rangle$ . Moreover, from results in number theory (cf., e.g., [Rose 1994, Problem 17 in Chapter 13]) we know that for any large enough  $N$  there are prime numbers  $p, q$  with  $\frac{N}{2} < p < q \leq N$ .

What we have seen is that there is no  $FO(\times)$ -formula  $\varphi_{<}(x, y)$  such that “ $\langle \underline{N}, \times \rangle \models \varphi_{<}(a, b)$  iff  $a < b$ ” is true for all  $N \in \mathbb{N}_{>0}$  and all  $a, b \in \underline{N}$ . It is remarkable, however, that “ $<$ ” is indeed  $FO(\times)$ -definable on numbers of size up to  $\sqrt{N}$ :

**LEMMA 3.3 [FOLKLORE].** *There is an  $FO(\times)$ -formula  $\varphi'_{<}(x, y)$  which defines “ $<$ ” on numbers of size up to  $\sqrt{N}$ . I.e., for all  $N \in \mathbb{N}_{>0}$  and all interpretations  $a, b \in \underline{N}$  of the variables  $x, y$ , we have  $\langle \underline{N}, \times \rangle \models \varphi'_{<}(a, b)$  iff  $a < b \leq \sqrt{N}$ .  $\square$*

**PROOF.** The  $FO(\times)$ -formula  $\varphi'_{<}(x, y)$  is defined via

$$\exists z \, x \times x = z \wedge \exists z \, y \times y = z \wedge \exists u \left( (\exists v \, x \times u = v) \wedge (\neg \exists v' \, y \times u = v') \right).$$

For the “only if” direction let  $a, b \in \underline{N}$  such that  $\langle \underline{N}, \times \rangle \models \varphi'_{<}(a, b)$ . Clearly, the first two conjunctions of  $\varphi'_{<}$  ensure that  $a, b \leq \sqrt{N}$ . The third conjunction ensures that there is some  $u \in \underline{N}$  such that  $a \times u \leq N$  and  $b \times u > N$ , and hence, in particular  $a < b$ .

For the “if” direction let  $a < b \leq \sqrt{N}$ . In particular,  $a \times a \leq N$  and  $b \times b \leq N$ , and hence the first two conjunctions of  $\varphi'_{<}$  are satisfied. Choose  $u \in \underline{N}$  maximal such that  $a \times u \leq N$ . In particular,  $u \geq a$ , and there is some  $r$  with  $0 \leq r < a \leq u$  such that  $N = a \times u + r$ . Since  $b \geq a + 1$  we thus have  $b \times u \geq (a + 1) \times u = a \times u + u > a \times u + r = N$ . Hence, also the third conjunction in  $\varphi'_{<}$  is satisfied.  $\blacksquare$

When considering an initial segment  $\underline{N}$ , the relations  $<, +, \times$ , *Bit* can a priori speak only about numbers of size at most  $N$ . This can be improved up to  $N^d$  (for any fixed  $d \in \mathbb{N}_{>0}$ ) by using  $(N+1)$ -ary representations of numbers: We use a  $d$ -tuple  $\vec{x} := (x_{d-1}, \dots, x_0) \in (\underline{N})^d$  to represent the number  $\sum_{i=0}^{d-1} x_i (N+1)^i$ . The following Theorem 3.4 shows that

**the  $d$ -tuple versions of  $<, +, \times$ , and *Bit*, respectively, are first-order definable on initial segments of  $\mathbb{N}$ .**

This fact has been observed and used in various places, e.g., [Harrow 1973; Atserias 1999].

**THEOREM 3.4 [FOLKLORE].** *For every  $d \in \mathbb{N}_{>0}$  there is*

- (a) *an  $FO(<)$ -formula  $\varphi_{<}^d(x_{d-1}, \dots, x_0, y_{d-1}, \dots, y_0)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\vec{x}, \vec{y} \in \underline{N}$  of the variables  $\vec{x}, \vec{y}$ , we have  $\langle \underline{N}, < \rangle \models \varphi_{<}^d(\vec{x}, \vec{y})$  iff  $\sum_{i=0}^{d-1} x_i (N+1)^i < \sum_{i=0}^{d-1} y_i (N+1)^i$ .*
- (b) *an  $FO(+)$ -formula  $\varphi_+^d(x_{d-1}, \dots, x_0, y_{d-1}, \dots, y_0, z_d, \dots, z_0)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\vec{x}, \vec{y}, \vec{z} \in \underline{N}$  of the variables  $\vec{x}, \vec{y}, \vec{z}$ , we have  $\langle \underline{N}, <, + \rangle \models \varphi_+^d(\vec{x}, \vec{y}, \vec{z})$  iff  $\sum_{i=0}^{d-1} x_i (N+1)^i + \sum_{i=0}^{d-1} y_i (N+1)^i = \sum_{i=0}^d z_i (N+1)^i$ .*
- (c) *for every fixed  $n \in \mathbb{N}_{>0}$ , an  $FO(+)$ -formula  $\varphi_{\equiv_n}^d(x_{d-1}, \dots, x_0, y_{d-1}, \dots, y_0)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\vec{x}, \vec{y} \in \underline{N}$  of the variables  $\vec{x}, \vec{y}$ , we have  $\langle \underline{N}, <, + \rangle \models \varphi_{\equiv_n}^d(\vec{x}, \vec{y})$  iff  $\sum_{i=0}^{d-1} x_i (N+1)^i \equiv_n \sum_{i=0}^{d-1} y_i (N+1)^i$ .*
- (d) *an  $FO(+, \times)$ -formula  $\varphi_{\times}^d(x_{d-1}, \dots, x_0, y_{d-1}, \dots, y_0, z_{2d-1}, \dots, z_0)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\vec{x}, \vec{y}, \vec{z} \in \underline{N}$  of the variables  $\vec{x}, \vec{y}, \vec{z}$ , we have  $\langle \underline{N}, +, \times \rangle \models \varphi_{\times}^d(\vec{x}, \vec{y}, \vec{z})$  iff  $\sum_{i=0}^{d-1} x_i (N+1)^i \times \sum_{i=0}^{d-1} y_i (N+1)^i = \sum_{i=0}^{2d-1} z_i (N+1)^i$ .*
- (e) *an  $FO(\text{Bit})$ -formula  $\varphi_{\text{Bit}}^d(x_{d-1}, \dots, x_0, y)$ , such that for every  $N \in \mathbb{N}_{>0}$  and all assignments  $\vec{x}, y \in \underline{N}$  of the variables  $\vec{x}, y$ , we have  $\langle \underline{N}, \text{Bit} \rangle \models \varphi_{\text{Bit}}^d(\vec{x}, y)$  iff the  $y$ -th bit in the binary representation of  $\sum_{i=0}^{d-1} x_i (N+1)^i$  is 1.  $\square$*

The proof of Theorem 3.4 is straightforward but tedious. For the sake of completeness — since the author does not know references that contain complete proofs of all parts of this theorem — a proof is given in the appendix.

### 3.3 Counting vs. Arithmetic on Finite Structures

There is a close connection between arithmetic on finite structures and circuit complexity. A concise overview of circuit complexity can be found in [Allender 1996]. The complexity class  $AC^0$  consists of all problems solvable by polynomial size, constant depth circuits of AND, OR, and NOT gates of unbounded fan-in. It was shown in [Barrington et al. 1990] that, for ordered structures over arbitrary signatures  $\tau$ , logtime-uniform  $AC^0$  is exactly the class of all problems definable in  $FO(+, \times, \tau)$ . It is a deep result of [Ajtai 1983; Furst et al. 1984] that

$$\text{PARITY} := \{ \langle \underline{N}, <, \mathbf{Y} \rangle : N \in \mathbb{N}_{>0}, \mathbf{Y} \subseteq \underline{N}, |\mathbf{Y}| \text{ is even} \}$$

does not belong to  $AC^0$ , and hence is not definable in  $FO(+, \times, Y)$ . This is known even for non-uniform  $AC^0$ , which translates to  $FO(\mathfrak{Arb}, Y)$ , where  $\mathfrak{Arb}$  is the collection of *arbitrary*, i.e. all, built-in predicates on initial segments of  $\mathbb{N}$ . From [Fagin et al. 1985; Denenberg et al. 1986] we also know that, for any  $\varepsilon > 0$ ,  $FO(\mathfrak{Arb}, Y)$  cannot count cardinalities of sets up to size  $N^\varepsilon$ :

**THEOREM 3.5** [ $FO(\mathfrak{Arb})$  CANNOT COUNT ON FINITE STRUCTURES].

Let  $\varepsilon > 0$ . There is no  $FO(\mathfrak{Arb}, Y)$ -formula  $\chi_\#(x, Y)$  such that

$$\langle \underline{N}, \mathfrak{Arb}, \mathbf{x}, \mathbf{Y} \rangle \models \chi_\#(x, Y) \text{ iff } x = |\mathbf{Y}| \leq N^\varepsilon$$

is true for all  $N \in \mathbb{N}_{>0}$ , all  $\mathbf{Y} \subseteq \underline{N}$ , and all  $\mathbf{x} \in \underline{N}$ . □

However, it was shown in [Fagin et al. 1985; Denenberg et al. 1986; Ajtai and Ben-Or 1984] that, for any  $c \in \mathbb{N}_{>0}$ ,  $FO(+, \times, Y)$  can indeed count cardinalities of sets up to size  $(\lg N)^c$ :

**THEOREM 3.6** [POLYLOG COUNTING CAPABILITY OF  $FO(+, \times)$ ].

For every  $c \in \mathbb{N}_{>0}$  there is an  $FO(+, \times, Y)$ -formula  $\chi_\#^c(x, Y)$  such that

$$\langle \underline{N}, +, \times, \mathbf{x}, \mathbf{Y} \rangle \models \chi_\#^c(x, Y) \text{ iff } x = |\mathbf{Y}| \leq (\lg N)^c$$

is true for all  $N \in \mathbb{N}_{>0}$ , all  $\mathbf{Y} \subseteq \underline{N}$ , and all  $\mathbf{x} \in \underline{N}$ . □

A self-contained, purely logical proof of this theorem can be found in [Durand et al. 1998].

### 3.4 Counting vs. Pure Arithmetic on Initial Segments of $\mathbb{N}$

There is a direct correspondence between *pure arithmetic*  $FO(+, \times)$  on initial segments of  $\mathbb{N}$  and *bounded arithmetic*  $\Delta_0$  on  $\mathbb{N}$ . The class  $\Delta_0$  is defined as the set of all  $FO(+, \times)$ -formulas in which quantified variables are bounded by other variables via  $\exists x (x \leq y \wedge \dots)$ . The  $\Delta_0$ -definable relations in  $\mathbb{N}$  are called the *rudimentary relations*. An overview of this line of research can be found in [Esbelin and More 1998], where it is also pointed out that there is a precise correspondence between

1. the  $FO(+, \times)$ -definable spectra (the *spectrum* of an  $FO(+, \times)$ -sentence  $\varphi$  is the set of all  $N \in \mathbb{N}_{>0}$  such that  $\langle \underline{N}, +, \times \rangle \models \varphi$ ),

2. the unary rudimentary relations,
3. the linear time hierarchy  $LINH$ , and
4. the string languages definable in monadic second order logic  $MSO(+)$ .

Researchers concerned with rudimentary relations have developed clever encoding techniques that expose the expressive power of bounded arithmetic. For example, the exponentiation relation  $x=y^z$  was proved to be rudimentary (and hence  $FO(+, \times)$ -definable on initial segments of  $\mathbb{N}$ ) already in [Bennett 1962]. Furthermore, Theorem 3.4 corresponds to Harrow's result [Harrow 1973] that, for expressing rudimentary relations, one may make use of polynomially bounded quantification such as  $\exists x (x \leq y^d \wedge \dots)$ . Esbelin and More [Esbelin and More 1998] developed a toolbox that allows to express certain primitive recursive functions by  $\Delta_0$ -formulas.

On the other hand, hardly any tools are known which enable us to prove that some relation is *not* rudimentary. According to [Esbelin and More 1998; Paris and Wilkie 1986] it is still open whether the rudimentary relations are closed under counting. Translated into the setting used in the present paper, this corresponds to the following:

**QUESTION 3.7.** *Is there, for every  $FO(+, \times)$ -formula  $\varphi(y, \vec{z})$ , an  $FO(+, \times)$ -formula  $\chi(x, \vec{z})$  such that*

$$\langle \underline{N}, +, \times \rangle \models \chi(\mathbf{x}, \vec{\mathbf{z}}) \text{ iff } \mathbf{x} = |\mathbf{Y}_{(N, \varphi, \vec{z})}|$$

*is true for all  $N \in \mathbb{N}_{>0}$ , for all  $\mathbf{x}, \vec{\mathbf{z}} \in \underline{N}$ , and for the set  $\mathbf{Y}_{(N, \varphi, \vec{z})} := \{\mathbf{y} \in \underline{N} : \langle \underline{N}, +, \times \rangle \models \varphi(\mathbf{y}, \vec{\mathbf{z}})\}$ .*  $\square$

Note that the non-counting capability formulated in Theorem 3.5 does *not* imply a negative answer to the above question: In the highly involved proofs of [Fagin et al. 1985; Denenberg et al. 1986] it is essentially used that there are lots of different possible interpretations of the set  $Y$ , whereas in Question 3.7 the set  $Y$  is defined by an  $FO(+, \times)$ -formula and has thus exactly *one* interpretation.

In fact, in [Paris and Wilkie 1986] it was shown that the following *approximate* counting is indeed possible for rudimentary relations: For every  $\varepsilon > 0$  and every  $FO(+, \times)$ -formula  $\varphi(y, \vec{z})$  there is an  $FO(+, \times)$ -formula  $\chi(x, \vec{z})$  such that the following is true for every  $N \in \mathbb{N}_{>0}$  and all  $\vec{\mathbf{z}} \in \underline{N}$ :

$$\begin{aligned} &\text{there is exactly one } \mathbf{x} \in \underline{N} \text{ with } \langle \underline{N}, +, \times \rangle \models \chi(\mathbf{x}, \vec{\mathbf{z}}), \text{ and} \\ &\text{for this } \mathbf{x} \text{ we have } |\mathbf{Y}_{(N, \varphi, \vec{z})}| \leq \mathbf{x} < |\mathbf{Y}_{(N, \varphi, \vec{z})}|^{1+\varepsilon}. \end{aligned}$$

[Paris and Wilkie 1986] conjecture that Question 3.7 has a negative answer (without giving any evidence, except for the fact that known techniques do not enable us to give a positive answer). Let us remark, however, that a negative answer would have the serious complexity theoretic consequence that  $LINH \neq ETIME$ , where  $ETIME$  denotes the class of all problems solvable on a deterministic Turing machine in linear exponential time  $2^{O(n)}$ . This can be seen as follows: a negative answer to Question 3.7 would imply that  $FO(+, \times)$  is strictly less expressive than *least fixed point logic*  $LFP(+, \times)$  on initial segments of  $\mathbb{N}$ . However, it has been mentioned in [Atserias and Kolaitis 1999] and proved in [Atserias 1999, Theorem 14] that  $FO(+, \times) \neq LFP(+, \times)$  on initial segments of  $\mathbb{N}$  if, and only if,  $LINH \neq ETIME$ . The efforts to separate  $FO$  from  $LFP$  on various kinds of ordered structures are subsumed under the keyword *the Ordered Conjecture*. An overview of what

is known about this conjecture can be found in [Atserias and Kolaitis 1999].

In the subsequent sections of this paper we consider the expressive power of the logic one obtains by extending first-order logic with the ability to count. In Section 5 we will give a positive answer to the analogue of Question 3.7 which speaks about  $FO(+)$  rather than  $FO(+, \times)$ .

#### 4. FIRST-ORDER LOGIC WITH COUNTING QUANTIFIERS

In this section we fix the syntax and semantics of first-order logic with counting quantifiers, and we summarize some important properties of this logic. In particular, we show that on Skolem arithmetic  $(\mathbb{N}, \times)$  and its initial segments it fails to have the isomorphism property.

