Information and Computation 209 (2011) 1–19

Contents lists available at ScienceDirect

Information and Computation

journal homepage: www.elsevier.com/locate/ic

Extensions of MSO and the monadic counting hierarchy

Juha Kontinen [*,1], Hannu Niemistö, [2,3]

Department of Mathematics and Statistics, University of Helsinki, P.O. Box 68, FI-00014 Helsinki, Finland

ARTICLE INFO

Article history:
Received 21 December 2006
Revised 4 June 2009
Available online 29 September 2010

MSC:
68Q19

Keywords:
Counting hierarchy
Monadic second-order logic
Majority quantifier
Second-order generalized quantifier

ABSTRACT

In this paper we study the expressive power of the extension of first-order logic by the unary second-order majority quantifier Most^1. We consider first certain sublogics of $\mathrm{FO}(\mathrm{Most}^1)$ over unary vocabularies. We show that over unary vocabularies the logic MSO(R), where MSO is monadic second-order logic and R is the first-order Rescher quantifier, can be characterized by Presburger arithmetic, whereas the logic $\mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+}$, where R^n is the nth vectorization of R, corresponds to the Δ_0-fragment of arithmetic. Then we show that $\mathrm{FO}(\mathrm{Most}^1) \geq \mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+}$ and that, on unary vocabularies, $\mathrm{FO}(\mathrm{Most}^1)$ collapses to uniform-TC^0. Using this collapse, we show that first-order logic with the binary second-order majority quantifier is strictly more expressive than $\mathrm{FO}(\mathrm{Most}^1)$ over the empty vocabulary. On the other hand, over strings, $\mathrm{FO}(\mathrm{Most}^1)$ is shown to capture the linear fragment of the counting hierarchy. Finally we show that, over non-unary vocabularies, $\mathrm{FO}(\mathrm{Most}^1)$ can express problems complete via first-order reductions for each level of the counting hierarchy.

1. Introduction

The main goal of descriptive complexity theory is to give logical characterizations of central complexity classes. The seminal result in the field was Fagin's [2] characterization of NP in terms of problems describable in existential second-order logic ($\exists$ SO). Since then, most of the central complexity classes have been given such logical characterization. In [3] Stockmeyer defined the polynomial hierarchy (PH) and observed that full second-order logic describes exactly the problems in the polynomial hierarchy.

Fagin's characterization of NP implies that NP = coNP iff $\exists\,\mathrm{SO} \equiv \forall\,\mathrm{SO}$ on finite structures. The full logics $\exists$ SO and $\forall$ SO have turned out to be very difficult to study using techniques of finite-model theory, e.g., Ehrenfeucht–Fraïssé games. Therefore, the monadic fragments of $\exists$ SO and $\forall$ SO have been studied extensively. The hope has been that the restriction to the monadic case will yield more tractable questions [4]. For example, it was shown in [5] that the monadic second-order quantifier alternation hierarchy over the class of finite graphs is strict.

The counting hierarchy (CH) is the analogue of the polynomial hierarchy, the building block being probabilistic polynomial time (PP) instead of NP:

1. $\mathrm{C_0P} = \mathrm{P}$,
2. $\mathrm{C_{k+1}P} = \mathrm{PP}^{\mathrm{C_kP}}$,
3. $\mathrm{CH} = \bigcup_{k\in\mathbb{N}} \mathrm{C_kP}$.

* Corresponding author.
E-mail addresses: juha.kontinen@helsinki.fi (J. Kontinen), hannu.niemisto@vtt.fi (H. Niemistö).
1 Financially supported by Grants 106300 and 127661 of the Academy of Finland.
2 Financially supported by the graduate school MALJA.
3 Present address: VTT Technical Research Centre of Finland.

0890-5401/$ - see front matter
doi:10.1016/j.ic.2010.09.002

The counting hierarchy was defined by Wagner [6]. The definition above is due to Torán [7]. The class PP consists of languages L for which there is a polynomial time-bounded nondeterministic Turing machine N such that, for all inputs x, $x \in L$ iff more than half of the computations of N on input x end up accepting.

In [1] it was shown that the extension of FO by second-order majority quantifiers of all arities describes exactly the problems in the counting hierarchy. This characterization is based on the observations that the k-ary second-order existential quantifier can be defined in terms of the k-ary second-order majority quantifier Most^k and first-order logic. Further, by using both the k-ary second-order existential quantifier and Most^k, it was shown that, for $k > 1$, the k-ary second-order Rescher quantifier $\mathcal{R}^k$ is expressible in the logic $\mathrm{FO}(\mathrm{Most}^k)$.

Since it holds that

$$\mathrm{PH} \leq \mathrm{CH} \leq \mathrm{PSPACE},$$

it is a difficult task to separate the classes PH and CH. By the results in [3] and [1], this question is equivalent to the question: is $\mathrm{SO} \equiv \mathrm{FO}(\mathrm{Most}^k)_{k\in\mathbb{Z}_+}$ on finite structures. In this paper, we study the relationship of the monadic fragments of these two logics: $\mathrm{FO}(\mathrm{Most}^1)$ and MSO. The analogous approach regarding the question NP = coNP? has turned out to be fruitful before.

So, in this paper we take up the study of the expressive power of $\mathrm{FO}(\mathrm{Most}^1)$, i.e., the monadic fragment of the counting hierarchy. In [1] it was shown that $\mathrm{FO}(\mathrm{Most}^1) \geq \mathrm{MSO}(\mathrm{R})$, where R is the first-order Rescher quantifier. Since the quantifier R is not definable in MSO, this result already separates the logics $\mathrm{FO}(\mathrm{Most}^1)$ and MSO.

We consider first the expressive power of logics over unary vocabularies. Suppose that $\tau = \{P_1, \ldots, P_n\}$ is a vocabulary, where each P_i is unary, and $\mathfrak{A}$ is a τ-structure. The atomic 1-types $t(x)$ of vocabulary τ induce a partition of the universe of $\mathfrak{A}$ into 2^n many disjoint parts, the sizes of which determine $\mathfrak{A}$ up to isomorphisms. Therefore, we can encode τ-structures by 2^n-length tuples of natural numbers, and classes of τ-structures by sets of such tuples.

We begin our study with the logic MSO(R), which was shown to be a sublogic of $\mathrm{FO}(\mathrm{Most}^1)$ in [1]. We show that the logic MSO(R) can be characterized in terms of Presburger arithmetic (i.e., the semi-linear relations of $\mathbb{N}$). A natural generalization is then to allow also vectorizations of R in the logic. It turns out that the logic $\mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+}$, R^n being the nth vectorization of R, corresponds to the Δ_0-fragment of arithmetic. The proof additionally shows that

$$\mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+} \equiv \mathrm{MSO}(\mathrm{R}^2)$$

on unary vocabularies.

Coming back to the logic $\mathrm{FO}(\mathrm{Most}^1)$, we then show that

$$\mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+} \leq \mathrm{FO}(\mathrm{Most}^1).$$

On the other hand, over unary vocabularies, all $\mathrm{FO}(\mathrm{Most}^1)$-definable classes (encoded as relations over $\mathbb{N}$) turn out to be definable in the logic FO(M) over initial segments of arithmetic, where M denotes the unary first-order majority quantifier.

In [8] it was shown that the languages in the linear counting hierarchy LINCH correspond exactly to the class $\mathcal{R}^\sharp$ of so-called *counting rudimentary sets*. Also, finding a logical characterization for the class LINCH was left as an open question. Using the result in [8], we show that, on strings, $\mathrm{FO}(\mathrm{Most}^1)$ captures LINCH. Our proof follows the ideas in [9] where it was shown that MSO captures the linear-time hierarchy LINH on strings with built-in addition.