##### 4.1 Syntax and Semantics

First-order logic with *unary* counting quantifiers,  $FOunC$ , is the extension of first-order logic obtained by adding unary counting quantifiers of the form  $\exists^{=x}y$ . For an interpretation  $\mathbf{x}$  of the variable  $x$ , a formula  $\exists^{=x}y \varphi(y)$  expresses that there are exactly  $x$  many different interpretations  $\mathbf{y}$  of the variable  $y$  such that the formula  $\varphi(y)$  is satisfied.

Accordingly, for  $k \in \mathbb{N}_{>0}$ , first-order logic with *k-ary* counting quantifiers,  $FOk\text{-ary}C$ , is the extension of first-order logic obtained by adding *k-ary* counting quantifiers of the form  $\exists^{=x_1, \dots, x_k}y_1, \dots, y_k$ , which allow to count the number of interpretations of *k*-tuples  $(y_1, \dots, y_k)$  of variables.

To be precise: Let  $k \in \mathbb{N}_{>0}$ , and let  $\tau$  be a signature. The class of  $FOk\text{-ary}C(\tau)$ -formulas is obtained by the extension of the calculus for  $FO(\tau)$  via the following rule:

If  $\varphi$  is an  $FOk\text{-ary}C(\tau)$ -formula and  $x_1, \dots, x_k$  and  $y_1, \dots, y_k$  are distinct variables, then  $\exists^{=x_1, \dots, x_k}y_1, \dots, y_k \varphi$  is an  $FOk\text{-ary}C(\tau)$ -formula.

The variables  $y_1, \dots, y_k$  are bound by this quantifier, whereas the variables  $x_1, \dots, x_k$  remain free, i.e.,  $free(\exists^{=\vec{x}}\vec{y} \varphi) = \{\vec{x}\} \cup (free(\varphi) \setminus \{\vec{y}\})$ .

We will evaluate  $FOk\text{-ary}C(\tau)$ -formulas only in structures whose universe is  $\mathbb{Z}$ ,  $\mathbb{N}$ , or some initial segment of  $\mathbb{N}$ . For such a structure  $\mathcal{A}$ , the semantics of an  $FOk\text{-ary}C(\tau)$ -formula of the form  $\exists^{=\vec{x}}\vec{y} \varphi(\vec{x}, \vec{y}, \vec{z})$  is defined as follows<sup>1</sup>: for interpretations  $\vec{x}, \vec{z} \in A$  of the variables  $\vec{x}, \vec{z}$  we have

$$\langle \mathcal{A}, \vec{x}, \vec{z} \rangle \models \exists^{=\vec{x}}\vec{y} \varphi(\vec{x}, \vec{y}, \vec{z}) \quad \text{if, and only if,}$$

$$\sum_{i=1}^k \mathbf{x}_i \cdot |A|^{k-i} = |\{(\vec{y}) \in A^k : \langle \mathcal{A}, \vec{x}, \vec{y}, \vec{z} \rangle \models \varphi(\vec{x}, \vec{y}, \vec{z})\}|.$$

For *infinite*  $A$  this in particular implies that  $x_k$  is the only variable in  $\vec{x}$  which may be interpreted by a number different from 0. For finite  $A = \underline{N}$ , the formula  $\exists^{=\vec{x}}\vec{y} \varphi$  expresses that that the *k*-tuple  $\vec{x}$  is the  $(N+1)$ -ary representation of the number of *k*-tuples  $\vec{y}$  which satisfy  $\varphi$ .

To denote first-order logic with unary and binary counting quantifiers, respectively, we write  $FOunC$  and  $FObinC$  instead of  $FO1\text{-ary}C$  and  $FO2\text{-ary}C$ .

<sup>1</sup>Recall that  $\varphi(\vec{x}, \vec{y}, \vec{z})$  indicates that  $free(\varphi) \subseteq \{\vec{x}, \vec{y}, \vec{z}\}$ , i.e., it is *not* required that all the variables do indeed occur free in  $\varphi$ .

## 4.2 The Isomorphism Property

For any reasonable logical system one requires it to have the *isomorphism property*. In the present setting this means that the evaluation of an  $FOk\text{-aryC}(\tau)$ -formula  $\varphi(\vec{x})$  makes sense only for  $\tau$ -structures  $\mathcal{A}$  with universe  $\mathbb{Z}$ ,  $\mathbb{N}$ , or  $\underline{N}$  (for some  $N \in \mathbb{N}$ ), that have the following property

(\*) : If  $\pi$  is an automorphism of  $\mathcal{A}$  and  $\vec{a} \in A$  is an interpretation of the variables  $\vec{x}$ , then  $\mathcal{A} \models \varphi(\vec{a})$  iff  $\mathcal{A} \models \varphi(\pi(\vec{a}))$ .

This property is, of course, true for *rigid* structures, i.e., for structures which have no automorphisms except for the identity function. In particular, structures with a discrete linear ordering, such as  $\langle \mathbb{Z}, < \rangle$ ,  $\langle \mathbb{N}, < \rangle$ ,  $\langle \underline{N}, < \rangle$ , and their extensions, are rigid. Therefore, it does make sense to study the expressive power of  $FOk\text{-aryC}$ -formulas on those structures.

But what about *Skolem arithmetic*  $\langle \mathbb{N}, \times \rangle$  and its initial segments  $\langle \underline{N}, \times \rangle$ ? In Section 3 we have already seen that these structures are not rigid. There, we have observed that the mapping  $\pi_{p \leftrightarrow q}$  (which interchanges the prime numbers  $p$  and  $q$  and which leaves fixed all other prime numbers), is an automorphism of  $\langle \mathbb{N}, \times \rangle$ , and, as soon as  $p, q > \frac{N}{2}$ , even an automorphism of  $\langle \underline{N}, \times \rangle$ . However, the non-rigidness does not necessarily imply that  $FOk\text{-aryC}$  does not have the isomorphism property on these structures. Nevertheless, for any  $k \in \mathbb{N}_{>0}$ ,  $FOk\text{-aryC}(\times)$  does indeed neither have the isomorphism property on  $\langle \mathbb{N}, \times \rangle$  nor on the class of initial segments of  $\langle \mathbb{N}, \times \rangle$ :

PROPOSITION 4.1.

- (a)  $FOunC(\times)$  does not have the isomorphism property on  $\langle \mathbb{N}, \times \rangle$ .  
 (b)  $FOunC(\times)$  does not have the isomorphism property on  $\{\langle \underline{N}, \times \rangle : N \in \mathbb{N}_{>0}\}$ .  $\square$

PROOF. (a): The failure of the isomorphism property of  $FOunC(\times)$  on  $\langle \mathbb{N}, \times \rangle$  is a direct consequence of the fact that  $<$  is  $FOunC(\times)$ -definable on  $\mathbb{N}$ . I.e., there is an  $FOunC(\times)$ -formula  $\varphi_{<}(x, y)$  such that “ $\langle \mathbb{N}, \times \rangle \models \varphi_{<}(a, b)$  iff  $a < b$ ” is true for all  $a, b \in \mathbb{N}$ . For the construction of the formula  $\varphi_{<}(x, y)$  note that  $x < y$  is true if and only if  $x \neq y$  and there are a prime number  $p$  and  $p$ -powers  $u$  and  $v$  such that  $u = p^x$ ,  $v = p^y$ , and  $u \mid v$ . Furthermore,

- “ $u \mid v$ ” can be expressed in  $FO(\times)$  via “ $\exists w (u \times w = v)$ ”,
- “ $p$  is a prime number” can be expressed in  $FO(\times)$  via “ $p \neq 1 \wedge \forall w (w \mid p) \rightarrow (w = 1 \vee w = p)$ ”,
- “ $u$  is a power of the prime number  $p$ ” can be expressed in  $FO(\times)$  via “ $p$  is a prime number  $\wedge \forall q (q \mid u \wedge q \text{ is a prime number}) \rightarrow q = p$ ”,
- “ $u = p^x$ ” can be expressed in  $FOunC(\times)$  via “ $u$  is a power of the prime number  $p \wedge \exists^{=x} w (w \neq u \wedge w \mid u)$ ”.

Altogether, this gives us the desired  $FOunC(\times)$ -formula  $\varphi_{<}(x, y)$ .

To see that the isomorphism property (\*) is not satisfied, let  $p, q$  be prime numbers with  $p < q$ , and let  $\pi := \pi_{p \leftrightarrow q}$  be the automorphism of  $\langle \mathbb{N}, \times \rangle$  which interchanges  $p$  and  $q$ . Clearly, we have  $\langle \mathbb{N}, \times \rangle \models \varphi_{<}(p, q)$ , but  $\langle \mathbb{N}, \times \rangle \not\models \varphi_{<}(\pi(p), \pi(q))$ .

(b): Note that the formula  $\varphi_{<}(x, y)$  of part (a) is of no use here, because it gives us “<” only for numbers of size up to  $\lg N$  when  $\underline{N}$  is the underlying universe — and from Lemma 3.3 we know that “<” is  $FO(\times)$ -definable even for numbers of size up to  $\sqrt{N}$ . However, the failure of the isomorphism property of the logic  $FOunC(\times)$  on the class  $\{\langle \underline{N}, \times \rangle : N \in \mathbb{N}_{>0}\}$  can be obtained as follows: Consider the  $FOunC(\times)$ -formula

$$\psi(x) := \exists^{=x} y \neg(y \text{ is a prime number}).$$

Of course we have, for all  $N \in \mathbb{N}_{>0}$  and all interpretations  $a \in \underline{N}$  of the variable  $x$ , that  $\langle \underline{N}, \times \rangle \models \psi(a)$  iff  $a = |\{b \in \underline{N} : b \text{ is not a prime number}\}|$ .

However, for  $N := 8$  and  $p := 5$  and  $q := 7$ , the mapping  $\pi := \pi_{p \leftrightarrow q}$  is an automorphism of  $\langle \underline{N}, \times \rangle$ , for which the property (\*) describing the isomorphism property is not satisfied: The set of non-prime numbers in  $\underline{N}$  is  $\{0, 1, 4, 6, 8\}$ . This set has cardinality  $p=5$ , and thus we have  $\langle \underline{N}, \times \rangle \models \psi(p)$ , but  $\langle \underline{N}, \times \rangle \not\models \psi(\pi_{p \leftrightarrow q}(p))$ .

Let us mention that from the *Prime Number Theorem* (cf., e.g., [Rose 1994]) it follows that for any  $N_0$  there are a  $N \geq N_0$  and two different prime numbers  $p, q$  with  $\frac{N}{2} < p, q \leq N$  such that  $\langle \underline{N}, \times \rangle \models \psi(p)$ , but  $\langle \underline{N}, \times \rangle \not\models \psi(\pi_{p \leftrightarrow q}(p))$ . I.e., the isomorphism property of  $FOunC(\times)$  cannot be obtained by restricting considerations to initial segments that are “large enough”. ■

### 4.3 Easy Facts and Known Results

For the rest of this paper we will concentrate on first-order logic with counting quantifiers on rigid structures such as  $\langle \underline{N}, < \rangle$  and  $\langle \underline{N}, + \rangle$ . It is obvious that

**+ is definable in  $FOunC(<)$   
on initial segments of  $\mathbb{N}$ , on finite structures, and on  $\mathbb{N}$ ,**

via the formula  $\varphi_+(x, y, z) := \exists^{=y} u (x < u \leq z)$ . Furthermore,

**$\times$  is definable in  $FObinC(<)$   
on initial segments of  $\mathbb{N}$ , on finite structures, and on  $\mathbb{N}$ ,**

via the formula  $\varphi_\times(x, y, z) := \exists^{=0,z} u, v (1 \leq u \leq x \wedge 1 \leq v \leq y)$ . This is true because

$$x \times y = \sum_{u=1}^x y = \sum_{u=1}^x \sum_{v=1}^y 1 = |\{(u, v) : 1 \leq u \leq x \wedge 1 \leq v \leq y\}|.$$

It is not difficult to see the following:

PROPOSITION 4.2. For all  $k \in \mathbb{N}_{>0}$ ,  $FOk\text{-ary}C(+, \times) = FO(+, \times)$  on  $\mathbb{N}$ . □

PROOF. We encode a finite set  $Y$  by the unique number  $u$  which satisfies, for all  $y \in \mathbb{N}$ , that  $Bit(u, y)$  iff  $y \in Y$ . The  $FO(+, \times)$ -formula  $\varphi_{Bit}(u, y)$  from Theorem 3.2 hence expresses that  $y$  belongs to the set encoded by  $u$ . Furthermore, from the counting capability of Theorem 3.6 we obtain an  $FO(+, \times)$ -formula  $\varphi_{BITSUM}(x, u)$  expressing that  $x$  is the number of  $y \in \mathbb{N}$  which satisfy  $Bit(u, y)$ . I.e.,  $\varphi_{BITSUM}(x, u)$  expresses that  $x$  is the cardinality of the set encoded by  $u$ . Now, a given  $FOunC(+, \times)$ -formula  $\exists^{=x} y \psi(x, y, \vec{z})$  is equivalent over  $\mathbb{N}$  to the  $FO(+, \times)$ -formula

$$\exists u \left( \varphi_{BITSUM}(x, u) \wedge \forall y (\varphi_{Bit}(u, y) \leftrightarrow \psi(x, y, \vec{z})) \right).$$

Here,  $u$  encodes the set of all  $y$  satisfying  $\psi$ .

For a given  $FOk\text{-ary}C(+, \times)$ -formula it hence suffices to find an equivalent formula in  $FOunC(+, \times)$ .

We encode a tuple  $(y_1, \dots, y_k) \in \mathbb{N}^k$  by the single number  $v = p_1^{y_1} \dots p_k^{y_k}$ , where  $p_i$  denotes the  $i$ -th largest prime number (for  $i \in \{1, \dots, k\}$ ). A given  $FOk\text{-ary}C(+, \times)$ -formula  $\exists^{=x_1 \dots x_k} y_1, \dots, y_k \psi(\vec{x}, \vec{y}, \vec{z})$  is thus equivalent over  $\mathbb{N}$  to an  $FOunC(+, \times)$ -formula which expresses that

$$x_1=0 \wedge \dots \wedge x_{k-1}=0 \wedge \exists^{=x_k} v (\exists y_1 \dots \exists y_k v = p_1^{y_1} \dots p_k^{y_k} \wedge \psi(\vec{x}, \vec{y}, \vec{z})).$$

This completes the proof of Proposition 4.2. ■

Note that the above proof does not work for initial segments of  $\mathbb{N}$ , because the number  $u$  which encodes a finite set  $Y$  is exponentially larger than the elements of  $Y$ . Indeed, it is still open whether  $FO(+, \times) = FOunC(+, \times)$  on initial segments of  $\mathbb{N}$ . However, from Theorem 3.5 we know that  $FO(+, \times) \neq FOunC(+, \times)$  on finite structures.

It was shown in [Barrington et al. 1990] that, for ordered finite structures over arbitrary signatures  $\tau$ , the class of problems definable in  $FOunC(+, \times, \tau)$  is exactly the (logtime-uniform version of the) circuit complexity class  $TC^0$ .<sup>2</sup> I.e.,

$$FOunC(+, \times) = TC^0 \text{ on finite structures.}$$

It is a deep result, following from [Barrington et al. 1990], that for all  $k \in \mathbb{N}_{>0}$ ,

$$FOk\text{-ary}C(+, \times) = FOunC(+, \times) \\ \text{on finite structures and on initial segments of } \mathbb{N}.$$

Actually, in Proposition 10.3 of [Barrington et al. 1990] it is shown that a *binary counting quantifier* can be expressed using *unary majority quantifiers* and the *Bit* predicate. Here, a unary majority quantifier  $My \varphi(y)$  expresses that more than half of the interpretations of  $y$  do satisfy  $\varphi(y)$ . The proof of [Barrington et al. 1990] easily generalizes from *binary* to *k-ary* counting quantifiers, leading to the result that  $FOk\text{-ary}C(+, \times) = FOunC(+, \times) = FOunM(<, Bit) = TC^0$ . (Note that the unary majority quantifier  $My \varphi(y)$  can easily be expressed using unary counting via  $\exists u \exists v u > v \wedge \exists^{=u} y \varphi(y) \wedge \exists^{=v} y \neg \varphi(y)$ .)