We also show that over initial segments of arithmetic the logic $\mathrm{FO}(\mathrm{Most}^1)$ is strictly more expressive than FO(M). By combining these results, and the fact that ordering and the arithmetic relations can be defined using second-order existential quantification over binary predicates in $\mathrm{FO}(\mathrm{Most}^2)$, it follows that $\mathrm{FO}(\mathrm{Most}^2)$ is strictly more expressive than $\mathrm{FO}(\mathrm{Most}^1)$ over the empty vocabulary. In the last section, we show that, over non-unary vocabularies, $\mathrm{FO}(\mathrm{Most}^1)$ can express problems complete via first-order reductions for each level of the counting hierarchy. We show that $\mathrm{FO}(\mathrm{Most}^1)$ can express a variant of the quantified boolean formula problem defined in terms of the majority quantifier.

2. Preliminaries

Vocabularies τ are finite sets consisting of relation symbols and constant symbols. All structures are assumed to be finite. The universe of a structure $\mathfrak{A}$ is denoted by $\mathrm{Dom}(\mathfrak{A})$. The class of all τ-structures is denoted by $\mathrm{Mod}(\tau)$. For a logic $\mathcal{L}$, the set of τ-formulas of $\mathcal{L}$ is denoted by $\mathcal{L}[\tau]$. If φ is a τ-sentence, then the class of τ-models of φ is denoted by $\mathrm{Mod}(\varphi)$. For logics $\mathcal{L}$ and $\mathcal{L}'$, we write $\mathcal{L} \leq \mathcal{L}'$ if for all vocabularies τ (unless otherwise specified), and all sentences $\varphi \in \mathcal{L}[\tau]$ there is a sentence $\varphi' \in \mathcal{L}'[\tau]$ such that $\mathrm{Mod}(\varphi) = \mathrm{Mod}(\varphi')$. We write $\mathcal{L} \equiv \mathcal{L}'$, if $\mathcal{L} \leq \mathcal{L}'$ and $\mathcal{L}' \leq \mathcal{L}$. The set of natural numbers is denoted by $\mathbb{N}$ and $\mathbb{N}^*$ (also $\mathbb{Z}_+$) denotes the set $\mathbb{N}\backslash\{0\}$. For an alphabet Σ, Σ^* denotes the set of all finite strings over Σ and $\Sigma^+ = \Sigma^*\backslash\{\lambda\}$ denotes the set of strings with positive length.

In the following, we characterize certain logics over unary vocabularies in terms of fragments of arithmetic. Over unary vocabularies, structures can be identified up to isomorphisms with certain vectors of natural numbers. For a vocabulary τ, we denote by $S_k(\tau)$ the set of all atomic k-types over the vocabulary τ, i.e., complete consistent sets of quantifier-free formulas in k variables over τ. Suppose that τ is a vocabulary containing only unary relation symbols. For a τ-structure $\mathfrak{A}$ define

$$c^{\mathfrak{A}} = (c_t^{\mathfrak{A}})_{t \in S_1(\tau)}$$

where $c_t^{\mathfrak{A}} = |\{a \in \mathrm{Dom}(\mathfrak{A}) \mid \mathfrak{A} \models t(a)\}|$. It is easy to verify that the sequence $c^{\mathfrak{A}}$ determines the structure $\mathfrak{A}$ up to isomorphisms. On the other hand, over non-unary vocabularies, structures cannot in general be encoded in such a succint way as above. In particular, structures, considered as inputs to Turing machines, are assumed to be ordered. Let $\tau = \{<, R_1, \ldots, R_s, c_1, \ldots, c_m\}$ be a vocabulary, where $<$ is always interpreted as an ordering of the universe. Fix a τ-structure $\mathfrak{A}$. We may assume that $\mathrm{Dom}(\mathfrak{A}) = \{0, \ldots, n-1\}$ for some n. Now each relation $R_i^{\mathfrak{A}}$ can be encoded by a binary string of length n^{r_i}, where r_i is the arity of R_i, such that "1" in a given position indicates that the corresponding tuple in the lexicographic ordering of $\mathrm{Dom}(\mathfrak{A})^{r_i}$ is in $R_i^{\mathfrak{A}}$. Similarly, the interpretation of a constant c_i is encoded by the string of length $\lceil \log n \rceil$ corresponding to the number $c_i^{\mathfrak{A}}$ in binary. The binary encoding $\mathrm{bin}(\mathfrak{A})$ of a structure $\mathfrak{A}$ is defined as the concatenation of the bit strings coding its relations and constants. In the case τ contains no relation symbols, we augment τ by a dummy unary relation symbol which is always intepreted by the emptyset. This ensures that $|\mathrm{bin}(\mathfrak{A})| \geq |\mathrm{Dom}(\mathfrak{A})|$.

Given a class K of ordered structures, we write

$$L_K = \{\mathrm{bin}(\mathfrak{A}) \mid \mathfrak{A} \in K\}$$

for the language corresponding to K. Now that we have encoded classes of structures to languages over alphabet $\{0, 1\}$, we define what it means for a logic to capture a complexity class. We say that a logic $\mathcal{L}$ captures a complexity class C, $\mathcal{L} \equiv C$, if for all τ of the form $\{<, R_1, \ldots, R_s, c_1, \ldots, c_m\}$, and all classes K of τ-structures,

$$L_K \in C \text{ iff } K = \mathrm{Mod}(\varphi) \text{ for some } \varphi \in \mathcal{L}[\tau]. \tag{1}$$

For a complexity class C, we denote by $C[\tau]$ the family of classes K of τ-structures for which $L_K \in C$. In Section 8 we show that the logic $\mathrm{FO}(\mathrm{Most}^1)$ captures the linear analogue of the counting hierarchy on unary vocabularies, i.e., the equivalence in (1) is shown to hold in the case $\tau = \{<, P_1, \ldots, P_m\}$, where each P_i is unary.

2.1. Generalized quantifiers

We study logics defined in terms of generalized quantifiers. Any class of relational structures, which is closed under isomorphisms, can be turned into a first-order generalized quantifier [10]. To take an example, suppose that $\tau = \{P\}$ is a vocabulary where P is a unary predicate symbol. Let K be the following class of τ-structures

$$K = \{(M, A) \mid A \subseteq M \text{ and } |A| \text{ is even}\}$$

Now the class K gives rise to the Lindström quantifier Q_{even} expressing even cardinality via the following semantics

$$\mathfrak{A} \models Q_{\mathrm{even}} x\, \varphi(x) \Leftrightarrow (\mathrm{Dom}(\mathfrak{A}), \varphi^{\mathfrak{A}}) \in K,$$

where $\varphi^{\mathfrak{A}} = \{a \in \mathrm{Dom}(\mathfrak{A}) \mid \mathfrak{A} \models \varphi(a)\}$.