Since  $+$  and  $\times$  are definable in  $FObinC(<)$ , it follows that for every  $k \geq 2$ ,

$$FOk\text{-ary}C(<) = FOk\text{-ary}C(+) = FOk\text{-ary}C(+, \times) \\ \text{on initial segments of } \mathbb{N}, \text{ on finite structures and on } \mathbb{N}.$$

Barrington, Immerman, and Straubing [Barrington et al. 1990] also gave a logical characterization of the class  $TC^0$  which does not need the *Bit* predicate, i.e., which does not need  $+$  and  $\times$ : They proved that  $TC^0 = FObinM(<)$  on finite structures. Here,  $FObinM$  is the extension of first-order logic obtained by adding *binary majority quantifiers* of the form  $Mx, y \varphi(x, y)$ , expressing that more than half of the interpretations of  $(x, y)$  do satisfy  $\varphi(x, y)$ .

<sup>2</sup>By definition, the class  $TC^0$  (in the literature sometimes also denoted  $ThC^0$ ) consists of all problems solvable by uniform polynomial size, constant depth circuits of AND, OR, NOT, and THRESHOLD gates of unbounded fan-in.

In [Lautemann et al. 2001, Corollary 4.4] it was shown that  $FOunM(<) \subsetneq FObinM(<)$  on finite structures. Although formulated in the terminology of certain *groupoidal Lindström quantifiers*, their proof basically shows the following: for *pure* arithmetic on initial segments of  $\mathbb{N}$ , all  $FOunM(<)$ -definable spectra are also definable in  $FO(<, +)$ .

Concerning the power of  $FO(<, +)$  for *pure* arithmetic, the main result of the following section goes one step further: in Theorem 5.4, Corollary 5.10, and Corollary 5.11 we will show that

$$FO(<, +) = FOUNC(<, +) \text{ on } \mathbb{Z}, \text{ on } \mathbb{N}, \text{ and on initial segments of } \mathbb{N}.$$

Altogether, we now have a detailed picture of the expressive power of first-order logic with counting quantifiers and arithmetic. This picture is visualized in Figure 4 and Figure 5 at the end of this paper.

## 5. PRESBURGER ARITHMETIC IS CLOSED UNDER UNARY COUNTING QUANTIFIERS

In this section we show that  $FOunC(<, +) = FO(<, +)$  on initial segments of  $\mathbb{N}$ , on  $\mathbb{N}$ , and on  $\mathbb{Z}$ . An important tool for our proof will be *Presburger's quantifier elimination* [Presburger 1930] which states the following:

Every  $FO(<, +)$ -formula  $\varphi(\vec{x})$  is equivalent over  $\mathbb{Z}$  to a Boolean combination of atoms of the form  $t = t'$ ,  $t < t'$ , and  $t \equiv_n t'$ , where<sup>3</sup>  $t$  and  $t'$  are terms built from the constants 0 and 1, the variables  $\vec{x}$ , and the addition function  $f_+$ . Essentially this means that  $FO(<, +)$  over  $\mathbb{Z}$  can express equality, inequality, and residue classes of terms — and nothing else! A well-presented proof of Presburger's quantifier elimination can be found, e.g., in the textbook [Smoryński 1991, Chapter III.4].

### 5.1 Basic Facts Concerning Presburger Arithmetic

We define the *Presburger signature*  $\mathfrak{Presb}$  to consist of all predicates needed for Presburger's quantifier elimination. I.e.,  $\mathfrak{Presb} := \{0, 1, f_+, <, (\equiv_n)_{n \in \mathbb{N}_{>0}}\}$  consists of constant symbols 0 and 1, a binary function symbol  $f_+$ , a binary relation symbol  $<$ , and binary relation symbols  $\equiv_n$ , for every  $n \in \mathbb{N}_{>0}$ . When considered over the universe  $\mathbb{Z}$  or  $\mathbb{N}$ , these symbols are always interpreted in the natural way via the numbers 0 and 1, the addition function, the linear ordering, and the congruence relation modulo  $n$ . It should be obvious that these predicates are  $FO(+)$ -definable in  $\langle \mathbb{N}, + \rangle$  and  $FO(<, +)$ -definable<sup>4</sup> in  $\langle \mathbb{Z}, <, + \rangle$ . Speaking about *Presburger arithmetic*, we therefore refer to any of the structures  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ ,  $\langle \mathbb{Z}, <, + \rangle$ ,  $\langle \mathbb{N}, \mathfrak{Presb} \rangle$ ,  $\langle \mathbb{N}, + \rangle$ .

From Presburger's quantifier elimination we know that the structure  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  has quantifier elimination. I.e., every  $FO(\mathfrak{Presb})$ -formula is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to a Boolean combination of atomic  $\mathfrak{Presb}$ -formulas. Moreover, in this Boolean combination of atoms, the negation  $\neg$  is not needed, because

- $\neg t_1 = t_2$  can be replaced by  $t_1 < t_2 \vee t_2 < t_1$ ,
- $\neg t_1 < t_2$  can be replaced by  $t_1 = t_2 \vee t_2 < t_1$ , and
- $\neg t_1 \equiv_n t_2$  can be replaced by  $t_1 \equiv_n t_2 + 1 \vee t_1 \equiv_n t_2 + 1 + 1 \vee \dots \vee t_1 \equiv_n t_2 + (n-1) \cdot 1$ .

<sup>3</sup>Recall that  $\equiv_n$  denotes the congruence relation modulo  $n$ .

<sup>4</sup>Note that  $+$  alone is not sufficient here, because the order relation " $<$ " (respectively, the unary relation " $>0$ ") are not  $FO(+)$ -definable in  $\langle \mathbb{Z}, + \rangle$ .

Hence Presburger's quantifier elimination can be formulated as follows:

**THEOREM 5.1 [PRESBURGER'S QUANTIFIER ELIMINATION].** *Every FO( $\mathfrak{Presb}$ )-formula  $\varphi(\vec{z})$  is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z})$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{\vec{z}\}$ .  $\square$*

In order to gain full understanding of Presburger arithmetic, let us have a look at what the  $\mathfrak{Presb}$ -atoms may express:

Let  $y$  and  $\vec{z} = z_1, \dots, z_\nu$  be distinct first-order variables. A  $\mathfrak{Presb}$ -atom  $\alpha(y, \vec{z})$  is built from the symbols in  $\{=\} \cup \{0, 1, f_+, <, \equiv_n : n \in \mathbb{N}_{>0}\} \cup \{y, \vec{z}\}$ . For better readability we will write  $+$  instead of  $f_+$ . I.e.,  $\alpha$  is of the form

$$(*) : \quad u_1 + \dots + u_k \times v_1 + \dots + v_l$$

where  $\times$  is an element in  $\{<, =, \equiv_n : n \in \mathbb{N}_{>0}\}$ , and  $u_1, \dots, u_k, v_1, \dots, v_l$  are (not necessarily distinct) elements in  $\{0, 1, y, \vec{z}\}$ .

Let  $m_1, m_y, m_{z_1}, \dots, m_{z_\nu}$  be the number of occurrences of the constant 1, the variable  $y$ , and the variables  $z_1, \dots, z_\nu$ , respectively, on the left side of  $(*)$ . Similarly, let  $n_1, n_y, n_{z_1}, \dots, n_{z_\nu}$  be the corresponding multiplicities for the right side of  $(*)$ . Interpreted in the structure  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ , the atom  $(*)$  expresses that

$$m_1 \cdot 1 + m_y \cdot y + \sum_{j=1}^{\nu} m_{z_j} \cdot z_j \times n_1 \cdot 1 + n_y \cdot y + \sum_{j=1}^{\nu} n_{z_j} \cdot z_j,$$

which is equivalent to  $(m_y - n_y) \cdot y \times (n_1 - m_1) \cdot 1 + \sum_{j=1}^{\nu} (n_{z_j} - m_{z_j}) \cdot z_j$ . I.e., there are  $c, d, k_1, \dots, k_\nu \in \mathbb{Z}$  such that  $(*)$  is equivalent to

$$(**) : \quad c \cdot y \times d + \sum_{j=1}^{\nu} k_j z_j.$$

In case  $c = 0$ ,  $(**)$  is equivalent to  $0 \times d + \sum_{j=1}^{\nu} k_j z_j$ . In case  $\times \in \{<, =\}$ ,  $(**)$  is equivalent to  $y \times \frac{1}{c} (d + \sum_{j=1}^{\nu} k_j z_j)$  if  $c > 0$ , and to  $\frac{1}{c} (d + \sum_{j=1}^{\nu} k_j z_j) \times y$  if  $c < 0$ . It remains to consider the case where  $c \neq 0$  and  $\times$  is a congruence relation  $\equiv_n$  for some  $n \in \mathbb{N}_{>0}$ . The following Lemma 5.2 shows that in this case there are  $d', k'_1, \dots, k'_\nu \in \mathbb{Z}$  and  $c', n' \in \mathbb{N}_{>0}$  such that  $(**)$  is equivalent to  $y \equiv_{n'} \frac{1}{c'} (d' + \sum_{j=1}^{\nu} k'_j z_j)$ .

**LEMMA 5.2.** *Let  $0 \neq c \in \mathbb{Z}$  and  $n \in \mathbb{N}_{>0}$ . Let  $g$  be the greatest common divisor of  $c$  and  $n$ , and let  $c' := \frac{c}{g}$  and  $n' := \frac{n}{g}$ . Since  $c'$  and  $n'$  are relatively prime there must exist a  $c'' \in \mathbb{N}_{>0}$  such that  $c' c'' \equiv_{n'} 1$ .*

*The following is true for all  $y, e \in \mathbb{Z}$ :  $cy \equiv_n e$  iff  $y \equiv_{n'} c'' \frac{e}{g}$ .  $\square$*

**PROOF.** Clearly,  $y \equiv_{n'} c'' \frac{e}{g}$  iff  $c' y \equiv_{n'} c' c'' \frac{e}{g}$  which, since  $c' c'' \equiv_{n'} 1$ , is equivalent to  $c' y \equiv_{n'} \frac{e}{g}$ . Furthermore,  $c' y \equiv_{n'} \frac{e}{g}$  iff there is a  $k \in \mathbb{Z}$  such that  $c' y = n' k + \frac{e}{g}$  iff  $gc' y = gn' k + e$  iff  $cy = nk + e$  iff  $cy \equiv_n e$ .  $\blacksquare$

To denote a fraction of the form  $\frac{1}{c} (d + \sum_{j=1}^{\nu} k_j z_j)$  with  $c, d, k_1, \dots, k_\nu \in \mathbb{Z}$  and  $c \neq 0$ , we will write  $t(\vec{z})$  for short, and we will call such fractions *generalized  $\mathfrak{Presb}$ -terms* over the variables  $\vec{z}$ . What we have just seen above is the following:

**FACT 5.3 [ $\mathfrak{Presb}$ -ATOMS].** *Let  $y$  and  $\vec{z} = z_1, \dots, z_\nu$  be distinct first-order variables. For every  $\mathfrak{Presb}$ -atom  $\alpha(y, \vec{z})$  there is a generalized  $\mathfrak{Presb}$ -term  $t(\vec{z})$  or a  $\mathfrak{Presb}$ -atom*

$\beta(\vec{z})$ , in which the variable  $y$  does not occur, such that  $\alpha(y, \vec{z})$  expresses over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  that

- $y > t(\vec{z})$  (lower bound on  $y$ ),
- $y < t(\vec{z})$  (upper bound on  $y$ ),
- $y \equiv_n t(\vec{z})$  (residue class of  $y$ , for an appropriate  $n \in \mathbb{N}_{>0}$ ),
- $y = t(\vec{z})$  (equation for  $y$ ), or
- $\beta(\vec{z})$  (independent of  $y$ ).

On the other hand, it is straightforward to see that for any  $\times \in \{>, <, =, \equiv_n : n \in \mathbb{N}_{>0}\}$  and any generalized  $\mathfrak{Presb}$ -term  $t(\vec{z})$ , the generalized atom  $y \times t(\vec{z})$  can be expressed by a quantifier free  $\text{FO}(\mathfrak{Presb})$ -formula. Similarly, for  $\times \in \{>, <, =\}$ , also the generalized atoms  $y \times \lceil t(\vec{z}) \rceil$  and  $y \times \lfloor t(\vec{z}) \rfloor$  can be expressed by quantifier free  $\text{FO}(\mathfrak{Presb})$ -formulas.  $\square$

## 5.2 $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ and Unary Counting Quantifiers

In this section we prove that Presburger’s quantifier elimination can be extended to unary counting quantifiers:

**THEOREM 5.4 [ELIMINATION OF UNARY COUNTING QUANTIFIERS].**

Every  $\text{FOunC}(\mathfrak{Presb})$ -formula  $\varphi(\vec{z})$  is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z})$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{\vec{z}\}$ .  $\square$

In particular, this means that  $\text{FOunC}(<, +) = \text{FO}(<, +)$  on  $\mathbb{Z}$ .

The proof of Theorem 5.4 will be given in a series of lemmas, the first (and most laborious to prove) is the following:

**LEMMA 5.5.** Every  $\text{FOunC}(\mathfrak{Presb})$ -formula of the form  $\exists^{=x} y \bigwedge_{j=1}^n \alpha_j(y, \vec{z})$ , where the  $\alpha_j$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{y, \vec{z}\}$ , is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to an  $\text{FO}(\mathfrak{Presb})$ -formula.  $\square$

Before proving Lemma 5.5 let us first look at an example that exposes all the relevant proof ideas.

**EXAMPLE 5.6.** Consider the formula  $\varphi(x, \vec{z}) :=$

$$\exists^{=x} y (z_2 + y < z_3 + y + y) \wedge (y < z_2) \wedge (y + y + y < z_1) \wedge (y + z_4 \equiv_4 z_3).$$

For interpretations  $x, \vec{z}$  in  $\mathbb{Z}$  of the variables  $x, \vec{z}$ , this formula expresses that there are exactly  $x$  many different  $y \in \mathbb{Z}$  which satisfy the constraints

$$(*) : \quad \underbrace{y > z_2 - z_3}_{\text{lower bound}}, \quad \underbrace{y < z_2, \quad y < \frac{z_1}{3}}_{\text{upper bound}}, \quad \text{and} \quad \underbrace{y \equiv_4 z_3 - z_4}_{\text{residue class}}.$$

We consider the integers  $\mathit{low} := z_2 - z_3$ ,  $\mathit{up} := \min\{z_2, \lceil \frac{z_1}{3} \rceil\}$ , and  $\mathit{first}$ , where  $\mathit{first}$  is the smallest integer  $> \mathit{low}$  which belongs to the correct residue class, i.e. which satisfies  $\mathit{first} \equiv_4 z_3 - z_4$ . The constraints  $(*)$  can be visualized as shown in Figure 1.

From Figure 1 one can directly see that there are exactly  $\max\left\{0, \left\lceil \frac{\mathit{up} - \mathit{first}}{4} \right\rceil\right\}$  many different  $y \in \mathbb{Z}$  which satisfy the constraints  $(*)$ . Hence, the statement “there are exactly

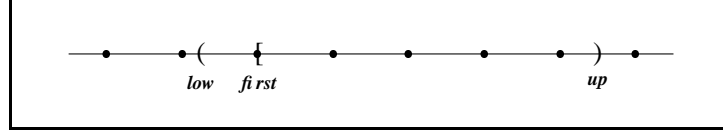


Fig. 1. Visualization of the constraints (\*). The black points are those which belong to the correct residue class; the black points in the interval  $[fi\ rst, up)$  are exactly those integers  $y$  which satisfy the constraints (\*).