We say that a quantifier Q, over vocabulary τ, is definable in a logic $\mathcal{L}$ if $Q = \mathrm{Mod}(\varphi)$ for some sentence $\varphi \in \mathcal{L}[\tau]$. An important example of a quantifier not definable in FO is the first-order Rescher quantifier R:

$$\mathfrak{A} \models \mathrm{R}\, x, y\, (\varphi, \psi) \Leftrightarrow |\varphi^{\mathfrak{A}}| > |\psi^{\mathfrak{A}}|.$$

We shall also consider vectorizations of the quantifier R. The nth vectorization of R is a quantifier which binds two n-ary formulas with the following semantics:

$$\mathfrak{A} \models \mathrm{R}^n\, \bar{x}, \bar{y}\, (\psi_0(\bar{x}), \psi_1(\bar{y})) \iff |\psi_0^{\mathfrak{A}}| > |\psi_1^{\mathfrak{A}}|.$$

We need also the first-order majority quantifier M, defined as

$$\mathfrak{A} \models \mathrm{M}\, x\, \psi(x) \iff |\psi^{\mathfrak{A}}| > |\mathrm{Dom}(\mathfrak{A})|/2.$$

In the presence of linear order, R is definable by M.

The notion of a second-order generalized quantifier [11] can be defined analogously to the first-order case. Formally, second-order quantifiers correspond to certain classes of second-order structures which are closed under isomorphisms. We refer to [11] for details. Let us look at some examples instead. The familiar k-ary second-order existential quantifier can be also defined as a generalized quantifier:

$$\mathfrak{A} \models \exists X \varphi(X) \Leftrightarrow \varphi^{\mathfrak{A}} \neq \emptyset,$$

where $\varphi^{\mathfrak{A}} = \{X \subseteq M^k \mid \mathfrak{A} \models \varphi(X)\}$. The k-ary second-order majority quantifier Most^k is defined by:

$$\mathfrak{A} \models \text{Most}^k X\varphi(X) \Leftrightarrow |\varphi^{\mathfrak{A}}| > 2^{|\text{Dom}(\mathfrak{A})|^k - 1}.$$

The k-ary second-order Rescher quantifier $\mathcal{R}^k$ is defined by:

$$\mathfrak{A} \models \mathcal{R}^k X, Y\, (\psi(X), \phi(Y)) \Leftrightarrow |\psi^{\mathfrak{A}}| > |\phi^{\mathfrak{A}}|.$$

A notion of definability can also be formulated for second-order generalized quantifiers [12]. For the purposes of this paper, it suffices to note that definability of a quantifier $\mathcal{Q}$ in a logic $\mathcal{L}$ gives us a uniform way to express $\mathcal{Q}$ in $\mathcal{L}$. The following definability results were shown to hold in [1]:

Fact 2.1

1. *The k-ary second-order existential quantifier is definable in* $\text{FO}(\text{Most}^k)$.
2. *If $k > 1$, then $\mathcal{R}^k$ is definable in* $\text{FO}(\text{Most}^k)$.
3. *The first-order Rescher quantifier* R *is definable in* $\text{FO}(\text{Most}^1)$.

It is an open question whether $\mathcal{R}^1$ is definable in the logic $\text{FO}(\text{Most}^1)$.

3. Arithmetic

We call the first-order theory of the natural numbers with addition, $\langle \mathbb{N}, + \rangle$, *Presburger arithmetic*. The canonical ordering $\leq$ and the relations $\equiv_p$ for all $p > 1$, where $a \equiv_p b \iff p \mid b - a$, are clearly definable in this theory. The theory is decidable by the following theorem [13].

Theorem 3.1. *First-order logic has quantifier elimination on* $\langle \mathbb{N}, +, \leq, 0, 1, (\equiv_p)_{p \in \mathbb{Z}_+} \rangle$.

When we add multiplication to the structure, even existential first-order formulas can define all recursively enumerable sets. One way to restrict the expressive power, is to allow only bounded quantifications.

Lemma 3.2. *Let R be a k-ary relation on $\mathbb{N}$. The following are equivalent:*

(a) *R is definable on $\langle \mathbb{N}, \leq, +, \times \rangle$ by a first-order formula $\varphi(\bar{x})$, whose all quantifications are of the form $(\exists v \leq t)\psi$, where t is a term.*
(b) *R is definable on $\langle \mathbb{N}, \leq, +, \times \rangle$ by a first-order formula $\varphi(\bar{x})$, whose all quantifications are of the form $(\exists v \leq u)\psi$, where u is a variable and whose atomic formulas are of the form $x + y = z$, $xy = z$ or $x = y$.*
(c) *There exists a first-order formula φ such that for all n, φ defines the relation $R \cap n^k$ on $\langle n, +', \times' \rangle$, where $+'$ and $\times'$ are the graphs of $+$ and $\times$ relativized to n.*

Proof. The implication (b) $\Rightarrow$ (a) and the equivalence (b) $\iff$ (c) are rather trivial. In order to prove the implication (a) $\Rightarrow$ (b), we need to code numbers in the form $u_0 + u_1 v + \cdots + u_k v^k$, where v is the maximum input variable and k depends on the terms t bounding the quantifications in (a). Complex terms can be transformed into three atomic formulas by adding existential quantifiers (see [14] for details). $\square$

We call a first-order formula a Δ_0-*formula*, if it satisfies the condition (a) of Lemma 3.2. Relations satisfying one of the conditions are called *rudimentary*. We may also define Δ_0-fragment of any other logic on arithmetic as in the condition (c).

4. MSO(R) and Presburger arithmetic

Let τ be a finite vocabulary containing only unary relation symbols. Recall that $S_k(\tau)$ is the set of all atomic k-types over the vocabulary τ. Given a formula ψ, let $\tau(\psi)$ be the set of all relation symbols occurring in ψ and given a structure $\mathfrak{A}$, let $\tau(\mathfrak{A})$ be the vocabulary of $\mathfrak{A}$.

Denote the first-order formula $\forall x(Ux \to Vx)$ by $U \subseteq V$ and the formula $\exists x(Ux \wedge \forall y(Uy \to x = y))$ by $|U| = 1$.

We consider in this section the expressive power of MSO(R) on $\text{Mod}(\tau)$ and show that it corresponds to Presburger arithmetic. The first step is to prove that first-order quantifiers of the logic can be pushed inwards behind the second-order quantifiers.

Lemma 4.1. *Let $\mathcal{Q}$ be a set of first-order quantifiers. Every* $\mathrm{MSO}(\mathcal{Q})[\tau]$*-formula* $\phi(x_0, \ldots, x_{n-1})$ *is equivalent to a* $\mathrm{MSO}(\mathcal{Q})[\tau]$*-formula* $\psi(U_{x_0}, \ldots, U_{x_{n-1}})$ *without free first-order variables such that for all* $\mathfrak{A}$ *and* $a_0, \ldots, a_{n-1} \in \mathrm{Dom}(\mathfrak{A})$

$$\mathfrak{A} \models \phi(a_0, \ldots, a_{n-1}) \Leftrightarrow \mathfrak{A} \models \psi(\{a_0\}, \ldots, \{a_{n-1}\}),$$

and in $\psi(U_{x_0}, \ldots, U_{x_{n-1}})$ *first-order quantifiers occur only as part of the following subformulas:* $U \subseteq V$, $|U| = 1$ *or* $Q\overline{x}^0, \ldots, \overline{x}^{k-1}(\psi_0(\overline{x}^0), \ldots, \psi_{k-1}(\overline{x}^{k-1}))$*, where* $Q \in \mathcal{Q}$ *and every formula* ψ_i *is quantifier-free.*

Proof. We first define a transformation $[x \mapsto U_x]$ for $\mathrm{MSO}(\mathcal{Q})[\tau]$-formulas that replaces all free occurrences of x in a formula by a new unary relation U_x in the following way:

$$\begin{aligned}(x = y)[x \mapsto U_x] &\equiv U_x y\\ (Vx)[x \mapsto U_x] &\equiv U_x \subseteq V.\end{aligned}$$