$x$  many  $y \in \mathbb{Z}$  which satisfy the constraints (\*)” can be expressed by the  $FO(\mathfrak{Prsb})$ -formula  $\psi(x, \vec{z}) :=$

$$\begin{aligned} & \exists low \exists up \exists fi\ rst \\ & (low = z_2 - z_3) \wedge (up = z_2 \vee up = \lceil \frac{z_1}{3} \rceil) \wedge (up \leq z_2) \wedge (up \leq \lceil \frac{z_1}{3} \rceil) \wedge \\ & (fi\ rst > low) \wedge (fi\ rst \equiv_4 z_3 - z_4) \wedge (\forall v (v > low \wedge v \equiv_4 z_3 - z_4) \rightarrow v \geq fi\ rst) \wedge \\ & (up \leq fi\ rst \rightarrow x=0) \wedge (up > fi\ rst \rightarrow x = \lceil \frac{up - fi\ rst}{4} \rceil). \end{aligned}$$

Altogether, we have constructed an  $FO(\mathfrak{Prsb})$ -formula  $\psi(x, \vec{z})$  which is equivalent over  $\langle \mathbb{Z}, \mathfrak{Prsb} \rangle$  to the  $FOunC(\mathfrak{Prsb})$ -formula  $\varphi(x, \vec{z})$ .  $\square$

Using the ideas presented in Example 5.6, we are now ready for the formal proof of Lemma 5.5.

#### PROOF OF LEMMA 5.5.

Let  $\varphi(x, \vec{z}) := \exists^{=x} y \bigwedge_{j=1}^n \alpha_j(y, \vec{z})$  be the given formula, where the  $\alpha_j$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Prsb} \cup \{y, \vec{z}\}$ . Our aim is to construct an  $FO(\mathfrak{Prsb})$ -formula  $\psi(x, \vec{z})$  which is equivalent to  $\varphi(x, \vec{z})$  over  $\langle \mathbb{Z}, \mathfrak{Prsb} \rangle$ .

The atoms  $\alpha_1, \dots, \alpha_n$  impose constraints on  $y$ . According to Fact 5.3 we can partition the set of atoms  $\{\alpha_1, \dots, \alpha_n\}$  into

- a set  $L$  consisting of all atoms  $\alpha_j$  which express a *lower bound* of the form  $y > t_j(\vec{z})$ ,
- a set  $U$  consisting of all atoms  $\alpha_j$  which express an *upper bound* of the form  $y < t_j(\vec{z})$ ,
- a set  $R$  consisting of all atoms  $\alpha_j$  which express a *residue class* of the form  $y \equiv_{n_j} t_j(\vec{z})$ ,
- a set  $E$  consisting of all atoms  $\alpha_j$  which express an *equation* of the form  $y = t_j(\vec{z})$ ,
- a set  $I$  consisting of all atoms  $\alpha_j$  which are *independent* of  $y$ , i.e. which are equivalent over  $\langle \mathbb{Z}, \mathfrak{Prsb} \rangle$  to an atom  $\beta_j(\vec{z})$  in which the variable  $y$  does not occur.

For interpretations  $x, \vec{z}$  in  $\mathbb{Z}$  of the variables  $x, \vec{z}$ , the formula

$$\varphi(x, \vec{z}) := \exists^{=x} y \bigwedge_{j=1}^n \alpha_j(y, \vec{z})$$

expresses that there are exactly  $x$  many different  $y \in \mathbb{Z}$  which satisfy all the constraints (\*) in  $L, U, R, E$ , and  $I$ .

We first consider the easy case where  $E \neq \emptyset$ .

W.l.o.g.  $\alpha_1 \in E$ . This means that an  $y \in \mathbb{Z}$  which satisfies the constraints (\*) must in particular satisfy the constraint  $y = t_1(\vec{z})$ . Hence there is at most one  $y \in \mathbb{Z}$  (namely,  $y :=$

$t_1(\vec{z})$  that satisfies all the constraints (\*); and the formula  $\varphi(x, \vec{z}) := \exists^{=x} y \bigwedge_{j=1}^n \alpha_j(y, \vec{z})$  is equivalent to the  $FO(\mathfrak{Presb})$ -formula  $\psi(x, \vec{z}) :=$

$$\begin{aligned} & \left( x = 0 \vee x = 1 \right) \wedge \left( x = 1 \leftrightarrow \right. \\ & \quad \bigwedge_{j:\alpha_j \in L} t_1(\vec{z}) > t_j(\vec{z}) \wedge \bigwedge_{j:\alpha_j \in U} t_1(\vec{z}) < t_j(\vec{z}) \wedge \\ & \quad \left. \bigwedge_{j:\alpha_j \in R} t_1(\vec{z}) \equiv_{n_j} t_j(\vec{z}) \wedge \bigwedge_{j:\alpha_j \in E} t_1(\vec{z}) = t_j(\vec{z}) \wedge \bigwedge_{j:\alpha_j \in I} \beta_j(\vec{z}) \right). \end{aligned}$$

Let us now consider the case where  $E = \emptyset$ .

First of all, we simplify the constraints in  $L$ ,  $U$ , and  $R$ : If  $L \neq \emptyset$ , the constraints in  $L$  can be replaced by the single constraint  $y > low$ , where the variable  $low$  is enforced to be interpreted by the maximum lower bound on  $y$  via the  $FO(\mathfrak{Presb})$ -formula

$$\psi_{low}(low, \vec{z}) := \left( \bigvee_{j:\alpha_j \in L} low = \lfloor t_j(\vec{z}) \rfloor \right) \wedge \bigwedge_{j:\alpha_j \in L} low \geq \lfloor t_j(\vec{z}) \rfloor.$$

Similarly, if  $U \neq \emptyset$ , we can replace the constraints in  $U$  with the single constraint  $y < up$ , where the variable  $up$  is enforced to be interpreted by the minimum upper bound on  $y$  via the  $FO(\mathfrak{Presb})$ -formula

$$\psi_{up}(up, \vec{z}) := \left( \bigvee_{j:\alpha_j \in U} up = \lceil t_j(\vec{z}) \rceil \right) \wedge \bigwedge_{j:\alpha_j \in U} up \leq \lceil t_j(\vec{z}) \rceil.$$

W.l.o.g. we have  $R \neq \emptyset$ . (We can assume that  $R$  contains, e.g., the constraint  $y \equiv_1 0$  which is satisfied by all  $y \in \mathbb{Z}$ .)

We use the following fact to simplify the constraints in  $R$ .

**FACT 5.7.** *Let  $k > 0$ ,  $a_1, \dots, a_k \in \mathbb{Z}$ ,  $n_1, \dots, n_k \in \mathbb{N}_{>0}$ , and let  $l := \text{lcm}\{n_1, \dots, n_k\}$  be the least common multiple of  $n_1, \dots, n_k$ .*

*If there exists an  $r \in \{0, \dots, l-1\}$  such that  $(r \equiv_{n_1} a_1 \wedge \dots \wedge r \equiv_{n_k} a_k)$  then, for all  $b \in \mathbb{Z}$ , we have*

$$(b \equiv_{n_1} a_1 \wedge \dots \wedge b \equiv_{n_k} a_k) \quad \text{iff} \quad b \equiv_l r.$$

*If no such  $r$  exists, then no  $b \in \mathbb{Z}$  satisfies  $(b \equiv_{n_1} a_1 \wedge \dots \wedge b \equiv_{n_k} a_k)$ .*  $\square$

**PROOF.** Let us first consider the case where there exists an  $r \in \{1, \dots, l-1\}$  such that  $(r \equiv_{n_1} a_1 \wedge \dots \wedge r \equiv_{n_k} a_k)$ . It is obvious that  $(b \equiv_{n_1} a_1 \wedge \dots \wedge b \equiv_{n_k} a_k)$  if, and only if,  $(b \equiv_{n_1} r \wedge \dots \wedge b \equiv_{n_k} r)$  if, and only if,  $(n_1 \mid b-r \wedge \dots \wedge n_k \mid b-r)$  if, and only if,  $\text{lcm}\{n_1, \dots, n_k\} \mid b-r$  if, and only if,  $b \equiv_l r$ .

For the second claim of the above fact we prove the contraposition. I.e. we assume that there is some  $b \in \mathbb{Z}$  with  $(b \equiv_{n_1} a_1 \wedge \dots \wedge b \equiv_{n_k} a_k)$ , and we show that an appropriate  $r$  does exist. In fact, let  $r \in \{0, \dots, l-1\}$  be the residue class of  $b$  modulo  $l$ , i.e.  $r \equiv_l b$ . Since  $l = \text{lcm}\{n_1, \dots, n_k\}$ , we know that  $n_j \mid l$ , and hence  $r \equiv_{n_j} b \equiv_{n_j} a_j$ , for every  $j \in \{1, \dots, k\}$ .  $\blacksquare$

The above fact tells us that we can replace the constraints in  $R$  by the single constraint  $y \equiv_l res$ , where  $l := \text{lcm}\{n_j : j \text{ such that } \alpha_j \in R\}$ , and where the interpretation of the

variable  $res$  is determined by the  $FO(\mathfrak{Prresb})$ -formula

$$\psi_{res}(res, \vec{z}) := (0 \leq res < l \cdot 1) \wedge \bigwedge_{j: \alpha_j \in R} res \equiv_{n_j} t_j(\vec{z}).$$

As already done in Example 5.6, we consider a variable  $first$  which is interpreted by the smallest integer  $> low$  that belongs to the correct residue class, i.e. that satisfies  $first \equiv_l res$ . This interpretation of the variable  $first$  can be enforced by the  $FO(\mathfrak{Prresb})$ -formula

$$\begin{aligned} \psi_{first}(first, low, res) := & (first > low) \wedge (first \equiv_l res) \wedge \\ & (\forall v (v > low \wedge v \equiv_l res) \rightarrow v \geq first). \end{aligned}$$

The constraints in  $L \cup U \cup R$  can be visualized as shown in Figure 1, from which we can directly see that there are exactly  $\max\left\{0, \left\lceil \frac{up - first}{l} \right\rceil\right\}$  many different  $\mathbf{y} \in \mathbb{Z}$  which satisfy all the constraints in  $L \cup U \cup R$ , provided that  $res$  exists and that  $L$  and  $U$  are nonempty. If  $res$  exists and  $L$  or  $U$  are empty, then there are infinitely many  $\mathbf{y} \in \mathbb{Z}$  which satisfy all the constraints in  $L \cup U \cup R$ . If  $res$  does not exist, then no  $\mathbf{y} \in \mathbb{Z}$  satisfies these constraints.

Remember that the given formula  $\varphi(x, \vec{z}) := \exists^{=x} y \bigwedge_{j=1}^n \alpha_j(y, \vec{z})$  may have, apart from the constraints in  $L \cup U \cup R$ , also constraints from  $I$  which are independent of  $y$ . (However, we assume that there are no equations, i.e., that  $E = \emptyset$ .) Altogether we obtain that  $\varphi(x, \vec{z})$  is equivalent to the  $FO(\mathfrak{Prresb})$ -formula  $\psi(x, \vec{z}) :=$

$$\begin{aligned} & \left( (\neg \bigwedge_{j: \alpha_j \in I} \beta_j(\vec{z})) \rightarrow x=0 \right) \wedge \left( (\bigwedge_{j: \alpha_j \in I} \beta_j(\vec{z})) \rightarrow \right. \\ & \left. \left( (\neg \exists res \psi_{res}(res, \vec{z})) \rightarrow x=0 \right) \wedge \left( (\exists res \psi_{res}(res, \vec{z})) \rightarrow \chi(x, \vec{z}, res) \right) \right), \end{aligned}$$

where  $\chi$  is defined as follows: If  $L$  or  $U$  are empty, then  $\chi(x, \vec{z}, res) := \neg x=x$ . If  $L$  and  $U$  are nonempty, then  $\chi(x, \vec{z}, res) :=$

$$\begin{aligned} & \exists low \exists up \exists first \\ & \psi_{low}(low, \vec{z}) \wedge \psi_{up}(up, \vec{z}) \wedge \psi_{first}(first, low, res) \wedge \\ & (up \leq first \rightarrow x=0) \wedge (up > first \rightarrow x = \left\lceil \frac{up - first}{l} \right\rceil). \end{aligned}$$

This completes the proof of Lemma 5.5. ■

From Lemma 5.5 we know how to eliminate the counting quantifier from a formula of the form  $\exists^{=x} y \theta(y, \vec{z})$ , where  $\theta$  is a conjunction of  $\mathfrak{Prresb}$ -atoms. The following lemma lifts the elimination of the counting quantifier to be valid also for formulas where  $\theta$  is a *disjunction* of conjunctions of atoms.

**LEMMA 5.8.** *Every  $FO_{unc}(\mathfrak{Prresb})$ -formula of the form  $\exists^{=x} y \bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(y, \vec{z})$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Prresb} \cup \{y, \vec{z}\}$ , is equivalent over  $\langle \mathbb{Z}, \mathfrak{Prresb} \rangle$  to an  $FO(\mathfrak{Prresb})$ -formula. □*

**PROOF.** The proof makes use of Lemma 5.5 and of the well-known *principle of inclusion and exclusion (P.I.E.)* for short; cf., e.g., the textbook [Cameron 1994]:

**FACT 5.9 [P.I.E.]** *For all  $m > 0$  and all finite sets  $C_1, \dots, C_m$ , the following is true:*

$$\left| \bigcup_{i=1}^m C_i \right| = \sum_{\emptyset \neq I \subseteq \{1, \dots, m\}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} C_i \right| \quad \square$$

We now concentrate on the proof of Lemma 5.8.

Let  $\exists^{=x}y \bigvee_{i=1}^m C_i(y, \vec{z})$  be the given formula, where  $C_i(y, \vec{z}) := \bigwedge_{j=1}^{n_i} \alpha_{i,j}(y, \vec{z})$ . Let  $\mathbf{x}, \vec{z}$  be interpretations in  $\mathbb{Z}$  of the variables  $x, \vec{z}$ . We write  $C_i(\cdot, \vec{z})$  to denote the set of all  $y \in \mathbb{Z}$  for which the conjunction  $C_i(y, \vec{z})$  is satisfied when interpreting  $y, \vec{z}$  by  $\mathbf{y}, \vec{z}$ . Obviously, we have

$$\langle \mathbb{Z}, \mathfrak{Presb}, \mathbf{x}, \vec{z} \rangle \models \exists^{=x}y \bigvee_{i=1}^m C_i(y, \vec{z}) \quad \text{if, and only if,}$$

$$x = \left| \bigcup_{i=1}^m C_i(\cdot, \vec{z}) \right| \stackrel{P.I.E.}{=} \sum_{\emptyset \neq I \subseteq \{1, \dots, m\}} (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} C_i(\cdot, \vec{z}) \right|.$$

For every set  $I$  we introduce a new variable  $x_I$  with the intended meaning that  $x_I = \left| \bigcap_{i \in I} C_i(\cdot, \vec{z}) \right|$ , which can be enforced by the formula  $\exists^{=x_I}y \bigwedge_{i \in I} C_i(y, \vec{z})$ . This leads to the fact that

$$x = \sum_I (-1)^{|I|-1} \cdot \left| \bigcap_{i \in I} C_i(\cdot, \vec{z}) \right| \quad \text{if, and only if,}$$

$$\langle \mathbb{Z}, \mathfrak{Presb}, \mathbf{x}, \vec{z} \rangle \models (\exists x_I)_I (x = \sum_I (-1)^{|I|-1} \cdot x_I) \wedge \bigwedge_I (\exists^{=x_I}y \bigwedge_{i \in I} C_i(y, \vec{z})).$$

Since  $\bigwedge_{i \in I} C_i(y, \vec{z}) = \bigwedge_{i \in I} \bigwedge_{j=1}^{n_i} \alpha_{i,j}(y, \vec{z})$ , we can apply Lemma 5.5 to replace each subformula  $\exists^{=x_I}y \bigwedge_{i \in I} C_i(y, \vec{z})$  by an  $FO(\mathfrak{Presb})$ -formula  $\varphi_I(x_I, \vec{z})$ .