The transformation $[x \mapsto U_x]$ is defined trivially on the connectives. For a tuple $\overline{x}$ of first-order variables occurring free in ϕ, we denote by $\phi_{\overline{x} \mapsto \overline{U}}$ the formula from which all the variables in $\overline{x}$ have been eliminated by a repeated application of the operation $[x \mapsto U_x]$. Note that the order in which the variables are eliminated using the operation $[x \mapsto U_x]$ does not matter modulo logical equivalence. In particular, we can transform any formula $\phi(\overline{x}) \in \mathrm{MSO}(\mathcal{Q})[\tau]$ into a formula $\phi_{\overline{x} \mapsto \overline{U}}$ without free first-order variables such that for all $\mathfrak{A}$ and $a_0, \ldots, a_{n-1} \in \mathrm{Dom}(\mathfrak{A})$

$$\mathfrak{A} \models \phi(a_0, \ldots, a_{n-1}) \Leftrightarrow \mathfrak{A} \models \phi_{\overline{x} \mapsto \overline{U}}(\{a_0\}, \ldots, \{a_{n-1}\}),$$

that is, $\phi_{\overline{x} \mapsto \overline{U}}$ satisfies the first requirement of the lemma. In order to satisfy the required structural properties, we need to define a further transformation $\psi \mapsto \psi'$ (applying to formulas $\phi_{\overline{x} \mapsto \overline{U}}$, for $\varphi(\overline{x}) \in \mathrm{MSO}(\mathcal{Q})[\tau]$) in the following way. For ψ of the form $U \subseteq V$ or $\neg(U \subseteq V)$, $\psi' := \psi$, and in the remaining cases the transformation is defined in the following way:

$$\begin{aligned}&\left(Q\overline{x}^0, \ldots, \overline{x}^{k-1}\left(\psi_0(\overline{x}^0), \ldots, \psi_{k-1}(\overline{x}^{k-1})\right)\right)' \equiv\\ &\qquad \bigvee_{\substack{I_0 \subseteq S_{|\overline{x}^0|}(\tau(\psi_0))\\ \vdots\\ I_{k-1} \subseteq S_{|\overline{x}^{k-1}|}(\tau(\psi_{k-1}))}} \left(\left[\forall \overline{x}^0\left(\psi_0(\overline{x}^0) \leftrightarrow \bigvee_{t \in I_0} t(\overline{x}^0)\right)\right]' \wedge\right.\\ &\qquad\qquad \cdots \wedge \left[\forall \overline{x}^{k-1}\left(\psi_{k-1}(\overline{x}^{k-1}) \leftrightarrow \bigvee_{t \in I_{k-1}} t(\overline{x}^{k-1})\right)\right]'\\ &\qquad\qquad \left.\wedge Q\overline{x}^0, \ldots, \overline{x}^{k-1}\left(\bigvee_{t \in I_0} t(\overline{x}^0), \ldots, \bigvee_{t \in I_{k-1}} t(\overline{x}^{k-1})\right)\right)\\ &(\exists X \theta(X))' \equiv \exists X \theta(X)'\\ &(\exists x \theta(x))' \equiv \exists U_x((\theta[x \mapsto U_x])' \wedge |U_x| = 1)\\ &(\neg\theta)' \equiv \neg\theta' \qquad \text{if the sentence is not of the form } U \subseteq V\\ &(\theta \wedge \gamma)' \equiv \theta' \wedge \gamma'\end{aligned}$$

We can now prove using induction on the structure of $\phi(\overline{x}) \in \mathrm{MSO}(\mathcal{Q})[\tau]$ that $\phi_{\overline{x} \mapsto \overline{U}}$ and $(\phi_{\overline{x} \mapsto \overline{U}})'$ are equivalent. If ϕ is an atomic formula, then there is nothing to prove since $\phi_{\overline{x} \mapsto \overline{U}} = (\phi_{\overline{x} \mapsto \overline{U}})'$. The induction is also trivial for the boolean connectives and for the monadic second-order existential quantifier. Suppose that φ is of the form $\exists x \theta(x, \overline{y})$. Let $\mathfrak{A}$ be a model and $\mathfrak{A} \models (\exists x \theta(x, \overline{y}))_{\overline{y} \mapsto \overline{U}}$. By definition $(\exists x \theta(x, \overline{y}))_{\overline{y} \mapsto \overline{U}} = \exists x \theta_{\overline{y} \mapsto \overline{U}}(x)$, hence $\mathfrak{A} \models \theta_{\overline{y} \mapsto \overline{U}}(a)$ for some $a \in \mathrm{Dom}(\mathfrak{A})$. Therefore it holds that

$$\mathfrak{A} \models \theta_{\overline{y} \mapsto \overline{U}}[x \mapsto U_x](\{a\})$$

and, by the induction assumption, that

$$\mathfrak{A} \models \exists U_x((\theta_{\overline{y} \mapsto \overline{U}}[x \mapsto U_x])' \wedge |U_x| = 1).$$

The other direction is analogous. Finally, note that the correctness of the translation of the generalized quantifier Q follows from the fact that, over unary vocabularies, if two sequences of elements have the same atomic type, there exists an automorphism of the structure mapping one sequence to another. Therefore, every definable relation is already definable by a quantifier-free formula.

We have now shown that for all $\phi(\overline{x}) \in \mathrm{MSO}(\mathcal{Q})[\tau]$ the formulas $\phi_{\overline{x}\mapsto\overline{U}}$ and $(\phi_{\overline{x}\mapsto\overline{U}})'$ are equivalent and hence $\phi(\overline{x})$ and $(\phi_{\overline{x}\mapsto\overline{U}})'$ satisfy the first requirement of the lemma. A similar induction shows that $(\phi_{\overline{x}\mapsto\overline{U}})'$ satisfies the required structural properties. □

Theorem 4.2. *Given a sentence $\varphi \in \mathrm{MSO}(\mathrm{R})[\tau]$, there exists a formula $\varphi^*((x_t)_{t\in S_1(\tau)}) \in \mathrm{FO}[\{+\}]$ such that for all $\mathfrak{A} \in \mathrm{Mod}(\tau)$, $\mathfrak{A} \models \varphi$ if and only if $\langle \mathbb{N}, +\rangle \models \varphi^*(c^{\mathfrak{A}})$.*

Proof. We may assume φ is in the form of Lemma 4.1. The claim of the theorem holds for the formulas $U \subseteq V$, $|U| = 1$ and $\mathrm{R}\,xy(\psi_0(x), \psi_1(y))$, where ψ_0 and ψ_1 are quantifier-free. We let

$$\begin{aligned}
(U \subseteq V)^*((x_t)_{t\in S_1(\tau)}) &\equiv \bigwedge_{\substack{t\in S_1(\tau)\\ Ux,\neg Vx\in t}} x_t = 0,\\
(|U| = 1)^*((x_t)_{t\in S_1(\tau)}) &\equiv \sum_{\substack{t\in S_1(\tau)\\ Ux\in t}} x_t = 1, \text{ and}\\
(\mathrm{R}\,uv(\psi_0(u), \psi_1(v)))^*((x_t)_{t\in S_1(\tau)}) &\equiv \sum_{\substack{t\in S_1(\tau)\\ \psi_0\in t}} x_t > \sum_{\substack{t\in S_1(\tau)\\ \psi_1\in t}} x_t.
\end{aligned}$$

If we consider a subformula of φ that is not a subformula of one of these formulas, then it does not have free first-order variables and thus we can prove the theorem by induction. If a $\tau \cup \{U\}$-sentence θ satisfies the theorem and $\varphi \equiv \exists U\theta(U)$, we may put

$$\varphi^*((x_t)_{t\in S_1(\tau)}) \equiv (\exists z_t \leq x_{t\restriction\tau})_{t\in S_1(\tau\cup\{U\})} \left(\theta^*(\overline{z}) \wedge \bigwedge_{t\in S_1(\tau)} z_{t\wedge Uv} + z_{t\wedge\neg Uv} = x_t\right),$$

where $t \wedge Uv$ denotes the unique atomic type on $\tau \cup \{U\}$ extending t and containing Uv and similarly for $t \wedge \neg Uv$. The induction is trivial for connectives. □

Theorem 4.2 has also the following converse showing that we need the whole expressive power of Presburger arithmetic.