Altogether, we obtain an  $FO(\mathfrak{Presb})$ -formula  $\psi(x, \vec{z})$  which is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to  $\exists^{=x}y \bigvee_{i=1}^m C_i(y, \vec{z})$ . This completes the proof of Lemma 5.8. ■

The result of Theorem 5.4, stating that Presburger's quantifier elimination can be extended to unary counting quantifiers, now is an easy consequence of Lemma 5.8 and Theorem 5.1:

#### PROOF OF THEOREM 5.4.

According to Presburger's quantifier elimination (Theorem 5.1) it suffices to show that every  $F\text{OunC}(\mathfrak{Presb})$ -formula  $\varphi$  is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to an  $FO(\mathfrak{Presb})$ -formula  $\psi$ . We proceed by induction on the construction of  $\varphi$ . The only nontrivial case is when  $\varphi$  is of the form  $\exists^{=x}y \chi(y, \vec{z})$ . By the induction hypothesis  $\chi$  is equivalent to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(y, \vec{z})$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{y, \vec{z}\}$ . Thus, from Lemma 5.8 we obtain the desired  $FO(\mathfrak{Presb})$ -formula  $\psi(x, \vec{z})$  which is equivalent to  $\varphi(x, \vec{z})$  over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ . ■

### 5.3 From $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ to $\langle \mathbb{N}, \mathfrak{Presb} \rangle$

It is straightforward to transfer Theorem 5.4 from  $\mathbb{Z}$  to  $\mathbb{N}$  to obtain

$$F\text{OunC}(<, +) = FO(<, +) \text{ on } \mathbb{N}.$$

Precisely, this means:

**COROLLARY 5.10.** *Every  $F\text{OunC}(\mathfrak{Presb})$ -formula  $\varphi(\vec{z})$  is equivalent over  $\langle \mathbb{N}, \mathfrak{Presb} \rangle$  to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z})$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{\vec{z}\}$ . □*

**PROOF.** We make use of Theorem 5.4 and of the following relativization of quantifiers which gives us, for every  $F\text{OunC}(\mathfrak{Presb})$ -formula  $\varphi(\vec{z})$ , an  $F\text{OunC}(\mathfrak{Presb})$ -formula  $\tilde{\varphi}(\vec{z})$  such that the following is valid for every interpretation  $\vec{z} \in \mathbb{N}$  of the variables  $\vec{z}$

$$(*) : \quad \langle \mathbb{N}, \mathfrak{Presb}, \vec{z} \rangle \models \varphi(\vec{z}) \quad \text{iff} \quad \langle \mathbb{Z}, \mathfrak{Presb}, \vec{z} \rangle \models \tilde{\varphi}(\vec{z}).$$

The formula  $\tilde{\varphi}$  is defined inductively via

- $\tilde{\varphi} := \varphi$  if  $\varphi$  is atomic,
- $\tilde{\varphi} := \neg\tilde{\psi}$  if  $\varphi = \neg\psi$ ,
- $\tilde{\varphi} := \tilde{\psi} \vee \tilde{\chi}$  if  $\varphi = \psi \vee \chi$ ,
- $\tilde{\varphi} := \exists y (y \geq 0 \wedge \tilde{\psi})$  if  $\varphi = \exists y \psi$ , and
- $\tilde{\varphi} := \exists^{=x} y (y \geq 0 \wedge \tilde{\psi})$  if  $\varphi = \exists^{=x} y \psi$ .

It is straightforward to see that  $(*)$  is indeed true.

According to Theorem 5.4, the formula  $\tilde{\varphi}(\vec{z})$  is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z})$ , where the  $\alpha_{i,j}$  are  $\mathfrak{Presb}$ -atoms. It is obvious that, whenever the variables  $\vec{z}$  are interpreted by non-negative integers  $\vec{z} \in \mathbb{N}$ , it makes no difference whether the atom  $\alpha_{i,j}(\vec{z})$  is evaluated in the structure  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  or in the structure  $\langle \mathbb{N}, \mathfrak{Presb} \rangle$ . We thus obtain for every interpretation  $\vec{z} \in \mathbb{N}$  of the variables  $\vec{z}$  that

$$\begin{aligned} \langle \mathbb{N}, \mathfrak{Presb}, \vec{z} \rangle \models \varphi(\vec{z}) & \text{ iff } \langle \mathbb{Z}, \mathfrak{Presb}, \vec{z} \rangle \models \tilde{\varphi}(\vec{z}) \\ & \text{ iff } \langle \mathbb{Z}, \mathfrak{Presb}, \vec{z} \rangle \models \bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z}) \\ & \text{ iff } \langle \mathbb{N}, \mathfrak{Presb}, \vec{z} \rangle \models \bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z}). \end{aligned}$$

I.e., the  $\mathit{FOunC}(\mathfrak{Presb})$ -formula  $\varphi(\vec{z})$  is equivalent over  $\langle \mathbb{N}, \mathfrak{Presb} \rangle$  to the quantifier free formula  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z})$ .  $\blacksquare$

#### 5.4 From $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$ to Initial Segments of $\mathbb{N}$

Let us now investigate the finite versions of Presburger arithmetic, where the universe is some initial segment of  $\mathbb{N}$ . I.e., for every  $N \in \mathbb{N}_{>0}$  we want to consider the substructure of  $\langle \mathbb{N}, \mathfrak{Presb} \rangle$  with universe  $\underline{N} := \{0, \dots, N\}$ .

There is some technical difficulty since  $\underline{N}$  is not closed under the addition function  $f_+$ . We therefore move over to the version  $\mathfrak{Presb}'$  of Presburger arithmetic without function symbols. I.e.,  $\mathfrak{Presb}' := \{0, 1, R_+, <, (\equiv_n)_{n \in \mathbb{N}_{>0}}\}$ , where  $R_+$  denotes the ternary addition relation (which, in this paper, is usually simply denoted  $+$ ).

Now, the initial segment  $\langle \underline{N}, \mathfrak{Presb}' \rangle$  of Presburger arithmetic is defined in the canonical way, i.e.,  $R_+$  is interpreted by the set of all triples  $(a, b, c) \in \underline{N}^3$  for which  $a + b = c$ . The aim of this section is to show that

$$\mathit{FOunC}(<, +) = \mathit{FO}(<, +) \text{ on initial segments of } \mathbb{N}.$$

Precisely, this means:

**COROLLARY 5.11.** *Every  $\mathit{FOunC}(\mathfrak{Presb}')$ -formula  $\varphi(\vec{z})$  is equivalent over the class  $\{\langle \underline{N}, \mathfrak{Presb}' \rangle : N \in \mathbb{N}_{>0}\}$  to an  $\mathit{FO}(\mathfrak{Presb}')$ -formula  $\psi(\vec{z})$ .  $\square$*

Here, the formula  $\psi$  cannot be taken quantifier free in general, because the addition is not present as a *function* (allowing to express summations of more than just two variables), but only as a *relation*.

**PROOF OF COROLLARY 5.11.**

The proof is similar to the proof of Corollary 5.10. However, the fact that the universe is finite and that the addition is only present as a relation, causes some technical problems.

We make use of Theorem 5.4 and an appropriate relativization of quantifiers: we introduce a new variable  $max$  with the intended meaning that  $max$  denotes the maximum element  $N$  in the underlying finite universe; and we transform a given  $FOunc(\mathfrak{Presb}')$ -formula  $\varphi(\vec{z})$  into an appropriate  $FOunc(\mathfrak{Presb})$ -formula  $\tilde{\varphi}(\vec{z}, max)$  such that the following is valid for every  $N \in \mathbb{N}_{>0}$  and for every interpretation  $\vec{z} \in \underline{N}$  of the variables  $\vec{z}$

$$(*) : \quad \langle \underline{N}, \mathfrak{Presb}', \vec{z} \rangle \models \varphi(\vec{z}) \quad \text{iff} \quad \langle \mathbb{Z}, \mathfrak{Presb}, \vec{z}, N \rangle \models \tilde{\varphi}(\vec{z}, max).$$

The formula  $\tilde{\varphi}$  is defined inductively via

- $\tilde{\varphi} := f_+(x, y) = z$  if  $\varphi = R_+(x, y, z)$ ,
- $\tilde{\varphi} := \varphi$  if  $\varphi$  is an atom not involving the addition relation  $R_+$ ,
- $\tilde{\varphi} := \neg\tilde{\psi}$  if  $\varphi = \neg\psi$ ,
- $\tilde{\varphi} := \tilde{\psi} \vee \tilde{\chi}$  if  $\varphi = \psi \vee \chi$ ,
- $\tilde{\varphi} := \exists y (0 \leq y \leq max \wedge \tilde{\psi})$  if  $\varphi = \exists y \psi$ , and
- $\tilde{\varphi} := \exists^{=x} y (0 \leq y \leq max \wedge \tilde{\psi})$  if  $\varphi = \exists^{=x} y \psi$ .

It is straightforward to see that  $(*)$  is indeed true.

According to Theorem 5.4, the formula  $\tilde{\varphi}(\vec{z}, max)$  is equivalent over  $\langle \mathbb{Z}, \mathfrak{Presb} \rangle$  to a formula of the form  $\bigvee_{i=1}^m \bigwedge_{j=1}^{n_i} \alpha_{i,j}(\vec{z}, max)$ , where the  $\alpha_{i,j}$  are atoms built from the symbols in  $\{=\} \cup \mathfrak{Presb} \cup \{\vec{z}, max\}$ .

Of course, it suffices to show that each such  $\mathfrak{Presb}$ -atom can be transformed into an  $FO(\mathfrak{Presb}')$ -formula  $\chi_{i,j}(\vec{z}, max)$  such that the following is valid for every  $N \in \mathbb{N}_{>0}$  and for every interpretation  $\vec{z} \in \underline{N}$  of the variables  $\vec{z}$

$$(**) : \quad \langle \mathbb{Z}, \mathfrak{Presb}, \vec{z}, N \rangle \models \alpha_{i,j}(\vec{z}, max) \quad \text{iff} \quad \langle \underline{N}, \mathfrak{Presb}', \vec{z}, N \rangle \models \chi_{i,j}(\vec{z}, max).$$

To see what is the problem about defining  $\chi_{i,j}$ , let us have a closer look at the  $\mathfrak{Presb}$ -atom  $\alpha_{i,j}$ . By definition, the atom  $\alpha_{i,j}$  expresses that

$$(***) : \quad u_1 + \cdots + u_k \times v_1 + \cdots + v_l$$

where  $k, l \in \mathbb{N}$ ,  $\times$  is an element in  $\{=, <, \equiv_n : n \in \mathbb{N}_{>0}\}$ , and  $u_1, \dots, u_k, v_1, \dots, v_l$  are (not necessarily distinct) elements in  $\{0, 1, \vec{z}, max\}$ .

When the variable  $max$  is interpreted by some  $N \in \mathbb{N}_{>0}$  and the variables  $\vec{z}$  are interpreted by numbers  $\vec{z} \in \underline{N}$ , then the term  $u_1 + \cdots + u_k$  evaluates to a number of size at most  $k \cdot N$ . But there is no guarantee that this number does not exceed  $N$ , i.e. that it belongs to the underlying finite universe  $\underline{N}$ . We therefore have to move over to the 2-tuple version which allows us to represent a number  $x$  of size at most  $N^2$  ( $> k \cdot N$ , for  $N$  large enough) by two numbers  $x_1, x_0$  in  $\underline{N}$  via  $x = x_1 \cdot (N+1) + x_0$ . From Theorem 3.4 we know that there is an  $FO(R_+)$ -formula  $\varphi_+^2$  which expresses the addition relation for numbers that are represented by such 2-tuples. Hence, the result of the summation  $u_1 + \cdots + u_k$  is the number represented by the 2-tuple  $(u_1^{(k)}, u_0^{(k)})$ , where  $(u_1^{(k)}, u_0^{(k)})$  is determined by the  $FO(R_+)$ -formula

$$(\exists u_1^{(i)} \exists u_0^{(i)})_{i \leq k} u_1^{(1)} = 0 \wedge u_0^{(1)} = u_1 \wedge \bigwedge_{i=2}^k \varphi_+^2(u_1^{(i-1)}, u_0^{(i-1)}, 0, u_i, u_1^{(i)}, u_0^{(i)}).$$

In the same way one obtains a 2-tuple  $(v_1^{(l)}, v_0^{(l)})$  which represents the result of the summation  $v_1 + \cdots + v_l$ . Finally, making use of the formulas  $\varphi_{<}^2$  and  $\varphi_{\equiv_n}^2$  from Theorem 3.4,  $(***)$  can be replaced by

- $(u_1^{(k)}=v_1^{(l)} \wedge u_0^{(k)}=v_0^{(l)})$  if  $\times$  is  $=$
- $\varphi_{<}^2(u_1^{(k)}, u_0^{(k)}, v_1^{(l)}, v_0^{(l)})$  if  $\times$  is  $<$
- $\varphi_{\equiv_n}^2(u_1^{(k)}, u_0^{(k)}, v_1^{(l)}, v_0^{(l)})$  if  $\times$  is a congruence relation  $\equiv_n$ .

Altogether we obtain an  $FO(\mathfrak{Resb}')$ -formula  $\chi_{i,j}$  that has property (\*\*). This completes the proof of Corollary 5.11. ■

## 6. APPLICATIONS

In this section we point out some applications of the result that  $FOUNC(<, +) = FO(<, +)$  on  $\mathbb{N}$  and on initial segments of  $\mathbb{N}$ . We point out how this result can be used for showing that some class of finite structures is not definable in first-order logic with unary counting quantifiers and addition. This leads to easy proofs that reachability and connectivity of finite graphs are not expressible in  $FOUNC(+)$ .

Afterwards, we obtain the failure of a particular version of the Crane Beach conjecture.

### 6.1 Reachability

A finite *graph*  $G = \langle V, E \rangle$  consists of a finite set  $V$  of *vertices* and a set  $E \subseteq V^2$  of directed edges. A directed *path*  $p = (v_0, \dots, v_k)$  of length  $k$  is a sequence of vertices satisfying  $E(v_i, v_{i+1})$  for all  $i \in \{0, \dots, k-1\}$ . We say that  $p$  is a path from  $s$  to  $t$  if  $s = v_0$  and  $t = v_k$ . The path  $p$  is called *deterministic* if, for each  $i \in \{0, \dots, k-1\}$ , the edge  $(v_i, v_{i+1})$  is the *unique* edge in  $G$  leaving vertex  $v_i$ , i.e., there is no vertex  $u \neq v_{i+1}$  in  $V$  such that  $E(v_i, u)$ .

**DEFINITION 6.1.** *Deterministic Reachability*, DET-REACH, is the set of all finite graphs  $G$ , together with a distinguished source vertex  $s$  and a distinguished target vertex  $t$ , such that there is a *deterministic path* from  $s$  to  $t$  in  $G$ . I.e.,

$$\text{DET-REACH} := \left\{ \langle G, s, t \rangle : \begin{array}{l} G = \langle V, E \rangle \text{ is a finite graph, } s, t \in V, \text{ and} \\ \text{there is a deterministic path from } s \text{ to } t \text{ in } G \end{array} \right\}.$$

□

The problem DET-REACH is complete for *LOGSPACE* via first-order reductions (cf., e.g., the textbook [Immerman 1999, Theorem 3.23]). An important open question in complexity theory is to separate *LOGSPACE* from other, potentially weaker, complexity classes. Such a separation could be achieved by showing that the problem DET-REACH does not belong to the potentially weaker class. One potentially weaker class for which no separation from *LOGSPACE* is known by now<sup>5</sup>, is the class  $TC^0$  that consists of all problems solvable with uniform threshold circuits of polynomial size and constant depth. As already mentioned in Section 4.3, it was shown in [Barrington et al. 1990] that, for ordered structures over arbitrary signatures  $\tau$ , logtime-uniform  $TC^0$  is exactly the class of all problems definable in  $FOUNC(+, \times, \tau)$ . To separate  $TC^0$  from *LOGSPACE* it would therefore suffice to show that DET-REACH is not definable in  $FOUNC(+, \times, E, s, t)$ .

Ruhl [Ruhl 1999] achieved a first step towards such a separation by showing the (weaker) result that DET-REACH is not definable in  $FOUNC(+, E, s, t)$ . Precisely, this means:

<sup>5</sup> $TC^0$  has not even been separated from *NP*, cf., [Allender 1996].

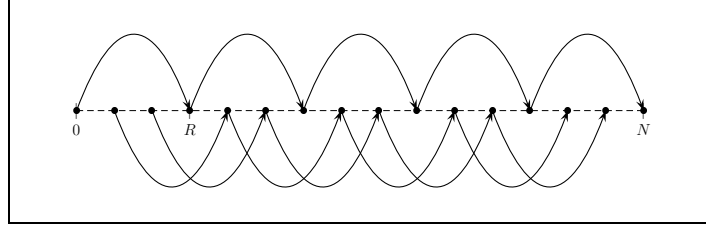


Fig. 2. Visualization of the graph  $G_{R,N}$  (for  $R = 3$  and  $N = 15$ ). There is an edge from a vertex  $u$  to a vertex  $v$  iff  $u + R = v$ .

**THEOREM 6.2 [RUHL 1999].** *There is no  $FOunC(+, E, s, t)$ -sentence  $\psi$  such that, for every  $N \in \mathbb{N}_{>0}$  and all graphs  $G = \langle \underline{N}, E \rangle$  with vertex set  $\underline{N}$ , and vertices  $s, t \in \underline{N}$ , we have  $\langle G, s, t \rangle \in \text{DET-REACH}$  iff  $\langle \underline{N}, +, E, s, t \rangle \models \psi$ .  $\square$*

The aim of this section is to point out that Ruhl’s theorem can be proved easily when making use of our result that  $FOunC(+)$  =  $FO(+)$  on initial segments of  $\mathbb{N}$ . Before presenting the easy proof, let us first outline Ruhl’s approach:

Ruhl’s proof method is the Ehrenfeucht-Fraïssé game for  $FOunC(+, E)$ . He considers, for each  $N \in \mathbb{N}_{>0}$  and  $R \in \underline{N}$  the graph  $G_{R,N} = \langle \underline{N}, E_{R,N} \rangle$  where the edge relation  $E_{R,N}$  is defined via “ $E_{R,N}(u, v)$  iff  $u + R = v$ ”, for all vertices  $u, v \in \underline{N}$ . An illustration of the graph  $G_{R,N}$  is given in Figure 2.

Note that the graph  $G_{R,N}$  is constructed in such a way that  $R \mid N$  if, and only if, there is a deterministic path from 0 to  $N$ , i.e.  $\langle G_{R,N}, 0, N \rangle \in \text{DET-REACH}$ .

For every fixed number  $M$  of rounds in the Ehrenfeucht-Fraïssé game, Ruhl constructs an  $N_M \in \mathbb{N}_{>0}$  and an  $R_M \in \underline{N_M}$  such that  $R_M \mid N_M$  and  $2R_M \nmid N_M$ . Afterwards he explicitly exposes a clever and very intricate winning strategy for the duplicator in the  $M$ -round Ehrenfeucht-Fraïssé game for  $FOunC(+, E, s, t)$  on the structures  $\langle G_{R_M, N_M}, 0, N_M \rangle$  and  $\langle G_{2R_M, N_M}, 0, N_M \rangle$ . He thus obtains, for every  $M$ , that the structures  $\langle G_{R_M, N_M}, 0, N_M \rangle \in \text{DET-REACH}$  and  $\langle G_{2R_M, N_M}, 0, N_M \rangle \notin \text{DET-REACH}$  cannot be distinguished by  $FOunC(+, E, s, t)$ -formulas of quantifier depth  $M$ . Altogether, this shows that  $\text{DET-REACH}$  is not definable in  $FOunC(+, E, s, t)$ .

As usual in Ehrenfeucht-Fraïssé arguments, precise bookkeeping is necessary for the proof. This bookkeeping can be avoided when using Presburger’s quantifier elimination and its extension to unary quantifiers:

**PROOF OF THEOREM 6.2.** By contradiction.

Suppose that  $\psi$  is an  $FOunC(+, E, s, t)$ -sentence defining  $\text{DET-REACH}$ .

The first step of the proof is to transform  $\psi$  into an  $FOunC(+)$ -formula  $\varphi_1(y_1, y_2)$  which expresses that  $R \mid N$ , whenever the variables  $y_1$  and  $y_2$  are interpreted by natural numbers  $R$  and  $N$ , respectively. For this transformation we make use of Ruhl’s graphs  $G_{R,N}$  from which we know that  $\langle G_{R,N}, 0, N \rangle \in \text{DET-REACH}$  if, and only if,  $R \mid N$ . The formula  $\varphi_1(y_1, y_2)$  is obtained from  $\psi$  by replacing every atom  $E(u, v)$  with the atom  $u + y_1 = v$ , by replacing  $s$  with 0, by replacing  $t$  with  $y_2$ , and by relativizing all quantifications to numbers  $\leq y_2$ . Here,  $y_1$  and  $y_2$  are variables not occurring in  $\psi$ . Of course we have for all

$R, N \in \mathbb{N}$  that

$$\begin{aligned} R \mid N & \text{ iff } \langle G_{R,N}, 0, N \rangle \in \text{DET-REACH} \\ & \text{ iff } \langle \underline{N}, +, E_{R,N}, 0, N \rangle \models \psi \\ & \text{ iff } \langle \mathbb{N}, +, R, N \rangle \models \varphi_1(y_1, y_2). \end{aligned}$$

This completes the first step of the proof.

From Corollary 5.10 we know that the counting quantifiers can be eliminated from  $\varphi_1(y_1, y_2)$ . I.e., we obtain an  $FO(+)$ -formula  $\varphi_2(y_1, y_2)$  which expresses that  $R \mid N$  whenever the variables  $y_1, y_2$  are interpreted by numbers  $R, N \in \mathbb{N}$ . This gives us an  $FO(+)$ -formula  $\varphi_3(y_2) := \forall y_1 \varphi_2(y_1, y_2) \rightarrow (y_1=1 \vee y_1=y_2)$  which expresses that  $y_2$  is a prime number. In other words:  $\varphi_3$  is an  $FO(+)$ -formula that defines the (non semi-linear) set of all prime numbers. This is a contradiction to the Theorem of Ginsburg and Spanier (cf., Section 3.2) and completes the proof of Theorem 6.2. ■

## 6.2 Generalizing this Approach

In this section we show that the above proof method can be generalized such that, via  $FOunC(+)$ -reductions, non- $FO(+)$ -definability of relations in  $\mathbb{N}$  can be transferred to non- $FOunC(+)$ -definability of graph properties.

A signature is called *relational* if it does not contain function symbols.

Let  $\sigma$  be a relational signature and let  $s \in \mathbb{N}_{>0}$ . An  $FOunC(+)$ -interpretation  $I$  of  $\sigma$  in  $\mathbb{N}^s$  consists of

1. an  $FOunC(+)$ -formula  $\varphi_{max}^I(x, y_1, \dots, y_s)$  such that the following is true: for every  $\vec{a} \in \mathbb{N}^s$  there is exactly one element in  $\mathbb{N}$ , denoted  $max_{\vec{a}}$ , such that  $\langle \mathbb{N}, + \rangle \models \varphi_{max}^I(max_{\vec{a}}, \vec{a})$ ; and for this element it is true that  $a_i \leq max_{\vec{a}}$ , for all  $i \in \{1, \dots, s\}$ .
2. an  $FOunC(+)$ -formula  $\varphi_c^I(x, y_1, \dots, y_s)$ , for every constant symbol  $c \in \sigma$ , such that the following is true: for every  $\vec{a} \in \mathbb{N}^s$  there is exactly one element in  $\mathbb{N}$ , denoted  $c_{\vec{a}}$ , such that  $\langle \mathbb{N}, + \rangle \models \varphi_c^I(c_{\vec{a}}, \vec{a})$ ; and for this element it is true that  $c_{\vec{a}} \leq max_{\vec{a}}$ .
3. an  $FOunC(+)$ -formula  $\varphi_R^I(x_1, \dots, x_{ar(R)}, y_1, \dots, y_s)$ , for every relation symbol  $R \in \sigma$ .

For every  $\vec{a} \in \mathbb{N}^s$  the finite  $\sigma$ -structure  $I(\vec{a})$  is defined as the structure with universe  $\{0, \dots, max_{\vec{a}}\}$ , constants  $c^{I(\vec{a})} := c_{\vec{a}}$ , for all  $c \in \sigma$ , and relations

$$R^{I(\vec{a})} := \{\vec{b} \in \{0, \dots, max_{\vec{a}}\}^{ar(R)} : \langle \mathbb{N}, + \rangle \models \varphi_R(\vec{b}, \vec{a})\},$$

for all  $R \in \sigma$ .

**DEFINITION 6.3.** Let  $s \in \mathbb{N}_{>0}$ , let  $S \subseteq \mathbb{N}^s$ , let  $\sigma$  be a relational signature, and let  $\mathcal{C}$  be a class of finite  $\sigma$ -structures.  $S$  is  $FOunC(+)$ -reducible to  $\mathcal{C}$  if there is an  $FOunC(+)$ -interpretation  $I$  of  $\sigma$  in  $\mathbb{N}^s$  such that, for all  $\vec{a} \in \mathbb{N}^s$ , we have  $\vec{a} \in S$  iff  $I(\vec{a}) \in \mathcal{C}$ . □

**LEMMA 6.4.** Let  $s \in \mathbb{N}_{>0}$ , let  $\sigma$  be a relational signature, and let  $I$  be an  $FOunC(+)$ -interpretation of  $\sigma$  in  $\mathbb{N}^s$ .

For every  $FOunC(+, \sigma)$ -sentence  $\psi$  there is an  $FO(+)$ -formula  $\hat{\psi}(y_1, \dots, y_s)$  such that the following is true for every  $\vec{a} \in \mathbb{N}^s$ :  $\langle \mathbb{N}, + \rangle \models \hat{\psi}(\vec{a})$  iff  $I(\vec{a}) \models \psi$ . □

**PROOF.** From Corollary 5.10 we know that it suffices to construct an  $FOunC(+)$ -formula  $\hat{\psi}(y_1, \dots, y_s)$  such that, for all  $\vec{a} \in \mathbb{N}^s$ , we have  $\langle \mathbb{N}, + \rangle \models \hat{\psi}(\vec{a})$  iff  $I(\vec{a}) \models \psi$ . We choose

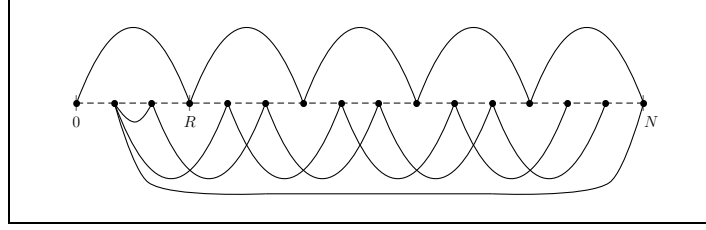


Fig. 3. Visualization of the graph  $H_{R,N}$  (for  $R = 3$  and  $N = 15$ ). There is an edge between vertices  $u$  and  $v$  iff  $(u+R=v) \vee (u=1 \wedge v=N) \vee (0 < u \wedge u+1=v \wedge v < R)$ .

$\tilde{\psi}$  as  $\exists z_{max} (\exists z_c)_{c \in \sigma} \varphi_{max}^I(z_{max}, \vec{y}) \wedge \bigwedge_{c \in \sigma} \varphi_c^I(z_c, \vec{y}) \wedge \tilde{\psi}(\vec{y}, z_{max}, \vec{z}_c)$ , where  $\tilde{\psi}$  is obtained from  $\psi$  by relativizing every quantification to numbers  $\leq z_{max}$ , replacing every occurrence of a constant symbol  $c$  by the variable  $z_c$ , and replacing every occurrence of an atomic formula of the form  $R(\vec{x})$  by the formula  $\varphi_R^I(\vec{x}, \vec{y})$ .

It is straightforward to check that  $\tilde{\psi}$  has the desired properties. ■

From Lemma 6.4 we directly obtain

**THEOREM 6.5.** *Let  $\mathcal{C}$  be a class of finite  $\sigma$ -structures, where  $\sigma$  is a relational signature. If there is an  $s \in \mathbb{N}_{>0}$  and a relation  $S \subseteq \mathbb{N}^s$  such that  $S$  is not  $FO(+)$ -definable in  $\mathbb{N}$  but  $S$  is  $FOunC(+)$ -reducible to  $\mathcal{C}$ , then  $\mathcal{C}$  is not definable by an  $FOunC(+, \sigma)$ -sentence. □*

Obviously, the above proof of Theorem 6.2 can be viewed as an application of Theorem 6.5. In a similar way, we can also show, e.g., that *connectivity* of finite graphs is not  $FOunC(+)$  definable:

**DEFINITION 6.6.** *Connectivity, CONN, is the set of all finite graphs  $G$  which are connected, i.e., where there is a path from  $u$  to  $v$ , for all vertices  $u \neq v$  in  $G$ . □*

**THEOREM 6.7.** *CONN is not definable in  $FOunC(+, E)$ , i.e., there is no  $FOunC(+, E)$ -sentence  $\psi$  such that, for every  $N \in \mathbb{N}_{>0}$  and all graphs  $G = \langle \underline{N}, E \rangle$ , we have  $\langle \underline{N}, E \rangle \in \text{CONN}$  iff  $\langle \underline{N}, +, E \rangle \models \psi$ . □*

**PROOF.** Let  $S$  be the divisibility relation on  $\mathbb{N}$ , i.e.,  $S = \{(R, N) \in \mathbb{N}^2 : R \mid N\}$ . Of course,  $S$  is not  $FO(+)$ -definable in  $\mathbb{N}$  (because otherwise, the non semi-linear set of all prime numbers would be  $FO(+)$ -definable, contradicting the Theorem of Ginsburg and Spanier (cf., Section 3.2)).

In order to show that CONN is not definable in  $FOunC(+, E)$ , it therefore, according to Theorem 6.5, suffices to show that  $S$  is  $FOunC(+)$ -reducible to CONN.

We choose the  $FOunC(+)$ -interpretation  $I$  of  $\{E\}$  in  $\mathbb{N}^2$  in such a way that, for all  $(R, N) \in \mathbb{N}^2$ , the structure  $I(R, N)$  is exactly the graph  $H_{R,N}$  illustrated in Figure 3.

I.e., we choose

$$\begin{aligned} \varphi_{max}^I(x, y_1, y_2) &:= (y_1 \leq y_2 \wedge x = y_2) \vee (y_1 > y_2 \wedge x = y_1), \quad \text{and} \\ \varphi_E^I(x_1, x_2, y_1, y_2) &:= y_1 \leq y_2 \wedge (\chi(x_1, x_2, y_1, y_2) \vee \chi(x_2, x_1, y_1, y_2)), \quad \text{where} \\ \chi(u_1, u_2, y_1, y_2) &:= (u_1 + y_1 = u_2) \vee (u_1 = 1 \wedge u_2 = y_2) \vee \\ &\quad (0 < u_1 \wedge u_1 + 1 = u_2 \wedge u_2 < y_1). \end{aligned}$$

It is straightforward to check that, for all  $(R, N) \in \mathbb{N}^2$ , we have  $R \mid N$  if, and only if, the graph  $I(R, N)$  is connected. Therefore, we have shown that  $S$  is  $F\text{OunC}(+)$ -reducible to  $\text{CONN}$ . Together with Theorem 6.5, this completes the proof of Theorem 6.7. ■

### 6.3 A Specific Case of the Crane Beach Conjecture

The Crane Beach conjecture deals with logical definability of neutral letter languages. A language  $L$  (i.e., a set of finite strings) over an alphabet  $A$  is said to have a *neutral letter*  $e \in A$  if inserting or deleting  $e$ 's from any string over  $A$  does not change the string's membership or non-membership in  $L$ .