Theorem 4.3. *For every formula $\varphi(\overline{x}) \in \mathrm{FO}[\{+\}]$, there exists a sentence $\varphi^* \in \mathrm{MSO}(\mathrm{R})[\overline{U}]$, $|\overline{U}| = |\overline{x}| = n$, such that for all $[\overline{U}]$-structures $\mathfrak{A}$,*

$$\langle \mathbb{N}, +\rangle \models \varphi(|U_0^{\mathfrak{A}}|, \ldots, |U_{n-1}^{\mathfrak{A}}|) \iff \mathfrak{A} \models \varphi^*.$$

Proof. By Theorem 3.1, we may assume that $\varphi(\overline{x})$ is a quantifier-free $\{+, \leq, 0, 1\} \cup \{\equiv_p \mid p \in \mathbb{Z}_+\}$-formula. If the claim of the theorem holds for formulas θ and γ it clearly holds for $\theta \wedge \gamma$ and $\neg\theta$. Thus it suffices to consider only atomic formulas (atomic in the vocabulary $\{+, \leq, 0, 1\} \cup \{\equiv_p \mid p \in \mathbb{Z}_+\}$).

Every atomic formula can be written as $x_{i_0} + \cdots + x_{i_{l-1}} + c \bowtie x_{j_0} + \cdots + x_{j_{m-1}} + d$, where $\bowtie$ is one of the relations $=$, $\leq$, or $\equiv_p$ and c and d are constant natural numbers. We write this as

$$\exists U_{i_l} U_{j_m} (|U_{i_l}| = c \wedge |U_{j_m}| = d \wedge |U_{i_0}| + \cdots + |U_{i_l}| \bowtie |U_{j_0}| + \cdots + |U_{j_m}|),$$

where i_l and j_m are different from the indices i_k, $k < l$ and j_k, $k < m$. Subformulas $|U_{i_l}| = c$ and $|U_{j_m}| = d$ are first-order expressible so our goal now is to write a MSO(R)-sentence that expresses

$$|U_{i_0}| + \cdots + |U_{i_l}| \bowtie |U_{j_0}| + \cdots + |U_{i_m}|. \tag{2}$$

If $\bowtie$ is $\leq$, we write (2) as

$$\begin{aligned}
\exists V_0 \ldots V_l W_0 \ldots W_m &\left(\bigwedge_{0\leq k\leq l} |U_{i_k}| = |V_k| \wedge \bigwedge_{0\leq k\leq m} |U_{j_k}| = |W_k| \right.\\
&\left.\wedge \forall x(|\{k \leq l \mid V_k x\}| \leq |\{k \leq m \mid W_k x\}|)\right).
\end{aligned}$$

To overcome the problem of sums being greater than the size of the model in (2), the idea is to move the sets $U_{i_0}, \ldots, U_{i_l}$ ($U_{j_0}, \ldots, U_{i_m}$) on top of each other by the sets $V_0, \ldots, V_l$ ($W_0, \ldots, W_m$) so that (2) can be expressed by comparing the cardinalities of the sets $\{k \le l \mid V_k x\}$ and $\{k \le m \mid W_k x\}$ elementwise. Above, subformulas $|U_{i_k}| = |V_k|$ are expressible using the Rescher quantifier and $|\{k \le l \mid V_k x\}| \le |\{k \le m \mid W_k x\}|$ can be written as a quantifier-free formula.

If $\bowtie$ is $=$, we can express (2) by using the previous formula and the fact that $x = y \iff x \le y \wedge y \le x$.

Finally, suppose, $\bowtie$ is $\equiv_p$. We write (2) now as

$$\bigvee \left\{ \bigwedge_{0 \le k \le l} |U_{i_k}| \equiv_p a_k \wedge \bigwedge_{0 \le k \le m} |U_{j_k}| \equiv_p b_k \right| \\ a_0, \ldots, a_l, b_0, \ldots, b_m \in \{0, \ldots, p-1\}, \sum_{k=0}^{l} a_k \equiv_p \sum_{k=0}^{m} b_k \right\},$$

where $|U| \equiv_p a$ can be written as

$$\exists V_0 \ldots V_p \left(U = \bigcup_{k=0}^{p} V_k \wedge \bigwedge_{0 \le k < k' \le p} V_k \cap V_{k'} = \emptyset \wedge \bigwedge_{0 \le k < k' < p} |V_k| = |V_{k'}| \wedge |V_p| = a \right). \quad \square$$

5. Vectorized Rescher quantifiers

As before, let τ be a finite vocabulary containing only unary relation symbols. We extend the result of the previous section and show that when MSO is extended with the vectorizations of the Rescher quantifier, the expressive power of the logic corresponds to Δ_0-arithmetic on unary vocabularies.

Lemma 5.1. *For every $s \in S_k(\tau)$, there exists a polynomial $p_s((x_t)_{t \in S_1(\tau)})$ such that for all τ-structures $\mathfrak{A}$, s has $p_s(c^{\mathfrak{A}})$ realizations in $\mathfrak{A}$.*

Proof. Let $s(\bar{x})$ be an arbitrary atomic k-type on τ. If $x_i = x_j \in s$ and $i \neq j$, then s has as many realizations as a type where the variable x_j and all formulas containing it are removed. Therefore, we may consider only types containing the formula $x_i \neq x_j$ for all $i \neq j$.

Since τ contains only unary relation symbols, a sequence $\bar{a}$ satisfies s if and only if every element of a_i satisfies the right 1-type. Suppose that the number of the elements a_i that need to satisfy the same type $t \in S_1(\tau)$ is m_t. We may now put

$$p_s((\bar{z}_t)_{t \in S_1(\tau)}) = \prod_{t \in S_1(\tau)} \prod_{i=0}^{m_t - 1} (z_t - i). \quad \square$$

Theorem 5.2. *Given a sentence $\varphi \in \mathrm{MSO}(\mathrm{R}^n)_{n \in \mathbb{Z}_+}[\tau]$, there exists a Δ_0-formula $\varphi^*((x_t)_{t \in S_1(\tau)})$ such that for all $\mathfrak{A} \in \mathrm{Mod}(\tau)$, $\mathfrak{A} \models \varphi$ if and only if $\langle \mathbb{N}, +, \times \rangle \models \varphi^*(c^{\mathfrak{A}})$.*

Proof. The proof is identical to the proof of Theorem 4.2 except that, we now have to find a translation for $\varphi \equiv \mathrm{R}^k\, \bar{x}, \bar{y}(\psi_0(\bar{x}), \psi_1(\bar{y}))$, where $\psi_j(\bar{x}) \equiv \bigvee_{s \in I_j} s(\bar{x})$ for $j \in \{0, 1\}$ and $I_j \subseteq S_k(\tau)$. A suitable translation is

$$\varphi^*((x_t)_{t \in S_1(\tau)}) \equiv \sum_{s \in I_0} p_s^+((x_t)_{t \in S_1(\tau)}) + \sum_{s \in I_1} p_s^-((x_t)_{t \in S_1(\tau)}) \\ > \sum_{s \in I_0} p_s^-((x_t)_{t \in S_1(\tau)}) + \sum_{s \in I_1} p_s^+((x_t)_{t \in S_1(\tau)}),$$

where p_s^+ is the sum of all positive terms of the polynomial p_s and p_s^- is the sum of negative terms. Note, that the translations of the other formulas are already written in the proof of Theorem 4.2 so that quantifications are bounded. $\square$

The following lemma is similar to the observation of [15] that addition and multiplication are definable by the second vectorization M^2 of the majority quantifier on ordered structures.

Lemma 5.3. *If U_0, U_1 and U_2 are unary relation symbols, then $|U_0^{\mathfrak{A}}| + |U_1^{\mathfrak{A}}| = |U_2^{\mathfrak{A}}|$ and $|U_0^{\mathfrak{A}}| \cdot |U_1^{\mathfrak{A}}| = |U_2^{\mathfrak{A}}|$ are expressible in* $\mathrm{MSO}(\mathrm{R}^2)$.

Proof. We can express $|U_0^{\mathfrak{A}}| + |U_1^{\mathfrak{A}}| > |U_2^{\mathfrak{A}}|$ as

$$\exists z_0 z_1 (z_0 \neq z_1 \wedge \mathrm{R}^2\, x_0 x_1, y_0 y_1 ((x_0 = z_0 \wedge U_0 x_1) \vee (x_0 = z_1 \wedge U_1 x_1), y_0 = y_1 \wedge U_2 y_0))$$

and $|U_0^{\mathfrak{A}}| \cdot |U_1^{\mathfrak{A}}| > |U_2^{\mathfrak{A}}|$ as

$$\mathrm{R}^2\, x_0 x_1, y_0 y_1 (U_0 x_0 \wedge U_1 x_1, y_0 = y_1 \wedge U_2 y_0).$$

By changing the subformulas of the Rescher quantifiers, we may reverse the inequalities. We get the desired equations by combining the inequalities. □

Theorem 5.4. *For every Δ_0-formula $\varphi(\overline{x})$, there exists a sentence $\varphi^* \in \mathrm{MSO}(\mathrm{R}^2)[\{\overline{U}\}]$, $|\overline{U}| = |\overline{x}| = n$, such that for all $\{\overline{U}\}$-structures $\mathfrak{A}$,*

$$\langle \mathbb{N}, +, \times \rangle \models \varphi \left(|U_0^{\mathfrak{A}}|, \ldots, |U_{n-1}^{\mathfrak{A}}| \right) \iff \mathfrak{A} \models \varphi^*.$$

Proof. By Lemma 3.2, we may assume all quantifications in φ are of the form $\exists (x \leq y)\psi$ and all atomic formulas are of the form $x = y$, $x + y = z$ or $xy = z$. We get the $\mathrm{MSO}(\mathrm{R}^2)$-sentence satisfying the theorem by replacing every first-order quantification $\exists(x_i \leq x_j)\psi$ by the monadic second-order quantification $\exists X_i(|X_i| \leq |X_j| \wedge \psi)$, and every atomic formula by the corresponding formula defined in Lemma 5.3. □

Corollary 5.5. $\mathrm{MSO}(\mathrm{R}^n)_{n \in \mathbb{Z}_+} \equiv \mathrm{MSO}(\mathrm{R}^2)$ *on unary vocabularies.*

It is interesting to note that, by Theorem 4.2 (and the computability of the map $\varphi \mapsto \varphi^*$ in the theorem), the set of satisfiable MSO(R) sentences over unary vocabularies is decidable. On the other hand, by Theorem 5.4, the set of satisfiable $\mathrm{MSO}(\mathrm{R}^2)$ sentences is undecidable already over the empty vocabulary by considering an arbitrary Δ_0-formula $\varphi(x)$, and substituting U_0 in the transformed sentence φ^* by $\top$.

6. Defining Rescher quantifiers in $\mathrm{FO}(\mathrm{Most}^1)$

In this section, we show that every vectorization R^n of the first-order Rescher quantifier is definable in $\mathrm{FO}(\mathrm{Most}^1)$. It follows that the logic $\mathrm{FO}(\mathrm{Most}^1)$ is at least as strong as Δ_0 over unary vocabularies and that, already over the empty vocabulary, the set of satisfiable $\mathrm{FO}(\mathrm{Most}^1)$ sentences is undecidable.

The following lemma shows that in some special cases the quantifier $\mathcal{R}^1$ can be expressed in $\mathrm{FO}(\mathrm{Most}^1)$. The general case is open.

Lemma 6.1. *Let M be a set and $G_1, G_2 \subseteq \mathcal{P}(M)$. Suppose either that*

1. *there is $a \in M$ such that $a \notin \bigcup(G_1 \cup G_2)$, or*
2. *$\forall X(X \in G_1 \cup G_2 \to |X| < |M|/2)$,*

then $|G_1| > |G_2|$ can be expressed in a uniform way in $\mathrm{FO}(\mathrm{Most}^1)$.

Proof. For case 1, define $C = \{A \subseteq M \mid a \in A\}$. Then $|C| = 2^{|M|-1}$. Now $|G_1| > |G_2|$ iff

$$|(C \backslash G_2^*) \cup G_1| > 2^{|M|-1},$$

where $G_2^* = \{X \cup \{a\} \mid X \in G_2\}$. Note that G_2^* can be defined from G_2 using monadic second-order existential quantification, i.e., $Y \in G_2^*$ iff

$$\exists X(G_2(X) \wedge \forall y(Yy \leftrightarrow (Xy \vee y = a))).$$

More formally, the above can be written as

$$\exists a \forall X((\vee_i G_i(X) \to \neg Xa) \wedge \mathrm{Most}^1\, Y\, ((Ya \wedge \neg G_2^*(Y)) \vee G_1(Y))).$$

Suppose then that G_1 and G_2 satisfy the assumption in case 2. Let $a \in M$ be arbitrary and define

$$C_i = \{X \subseteq M \mid X \in G_i \text{ and } a \notin X \text{ or } X^c \in G_i \text{ and } a \in X^c\}.$$

By the assumption in case 2, $|C_i| = |G_i|$, thus $|G_1| > |G_2|$ iff $|C_1| > |C_2|$. Note that C_1 and C_2 satisfy the assumption in case 1 with respect to $a \in M$, and C_i can be easily defined from G_i. Analogously to above, we can express $|G_1| > |G_2|$ by the formula

$$\exists a \,\mathrm{Most}^1\, Y\, ((Ya \wedge \neg C_2^*(Y)) \vee C_1(Y)). \quad \square$$

Using Lemma 6.1, every vectorization R^n of the first-order Rescher quantifier can be defined in $\mathrm{FO}(\mathrm{Most}^1)$.

Theorem 6.2. *Every vectorization* R^n *of the Rescher quantifier is definable in* $\mathrm{FO}(\mathrm{Most}^1)$.