A string  $w = w_0 \cdots w_N$  over alphabet  $A$  is represented as the  $(\{\langle \cdot \rangle\} \cup \{Q_a : a \in A\})$ -structure  $\mathcal{A}^w$  with universe  $\underline{N}$ , where the predicate  $Q_a(x)$  is true for all positions  $x$  in  $w$  that carry the letter  $a$ . A language  $L$  over  $A$  is *defined* by a sentence  $\varphi$  if, and only if, the following is true for all strings  $w$  over  $A$ :  $w \in L$  iff  $\mathcal{A}^w \models \varphi$ .

Given a logic  $F$  and a class  $\mathfrak{A}$  of arithmetic predicates, the Crane Beach conjecture is said to be true for  $F(\langle, \mathfrak{A} \rangle)$  iff for every finite alphabet  $A$  and every neutral letter language  $L$  over  $A$  the following is true: if  $L$  is definable in  $F(\langle, \mathfrak{A} \rangle)$  then  $L$  is already definable in  $F(\langle)$ .

The Crane Beach conjecture is closely related to uniformity conditions in circuit complexity theory and to collapse results in database theory. Depending on the logic  $F$  and the predicates  $\mathfrak{A}$ , the Crane Beach conjecture turns out to be true for some cases and false for others. A detailed investigation and a state-of-the-art overview of what is known about the Crane Beach conjecture can be found in [Barrington et al. 2004]. Using the result of Corollary 5.10 that  $F\text{OunC}(\langle, +) = FO(\langle, +)$  on  $\mathbb{N}$ , one can prove the conjecture to be false for the following specific case:

**THEOREM 6.8** [BARRINGTON ET AL. 2004].

*Let  $P \subseteq \mathbb{N}$  be a set that is not semi-linear. The Crane Beach conjecture is false for  $F\text{OunC}(\langle, P)$ . More precisely: There is a neutral letter language  $L$  over the alphabet  $\{a, e\}$  that can be defined in  $F\text{OunC}(\langle, P)$ , but not in  $F\text{OunC}(\langle)$ .* □

**PROOF (SKETCH).** Choose  $L$  to be the set of all strings  $w$  over  $\{a, e\}$  where the number of  $a$ 's in  $w$  belongs to  $P$ . Now assume, for the sake of contradiction, that  $L$  is definable by an  $F\text{OunC}(\langle)$ -sentence  $\chi$ . I.e., for every string  $w$  over  $\{a, e\}$  we assume that  $\mathcal{A}^w \models \chi$  iff  $w \in L$ . It is not difficult to translate  $\chi$  into an  $F\text{OunC}(\langle)$ -formula  $\varphi(x)$  such that  $P = \{N \in \mathbb{N} : \langle \mathbb{N}, \langle \rangle \models \varphi(N)\}$ . However, due to Corollary 5.10,  $\varphi(x)$  is equivalent over  $\mathbb{N}$  to a  $FO(\langle, +)$ -formula  $\psi(x)$ . From the Theorem of Ginsburg and Spanier we therefore obtain that  $P$  is semi-linear, which is a contradiction to the choice of  $P$ . ■

## 7. CONCLUSION AND OPEN QUESTIONS

In this paper we have gained a detailed picture of the expressive power of first-order logic with counting quantifiers and arithmetic. This picture if visualized in the following Figures 4 and 5. Concerning these diagrams, the only question that remains open is whether  $F\text{OunC}(+, \times) = FO(+, \times)$  on initial segments of  $\mathbb{N}$ . As pointed out in Section 3.4, inequality would imply  $LINH \neq ETIME$ , whereas no such complexity theoretic consequence is known for the case of equality.

A main theorem of this paper is that Presburger arithmetic is closed under unary counting quantifiers. As applications of this we obtained that the Crane Beach conjecture is false for  $FOunC(<, P)$  whenever  $P$  is a set of natural numbers that is not semi-linear. Also, we obtained (see Theorem 6.5) that, via  $FOunC(+)$ -reductions, non- $FO(+)$ -expressibility of relations in  $\mathbb{N}$  can be transferred to non- $FOunC(+)$ -definability of graph properties. In particular, this led to an easy proof of Ruhl's result that deterministic reachability in finite graphs is not definable in  $FOunC(+)$ , and similarly, that connectivity of finite graphs is not definable in  $FOunC(+)$ .

With regard to the questions here, we want to mention the following problems:

- Is there any serious complexity theoretic consequence in case that  $FOunC(+, \times) = FO(+, \times)$  on initial segments of  $\mathbb{N}$ ?
- The author thinks it would be fruitful to translate the tools developed for bounded arithmetic (cf., [Esbelin and More 1998]) into the language used for descriptive complexity and circuit complexity, i.e., into results about  $FO(+, \times)$  on initial segments of  $\mathbb{N}$  and on finite structures.
- It is an important task to search for inexpressibility results for  $FOunC(+, \times)$  on finite structures. Since  $FOunC(+, \times)$  corresponds to the complexity class  $TC^0$ , an inexpressibility result would give us a separation of complexity classes. This indicates that this task will be very hard to attack.
- More tractable seems the investigation of the fine structure of first-order logic with majority quantifiers. As mentioned in Section 4.3, it was shown in [Barrington et al. 1990] that

$$\mathbf{FObinM}(<) = \mathbf{FOunM}(+, \times) = \mathbf{FOunC}(+, \times) = \mathbf{TC}^0$$

**on finite structures.**

In [Lautemann et al. 2001] it was shown that  $FOunM(<) \subsetneq FObinM(<)$ . It is not difficult to see that  $FO(<) \subsetneq FOunM(<)$ : The  $FOunM(<)$ -formula  $\exists x (My(y \leq x) \wedge My(y \geq x))$  expresses that the cardinality of the underlying universe is odd, whereas this is not expressible in  $FO(<)$  (cf., e.g., the textbook [Ebbinghaus and Flum 1999, Example 2.3.6]). It remains open whether on finite structures we have

$$\mathbf{FOunM}(<) \stackrel{?}{=} \mathbf{FOunM}(<, +) \stackrel{?}{=} \mathbf{FOunC}(<, +).$$

## APPENDIX

### PROOF OF THEOREM 3.4.

For a tuple  $\vec{x} := (x_{d-1}, \dots, x_0) \in (\underline{N})^d$  we write  $\#_N(\vec{x})$  for the number  $\sum_{i=0}^{d-1} x_i(N+1)^i$ .

(a): Obviously, the formulas  $\varphi_{<}^d$  can be inductively defined via

$$\begin{aligned} \varphi_{<}^1(x_0, y_0) &:= x_0 < y_0, \quad \text{and, for all } d \geq 1, \\ \varphi_{<}^{d+1}(x_d, \dots, x_0, y_d, \dots, y_0) &:= x_d < y_d \vee (x_d = y_d \wedge \varphi_{<}^d(x_{d-1}, \dots, x_0, y_{d-1}, \dots, y_0)). \end{aligned}$$

(b): We first concentrate on  $d=1$ . For  $x_0, y_0, z_1, z_0 \in \underline{N} := \{0, \dots, N\}$ , the formula  $\varphi_{+}^1(x_0, y_0, z_1, z_0)$  shall express that  $x_0 + y_0 = z_1 \cdot (N+1) + z_0$ .

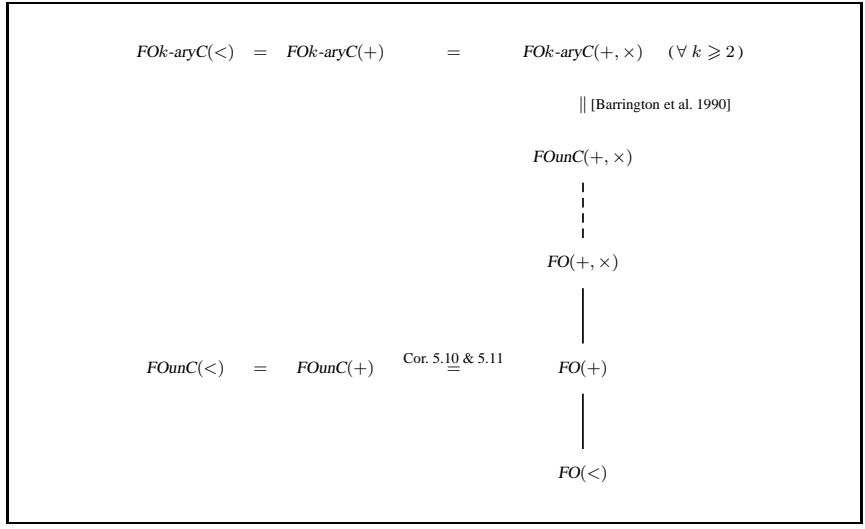


Fig. 4. Expressive power for *pure arithmetic*. Lines indicate proper inclusions. For  $\mathbb{N}$  the dashed line can be replaced by equality (cf., Proposition 4.2). For initial segments of  $\mathbb{N}$  this remains open; however, as pointed out in Section 3.4, inequality would imply  $LINH \neq ETIME$ .

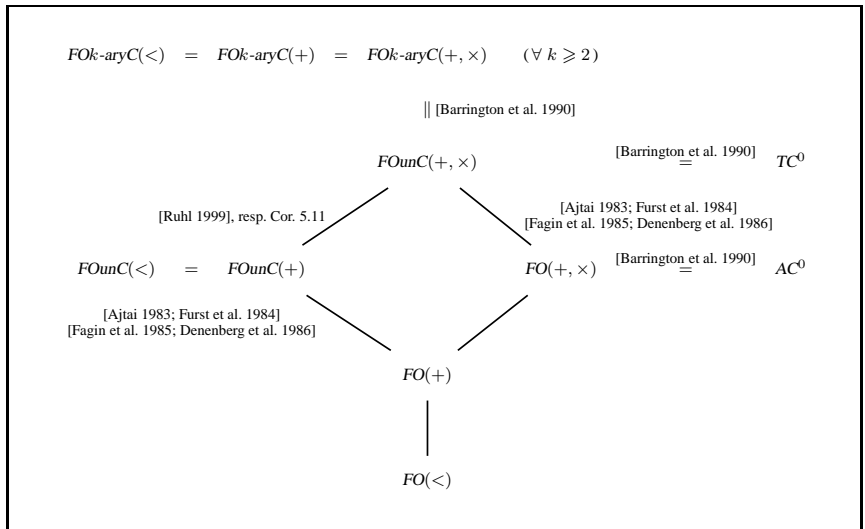


Fig. 5. Expressive power on *finite structures*. Lines indicate proper inclusions.

If  $x_0 + y_0 \leq N$ , then  $x_0 + y_0 = z_1 \cdot (N+1) + z_0$  iff  $z_1 = 0$  and  $z_0 = x_0 + y_0$ . Otherwise, we have  $N+1 \leq x_0 + y_0 < 2 \cdot (N+1)$ , and hence there are  $u, v \in \underline{N}$  such that  $x_0 + u = N$  and  $u + v = y_0 - 1$ . Thus  $x_0 + y_0 = x_0 + u + 1 + v = (N+1) + v$ . Hence,  $x_0 + y_0 = z_1 \cdot (N+1) + z_0$  iff  $z_1 = 1$  and  $z_0 = v$ .

This can easily be expressed in  $FO(+)$ .

For  $d \geq 1$  the formula  $\varphi_+^{d+1}$  can be defined by induction: Obviously,

$$\#_N(x_d, x_{d-1}, \dots, x_0) + \#_N(y_d, y_{d-1}, \dots, y_0) = \#_N(z_{d+1}, z_d, z_{d-1}, \dots, z_0)$$

if, and only if,

there is a carry  $c \in \{0, 1\}$  such that

$$\#_N(x_{d-1}, \dots, x_0) + \#_N(y_{d-1}, \dots, y_0) = \#_N(c, z_{d-1}, \dots, z_0)$$

$$\text{and } c + x_d + y_d = z_{d+1} \cdot (N+1) + z_d.$$

The formula  $\varphi_+^{d+1}$  can now be easily defined in  $FO(+)$  by using the formulas  $\varphi_+^d$  and  $\varphi_+^1$ .

(c): By definition we have for arbitrary numbers  $x, y \in \mathbb{N}$  that  $x \equiv_n y$  iff there is some  $z \in \{0, \dots, \max(x, y)\}$  such that  $x = y + n \cdot z$  or  $y = x + n \cdot z$ . Since  $n$  is fixed,  $n \cdot z$  can be expressed by the  $n$ -fold sum  $z + \dots + z$ . When considering  $d$ -tuples representing the numbers  $x, y$ , then  $z$  can be represented by a  $d$ -tuple, too. By applying (b), the  $n$ -fold sum of those  $d$ -tuples can be expressed in  $FO(+)$ . This gives us the desired formula  $\varphi_{\equiv_n}^d$ .

Since the proof of part (d) is a bit lengthy, let us first concentrate on

(e): For  $y \in \underline{N}$  and  $\vec{x} := (x_{d-1}, \dots, x_0) \in (\underline{N})^d$  the formula  $\varphi_{\text{Bit}}^d(\vec{x}, y)$  shall express that the  $y$ -th bit in the binary representation of  $\#_N(\vec{x})$  is 1.

Because of  $\#_N(\vec{x}) := \sum_{i=0}^{d-1} x_i (N+1)^i < (N+1)^d$ , the  $y$ -th bit of  $\#_N(\vec{x})$  can be 1 only if  $y < d \cdot \lg(N+1)$ . For  $y < d \cdot \lg(N+1)$  let  $y = y_1 + \dots + y_d$  where  $y_i < \lg(N+1)$ , and let  $z_i := 2^{y_i} \in \underline{N}$  for  $i \in \{1, \dots, d\}$ . The  $y$ -th Bit of  $\#_N(\vec{x})$  is 1 iff  $\left\lfloor \frac{\#_N(\vec{x})}{2^y} \right\rfloor = \left\lfloor \frac{\#_N(\vec{x})}{2^{y_1} \dots 2^{y_d}} \right\rfloor = \left\lfloor \frac{\#_N(\vec{x})}{z_1 \dots z_d} \right\rfloor$  is odd.

Because of  $\left\lfloor \frac{a}{bc} \right\rfloor = \left\lfloor \frac{\lfloor \frac{a}{c} \rfloor}{b} \right\rfloor$  we hence obtain that the  $y$ -th Bit of  $\#_N(\vec{x})$  is 1 iff there are  $y_1, \dots, y_d, z_1, \dots, z_d \in \underline{N}$  such that  $y = y_1 + \dots + y_d$ , and  $z_i = 2^{y_i}$  for all  $i \in \{1, \dots, d\}$ , and there are  $u_{d-1}^i, \dots, u_0^i \in \underline{N}$  for all  $i \in \{0, \dots, d\}$  such that  $(u_{d-1}^0, \dots, u_0^0) = (x_{d-1}, \dots, x_0)$ , and  $\#_N(u_{d-1}^{i+1}, \dots, u_0^{i+1}) = \left\lfloor \frac{\#_N(u_{d-1}^i, \dots, u_0^i)}{z_{i+1}} \right\rfloor$  for all  $i \in \{0, \dots, d-1\}$ , and  $\#_N(u_{d-1}^d, \dots, u_0^d)$  is odd.

Making use of Theorem 3.2 and of parts (a), (b), and (d) of Theorem 3.4, this can easily be expressed by a  $FO(\text{Bit})$ -formula  $\varphi_{\text{Bit}}^d$ .