Proof. Let S_0 and S_1 be n-ary relation symbols. In order to prove the theorem, it is sufficient to define a $\mathrm{FO}(\mathrm{Most}^1)$-sentence φ equivalent to $\mathrm{R}^n\, \overline{xy}(S_0\overline{x}, S_1\overline{y})$.

Choose an integer m such that $2^m \geq (m+n)^n$. Let $\mathrm{Bit}\colon 2^m \to \mathcal{P}(m)$ be a function such that $i \in \mathrm{Bit}(j)$ if and only if the ith bit of the binary representation of j is one.

For $j \in \{0, 1\}$, define

$$\psi_j(X, \overline{z}) = \bigvee_{0 \leq c \leq 2^m} \Bigg(\bigwedge_{i \in \mathrm{Bit}(c)} Xz_i \wedge \bigwedge_{i \in m \setminus \mathrm{Bit}(c)} \neg Xz_i \\ \wedge \exists^{>c}\overline{x}(S_j\overline{x} \;\wedge\; X \setminus [\overline{z}] \subseteq [\overline{x}] \subseteq X \cup [\overline{z}]) \Bigg),$$

where $[\overline{x}]$ denotes the set $\{x_i \mid i < |\overline{x}|\}$. Let

$$\varphi' \equiv \exists z_0, \ldots, z_{m-1} \left(\bigwedge_{0 \leq i < j < m} z_i \neq z_j \wedge \mathcal{R}^1\, XY(\psi_0(X, \overline{z}), \psi_1(Y, \overline{z})) \right),$$

where $\mathcal{R}^1$ is the unary second-order Rescher quantifier. The formula $\psi_j(X, \overline{z})$ implies in particular that $|X \setminus [\overline{z}]| \leq n$, thus if it holds, $|X| \leq n + m$. By case 2 of Lemma 6.1, the application of the quantifier $\mathcal{R}^1$ in the formula φ' is expressible in all structures of size greater than $2(n+m)$.

Let $\varphi \equiv (\theta \wedge \exists^{\leq 2(n+m)}x(x = x)) \vee (\varphi' \wedge \exists^{>2(n+m)}x(x = x))$, where θ defines the quantifier R^n on structures of size at most $2(n+m)$. We show that φ' defines the quantifier in all larger structures.

Let $\mathfrak{A}$ be a structure of size greater than $2(n+m)$ and let $\overline{b} \in (\mathrm{Dom}(\mathfrak{A}))^m$ be a sequence of distinct elements. Let $P = \{X \subseteq \mathrm{Dom}(\mathfrak{A}) \mid \mathfrak{A} \models \psi_0(X, \overline{b})\}$. For every set $Y \subseteq \mathrm{Dom}(\mathfrak{A}) \setminus [\overline{b}]$ with $|Y| \leq n$, let $S_Y = \{\overline{a} \in S_0^{\mathfrak{A}} \mid [\overline{a}] \setminus [\overline{b}] = Y\}$ and $P_Y = \{X \in P \mid X \setminus [\overline{b}] = Y\}$. The sets S_Y form a partition of $S_0^{\mathfrak{A}}$ and the sets P_Y form a partition of P.

Given $X \subseteq \mathrm{Dom}(\mathfrak{A})$, we have $\{\overline{a} \in S_0^{\mathfrak{A}} \mid X \setminus [\overline{b}] \subseteq [\overline{a}] \subseteq X \cup [\overline{b}]\} = S_Y$, where $Y = X \setminus [\overline{b}]$. Thus $\mathfrak{A} \models \exists^{>c}\overline{x}(S_0\overline{x} \wedge X \setminus [\overline{b}] \subseteq [\overline{x}] \subseteq X \cup [\overline{b}])$ if and only if $c < |S_Y|$. This gives us

$$P_Y = \{Y \cup \{b_i \mid i \in \mathrm{Bit}(c)\} \mid c < |S_Y|\}.$$

Because $|S_Y| \leq (n+m)^n \leq 2^m$, we have $|P_Y| = |S_Y|$. Hence $|P| = |S_0^{\mathfrak{A}}|$. In a similar way, we can show that $|S_1^{\mathfrak{A}}| = |\{X \subseteq \mathrm{Dom}(\mathfrak{A}) \mid \mathfrak{A} \models \psi_1(X, \overline{b})\}|$. $\square$

7. Complexity of $\mathrm{FO}(\mathrm{Most}^1)$ over unary predicates

Consider the initial segment of arithmetic $\langle n, <, +, \times\rangle$. The expressive power of FO(M) corresponds on these structures to uniform TC^0 (when n is coded in unary). There are two ways of coding integers on $\langle n, <, +, \times\rangle$. We call integers less than n^k *short* and code them as k-sequences of the elements in n:

$$S_k(m) = (m \mod n, \lfloor m/n \rfloor \mod n, \ldots, \lfloor m/n^{k-1} \rfloor \mod n).$$

The integers less than 2^{n^k} are called *long* and coded as k-ary relations:

$$L_k(m) = \{S_k(i) \mid i\text{th bit of } m \text{ is } 1\}.$$

We may also code the n^l-sequences of long integers:

$$L_{k,l}((m_i)_{i<n^l}) = \bigcup_{i<n^l} \{S_l(i)\} \times L_k(m_i).$$

Using the Bit-relation integers can be converted from short representation to long.

Theorem 7.1. *The relation* Bit*, defined as*

$$\mathrm{Bit}(S_k(a), S_l(b)) \iff S_k(a) \in L_k(b),$$

is rudimentary.

Define the operations Sum, Product, Division, Iterated-Sum and Iterated-Product as follows:

$$\begin{aligned}
S_{k+1}(i) \in \mathrm{Sum}(L_k(a), L_k(b)) &\iff S_{k+1}(i) \in L_{k+1}(a+b)\\
S_{k+1}(i) \in \mathrm{Product}(L_k(a), L_k(b)) &\iff S_{k+1}(i) \in L_{k+1}(ab)\\
S_k(i) \in \mathrm{Division}(L_k(a), L_k(b)) &\iff S_k(i) \in L_k(\lfloor a/b \rfloor)\\
S_{k+1}(i) \in \text{Iterated-Sum}(L_{k,l}((a_i)_{i<n^l})) &\iff S_{k+1}(i) \in L_{k+1}\left(\sum_{i<n^l} a_i\right)\\
S_{k+l}(i) \in \text{Iterated-Product}(L_{k,l}((a_i)_{i<n^l})) &\iff S_{k+l}(i) \in L_{k+l}\left(\prod_{i<n^l} a_i\right)
\end{aligned}$$

Theorem 7.2. *The operations* Sum, Product, Division, Iterated-Sum *and* Iterated-Product *are* FO(M)*-definable.*

Proof. The relations Division and Iterated-Product are the most difficult ones. That they are FO(M)-definable, is proved in [16]. □

Lemma 7.3. *Let $c_0, \ldots, c_{k-1}$ be constant symbols and let P be an k-ary relation symbol. Then a formula of* FO(M) *can express*

$$\sum_{\substack{\bar{a} \in P^{\mathfrak{A}} \\ a_i < c_i^{\mathfrak{A}}}} \binom{c_0^{\mathfrak{A}}}{a_0} \cdots \binom{c_{k-1}^{\mathfrak{A}}}{a_{k-1}} > 2^{n-1}.$$

Proof. For all $1 \leq m \leq n$, define a sequence $(a_i^m)_{i<n}$ as

$$a_i^m = \begin{cases} i+1 & \text{if } i+1 \leq m \\ 1 & \text{otherwise.} \end{cases}$$