(d): The proof is by induction on  $d$ . In *Step 1* we prove the induction step from  $d$  to  $d+1$ , and in *Step 2* we concentrate the induction start for  $d = 1$ .

*Step 1:* Let  $d \geq 1$ , and assume that the formulas  $\varphi_{\times}^1$  and  $\varphi_{\times}^d$  are already available. Our aim is to construct the formula  $\varphi_{\times}^{d+1}$ .

To expose the overall idea, we consider the multiplication of two decimal numbers. For example,  $5731 \times 2293 = (5000 + 731) \times (2000 + 293) =$

$$(5000 \times 2000) + (5000 \times 293) + (731 \times 2000) + (731 \times 293).$$

In the same way for numbers  $\vec{x}, \vec{y} \in (\underline{N})^{d+1}$  it obviously holds that

$$\begin{aligned}
 \#_N(x_d, x_{d-1}, \dots, x_0) \times \#_N(y_d, y_{d-1}, \dots, y_0) &= \\
 & \left( \#_N(x_d, 0, \dots, 0) \times \#_N(y_d, 0, \dots, 0) \right) && \text{[line 1]} \\
 & + \left( \#_N(x_d, 0, \dots, 0) \times \#_N(y_{d-1}, \dots, y_0) \right) && \text{[line 2]} \\
 & + \left( \#_N(x_{d-1}, \dots, x_0) \times \#_N(y_d, 0, \dots, 0) \right) && \text{[line 3]} \\
 & + \left( \#_N(x_{d-1}, \dots, x_0) \times \#_N(y_{d-1}, \dots, y_0) \right) && \text{[line 4]}
 \end{aligned}$$

The multiplication in line 1 can be done via the formula  $\varphi_{\times}^1$  as follows: Let  $u_{2d+1}^{(1)}$  and  $u_{2d}^{(1)}$  be the numbers which satisfy  $\varphi_{\times}^1(x_d, y_d, u_{2d+1}^{(1)}, u_{2d}^{(1)})$ , and let  $u_{2d-1}^{(1)} = \dots = u_0^{(1)} = 0$ . Obviously,  $\#_N(u_{2d+1}^{(1)}, u_{2d}^{(1)}, u_{2d-1}^{(1)}, \dots, u_0^{(1)})$  is the result of the multiplication in line 1.

The multiplication in line 2 can be done as follows: The formula  $\varphi_{\times}^d$  helps to determine numbers  $u_{2d+1}^{(2)}, \dots, u_d^{(2)}$  such that  $\#_N(u_{2d+1}^{(2)}, \dots, u_d^{(2)}) = x_d \times \#_N(y_{d-1}, \dots, y_0)$ . Furthermore, let  $u_{d-1}^{(2)} = \dots = u_0^{(2)} = 0$ . Clearly,  $\#_N(u_{2d+1}^{(2)}, u_{2d}^{(2)}, u_{2d-1}^{(2)}, \dots, u_0^{(2)})$  is the result of the multiplication in line 2.

Analogously we obtain a tuple  $\vec{u}^{(3)}$  such that  $\#_N(u_{2d+1}^{(3)}, u_{2d}^{(3)}, u_{2d-1}^{(3)}, \dots, u_0^{(3)})$  is the result of the multiplication in line 3.

Furthermore,  $\varphi_{\times}^d$  directly gives us a tuple  $\vec{u}^{(4)}$  such that  $\#_N(u_{2d-1}^{(4)}, \dots, u_0^{(4)})$  is the result of the multiplication in line 4.

For the addition of the numbers  $\#_N(\vec{u}^{(1)}) + \#_N(\vec{u}^{(2)}) + \#_N(\vec{u}^{(3)}) + \#_N(\vec{u}^{(4)})$  we make use of part (b) of Theorem 3.4.

Altogether, this gives us the desired  $FO(+, \times)$ -formula  $\varphi_{\times}^{d+1}$ .

*Step 2:* We now construct the  $FO(+, \times)$ -formula  $\varphi_{\times}^1(x, y, z_1, z_0)$ , expressing that  $x \cdot y = z_1 \cdot (N+1) + z_0$ .

Let  $M := \lfloor \sqrt{N} \rfloor$ . The basic idea is the following:

1. Move over from numbers  $x \in \{0, \dots, N\}$  to their  $(M+1)$ -ary representations  $x = u_1 \cdot (M+1) + u_0$  for  $u_1, u_0 \in \{0, \dots, M\}$ . Note that this is possible for all  $x \leq N$  since  $M^2 \leq N < (M+1)^2 = M \cdot (M+1) + M + 1$ .
2. Show that this decomposition can be defined by a  $FO(+, \times)$ -formula  $\chi(x, u_1, u_0)$  which expresses that  $x = \#_M(u_1, u_0)$ .
3. Construct a formula  $\psi_{\times}^2(u_1, u_0, v_1, v_0, w_3, w_2, w_1, w_0)$  that defines the multiplication for the  $(M+1)$ -ary representations.  
I.e.,  $\psi_{\times}^2$  expresses that  $\#_M(u_1, u_0) \times \#_M(v_1, v_0) = \#_M(w_3, w_2, w_1, w_0)$ .
4. Show that  $\chi$  can be extended to a formula  $\chi'(z_1, z_0, w_3, w_2, w_1, w_0)$  which expresses that  $\#_N(z_1, z_0) = \#_M(w_3, w_2, w_1, w_0)$ .

Afterwards, the desired formula  $\varphi_{\times}^1$  can be defined as follows:

$$\begin{aligned}
 \varphi_{\times}^1(x, y, z_1, z_0) &:= \exists u_1, u_0, v_1, v_0, w_3, w_2, w_1, w_0 \left( \chi(x, u_1, u_0) \wedge \chi(y, v_1, v_0) \wedge \right. \\
 & \qquad \qquad \qquad \psi_{\times}^2(u_1, u_0, v_1, v_0, w_3, w_2, w_1, w_0) \\
 & \qquad \qquad \qquad \left. \chi'(z_1, z_0, w_3, w_2, w_1, w_0) \right).
 \end{aligned}$$

Hence it suffices to construct the formulas  $\chi$ ,  $\psi_{\times}^2$ , and  $\chi'$ .

Of course, the formula

$$\zeta_M(z) := \exists y \left( z \times z = y \wedge \forall z' \left( z' > z \rightarrow \neg \exists y' z' \times z' = y' \right) \right)$$

expresses, for underlying universe  $\{0, \dots, N\}$ , that the variable  $z$  is interpreted with the number  $M := \lfloor \sqrt{N} \rfloor$ . Consequently, the following formula  $\chi(x, u_1, u_0)$  expresses that  $x = \#_M(u_1, u_0) = u_1 \cdot (M+1) + u_0$ :

$$\chi(x, u_1, u_0) := \exists z \exists v \exists w \left( \zeta_M(z) \wedge u_1 \leq z \wedge u_0 \leq z \wedge v = u_1 \times z \wedge w = v + u_1 \wedge x = w + u_0 \right).$$

It is straightforward to obtain a formula  $\psi_{\times}^1(u, v, w_1, w_0)$  which expresses, for underlying universe  $\{0, \dots, N\}$  and interpretations of  $u, v, w_1, w_0$  in  $\{0, \dots, M\}$ , that  $u \cdot v = w_1 \cdot (M+1) + w_0$ :

$$\psi_{\times}^1(u, v, w_1, w_0) := \exists w \left( \chi(w, w_1, w_0) \wedge w = u \times v \right).$$

In the same way as in *Step 1* we obtain a formula  $\psi_{\times}^2(u_1, u_0, v_1, v_0, w_3, w_2, w_1, w_0)$  which expresses, for underlying universe  $\{0, \dots, N\}$  and interpretations of  $\vec{u}, \vec{v}, \vec{w}$  in  $\{0, \dots, M\}$ , that

$$\#_M(u_1, u_0) \times \#_M(v_1, v_0) = \#_M(w_3, w_2, w_1, w_0).$$

All that remains to do is to construct a formula  $\chi'(z_1, z_0, w_3, w_2, w_1, w_0)$  which expresses that  $\#_N(z_1, z_0) = z_1 \cdot (N+1) + z_0 = \#_M(w_3, w_2, w_1, w_0)$ .

Choose  $a_1, a_0, b_1, b_0, n_1, n_0$  such that  $z_1 = \#_M(a_1, a_0)$ ,  $z_0 = \#_M(b_1, b_0)$ , and  $N+1 = \#_M(n_1, n_0)$ . For  $z_1$  and  $z_0$  this can be ensured by the formula  $\chi$ ; for  $N+1$  it can be ensured by a straightforward variant of  $\chi$ .

Obviously,  $z_1 \cdot (N+1) + z_0 = (\#_M(a_1, a_0) \times \#_M(n_1, n_0)) + \#_M(b_1, b_0)$ . Hence,

$$\begin{aligned} z_1 \cdot (N+1) + z_0 &= \#_M(w_3, w_2, w_1, w_0) && \text{if, and only if,} \\ (\#_M(a_1, a_0) \times \#_M(n_1, n_0)) + \#_M(b_1, b_0) &= \#_M(w_3, w_2, w_1, w_0). \end{aligned}$$

This multiplication and addition of  $(M+1)$ -ary representations can be done in a straightforward way by using the formula  $\psi_{\times}^2$  and an according formula  $\psi_{+}^4$  (obtained by a variant of part (b) of Theorem 3.4). Altogether, this gives us the desired formula  $\chi'$ .

Finally, the proof of part (d) and, altogether, the proof of Theorem 3.4 is complete. ■

## REFERENCES

- AJTAI, M. 1983.  $\Sigma_1^1$ -formulae on finite structures. *Ann. Pure Appl. Logic* 24, 1–48.
- AJTAI, M. AND BEN-OR, M. 1984. A theorem on probabilistic constant depth computations. In *STOC'84: 16th Annual ACM Symposium on the Theory of Computing*. Washington, D.C., 471–474.
- ALLENDER, E. 1996. Circuit complexity before the dawn of the new millenium. In *FSTTCS'96: 16th Conference on Foundations of Software Technology and Theoretical Computer Science*. Lecture Notes in Computer Science, vol. 1180. Springer, Hyderabad, India, 1–18.
- ATSERIAS, A. 1999. Computational aspects of first-order logic on finite structures. M.S. thesis, University of California, Santa Cruz, Department of Computer Science.
- ATSERIAS, A. AND KOLAITIS, P. G. 1999. First-order logic vs. fixed-point logic in finite set theory. In *LICS'99: 14th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, Trento, Italy, 275–284.
- BARRINGTON, D. A. M., IMMERMANN, N., LAUTEMANN, C., SCHWEIKARDT, N., AND THÉRIEN, D. 2004. First-order expressibility of languages with neutral letters or: the Crane Beach conjecture. To appear in *J. Comput. Syst. Sci.* Revised version of: The Crane Beach conjecture, *LICS'01: 16th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society, Boston, Massachusetts, USA, 187–196.
- BARRINGTON, D. A. M., IMMERMANN, N., AND STRAUBING, H. 1990. On uniformity within  $NC^1$ . *J. Comput. Syst. Sci.* 41, 274–306.

- BENEDIKT, M. AND KEISLER, H. J. 1997. The expressive power of unary counters. In *ICDT'97: 6th International Conference on Database Theory*. Lecture Notes in Computer Science, vol. 1186. Springer, 291–305.
- BENNETT, J. H. 1962. On spectra. Ph.D. thesis, Princeton University, Princeton, NJ.
- BÈS, A. 2002. A survey of arithmetical definability. In *A tribute to Maurice Boffa*. Soc. Math. Belgique, 1–54. Available at <http://www.univ-paris12.fr/lac1/bes/publications.html>.
- CAMERON, P. J. 1994. *Combinatorics*. Cambridge University Press, Cambridge.
- DAWAR, A., DOETS, K., LINDELL, S., AND WEINSTEIN, S. 1998. Elementary properties of finite ranks. *Math. Log. Q.* 44, 349–353.
- DENENBERG, L., GUREVICH, Y., AND SHELAH, S. 1986. Definability by constant-depth polynomial size circuits. *Information and Control* 70, 216–240.
- DURAND, A., LAUTEMANN, C., AND MORE, M. 1998. Counting results in weak formalisms. Tech. Rep. No. 1998-14, Université de Caen, France.
- EBBINGHAUS, H.-D. AND FLUM, J. 1999. *Finite model theory*, Second ed. Springer, New York.
- ESBELIN, H.-A. AND MORE, M. 1998. Rudimentary relations and primitive recursion: a toolbox. *Theor. Comput. Sci.* 193, 129–148.
- ETESSAMI, K. 1997. Counting quantifiers, successor relations, and logarithmic space. *J. Comput. Syst. Sci.* 54, 3, 400–411. Special issue for the 10th IEEE Structure in Complexity Theory Conference, 1995.
- FAGIN, R., KLAWE, M. M., PIPPENGER, N. J., AND STOCKMEYER, L. 1985. Bounded depth, polynomial size circuits for symmetric functions. *Theor. Comput. Sci.* 36, 239–250.
- FURST, M. L., SAXE, J. B., AND SIPSER, M. 1984. Parity, circuits, and the polynomial-time hierarchy. *Math. Syst. Theor.* 17, 13–27.
- HARROW, K. 1973. Sub-elementary classes of functions and relations. Ph.D. thesis, New York University, Department of Mathematics.
- IMMERMAN, N. 1999. *Descriptive complexity*. Springer, New York.
- KOREC, I. 2001. A list of arithmetical structures complete with respect to the first-order definability. *Theor. Comput. Sci.* 257, 115–151.
- KRYNICKI, M. AND ZDANOWSKI, K. 2003. Theories of arithmetics in finite models. Manuscript.
- LAUTEMANN, C., MCKENZIE, P., SCHWENTICK, T., AND VOLLMER, H. 2001. The descriptive complexity approach to LOGCFL. *J. Comput. Syst. Sci.* 62, 629–652.
- LEE, T. 2003. Arithmetical definability over finite structures. *Math. Log. Q.* 49, 4, 385–392.
- LINDELL, S. 1995. How to define exponentiation from addition and multiplication in first-order logic on finite structures. Email note, available from [slindell@haverford.edu](mailto:slindell@haverford.edu).
- LLIMA, R. E. 1998. Counting and  $k$ -recognizability. Tech. Rep. No. 64, LLAIC1, Université d'Auvergne – Clermont 1, France. Available at <http://www.iagora.com/~espel/index.html>.
- LYNCH, J. F. 1982. Complexity classes and theories of finite models. *Math. Syst. Theor.* 15, 127–144.
- MOSTOWSKI, M. 2001. On representing concepts in finite models. *Math. Log. Q.* 47, 4, 513–523.
- PARIS, J. AND WILKIE, A. 1986. Counting  $\Delta_0$  sets. *Fundam. Math.* 127, 67–76.
- PRESBURGER, M. Warsaw, 1930. Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen in welchem die Addition als einzige Operation hervortritt. *Comptes Rendus I Congrès des Mathématiciens des Pays Slaves*.
- PUGH, W. 1994. Counting solutions to Presburger formulas: How and why. In *PLDI'94: Annual ACM SIGPLAN Conference on Programming Language Design and Implementation*. SIGPLAN Notices 29(6). Orlando, Florida, USA, 121–134.
- ROSE, H. E. 1994. *A course in number theory*, Second ed. Oxford University Press.
- RUHL, M. 1999. Counting and addition cannot express deterministic transitive closure. In *LICS'99: 14th Annual IEEE Symposium on Logic in Computer Science*. IEEE Computer Society. Trento, Italy, 326–334.
- SCHWEIKARDT, N. 2001. On the expressive power of first-order logic with built-in predicates. Ph.D. thesis, Johannes Gutenberg-Universität Mainz, Fachbereich Mathematik und Informatik. Published at Logos-Verlag, Berlin, 2002, ISBN 3-8325-0017-0.
- SMORYŃSKI, C. 1991. *Logical number theory I*. Springer.

Received November 2002; revised February 2004; accepted February 2004