Then $L_{1,1}((a_i^m)_{i<n})$ is FO-definable using the Bit-relation. Now

$$\text{Iterated-Product}(L_{1,1}((a_i^m)_{i<n})) = L_2(m!)$$

and

$$\mathrm{Division}(L_2(m!), \mathrm{Product}(L_2(l!), L_2((m-l)!))) = L_2\left(\binom{m}{l}\right)$$

are FO(M)-definable. Using Product and Iterated-Sum, also

$$L_2\left(\sum_{\substack{\bar{a} \in P^{\mathfrak{A}} \\ a_i < c_i^{\mathfrak{A}}}} \binom{c_0^{\mathfrak{A}}}{a_0} \cdots \binom{c_{k-1}^{\mathfrak{A}}}{a_{k-1}}\right)$$

can be defined in FO(M). Using this representation, it is easy to express that the number is greater than 2^{n-1}. □

Theorem 7.4. *Given $\varphi \in$ FO(Most^1)$[\tau]$, where τ contains only unary relations, there exists a formula $\varphi^*((x_t)_{t \in S_1(\tau)})$ in* FO(M)$[\{<, +, \times\}]$ *such that for all $\mathfrak{A} \in \mathrm{Mod}(\tau)$, $\mathfrak{A} \models \varphi$ if and only if $\langle n, <, +, \times \rangle \models \varphi^*(c^{\mathfrak{A}})$.*

Proof. As in the earlier proofs, we may replace first-order variables by unary relations containing only one element and first-order existential quantifiers by MSO-quantifiers. Because this eliminates all free first-order variables (except some variables in subformulas that are in FO), we can prove the theorem inductively for all MSO(Most^1)-sentences.

If a sentence does not contain Most^1-quantifiers, we can choose φ^* in FO. If $\varphi(\overline{X}) \equiv \exists Y \theta(\overline{X}, Y)$, φ^* can be defined as in Theorem 4.2.

If $\varphi(\overline{X}) \equiv \text{Most}^1\, Y\theta(\overline{X}, Y)$ and θ satisfies the theorem, we define φ^* so that

$$\langle n, +, \times\rangle \models \varphi^*(\overline{c}^{\mathfrak{A}}) \iff \sum_{\overline{a}\in P^{\mathfrak{A}}} \prod_{t\in S_1(\tau(\mathfrak{A}))} \binom{c_t^{\mathfrak{A}}}{a_t} > 2^{n-1},$$

where $P^{\mathfrak{A}}$ is the set of all sequences $(a_t)_{t\in S_1(\tau(\mathfrak{A}))}$ such that $\theta^*(\overline{a}')$ and $\overline{a}' = (a'_t)_{t\in S_1(\tau(\mathfrak{A})\cup\{Y\})}$ is defined so that for all $t \in S_1(\tau(\mathfrak{A}))$, $a'_{t\wedge Yv} = a_t$ and $a'_{t\wedge\neg Yv} = c_t^{\mathfrak{A}} - a_t$. Clearly $P^{\mathfrak{A}}$ is uniformly definable by the assumption that θ satisfies the lemma and so Lemma 7.3 gives the definability of φ^*. $\square$

8. On strings FO($\mathbf{Most^1}$) captures the linear counting hierarchy

In this section, we show that on strings FO(Most^1) captures the linear fragment of the counting hierarchy LINCH. Finding a logical characterization for LINCH was left as an open question in [8]. Our proof is analogous to the proof of Theorem 2.8 in [9], where it was shown that MSO captures the linear-time hierarchy LINH on strings with built-in addition.

The class LINCH is defined by the oracle hierarchy with PLinTime, the linear fragment of PP, as the building block. In other words, the class LINCH is obtained by taking the union of the following classes Σ_i^{Plin}, where Σ_0^{Plin} is the class of languages recognized by deterministic Turing machines in linear time, and

$$\Sigma_{i+1}^{Plin} = \text{PLinTime}^{\Sigma_i^{Plin}}.$$

It is known that languages in LINH correspond to rudimentary sets of natural numbers [17]. In [8] it was shown that analogously the languages in LINCH correspond exactly to the class $\mathcal{R}^\sharp$ of *counting rudimentary sets*. In [8] it was also shown that $\mathcal{R}^\sharp = \mathcal{R}^{Maj}$, where the latter is the class of relations obtained by allowing majority operations in the definition of rudimentary relations. In order to formally define these classes, we first define the bounded counting and majority quantifiers: The bounded counting quantifier $(\exists^{=y}x < u)$ is defined by the clause

$$\langle \mathbb{N}, \leq, +, \times\rangle \models (\exists^{=y}x < u)\,\psi(c_0/y, c_1/u) \text{ iff}$$

there are exactly c_0 many different interpretations $w < c_1$ of the variable x such that $\langle \mathbb{N}, \leq, +, \times\rangle \models \psi(w/x, c_1/u)$. On the other hand, the bounded majority quantifier $(\text{Maj}\, x < u)$ is defined by

$$\langle \mathbb{N}, \leq, +, \times\rangle \models (\text{Maj}\, x < u)\,\psi(c/u) \text{ iff}$$

for more than half of the interpretations $w < c$ of the variable x it holds that $\langle \mathbb{N}, \leq, +, \times\rangle \models \psi(w/x, c/u)$.

Definition 8.1. Let R be a k-ary relation on $\mathbb{N}$. We set $R \in \mathcal{R}^\sharp$ ($R \in \mathcal{R}^{Maj}$) iff R is definable over $\langle \mathbb{N}, \leq, +, \times\rangle$ by a formula $\varphi(\overline{x})$, whose all quantifications are either of the form $(\exists v \leq u)\psi$ or $(\exists^{=y}x < u)\psi$ ($(\text{Maj}\, x < u)\psi$), where u is a variable and whose atomic formulas are of the form $x + y = z$, $xy = z$ or $x = y$. The collection of such formulas is denoted by $\Delta_0(\text{C})$ ($\Delta_0(\text{Maj})$).

Definition 8.2. Let $\mathcal{L}$ be a logic and $\varphi \in \mathcal{L}[\{\leq, +, \times\}]$ a sentence. The spectrum $\text{Sp}(\varphi)$ of a sentence φ is defined as

$$\text{Sp}(\varphi) = \{n \in \mathbb{N} \mid \langle n, \leq, +, \times\rangle \models \varphi\}.$$

We denote by $\text{Sp}(\mathcal{L})$ the set of spectra of all $\mathcal{L}$ sentences

$$\text{Sp}(\mathcal{L}) = \{\text{Sp}(\varphi) \mid \varphi \in \mathcal{L}[\{\leq, +, \times\}]\}.$$

By Lemma 3.2 it is easy to see that the rudimentary sets (and hence the languages in LINH) correspond exactly to Sp(FO) (this has been discussed, e.g., in [18]). In the analogous way, it holds that the unary relations in $\mathcal{R}^{Maj}$ coincide with Sp(FO(M)). It is worth noting that the spectra of first-order sentences φ, where φ can be of any vocabulary τ and not just $\{\leq, +, \times\}$, is known to correspond to NTIME[$2^{\mathrm{O(n)}}$] [19].

Proposition 8.3. *Let $A \subseteq \mathbb{N}^*$. Then $A \in \mathcal{R}^{Maj}$ iff $A \in$ Sp(FO(M)).*

Proof. For the inclusion $\text{Sp(FO(M))} \subseteq \mathcal{R}^{Maj}$, we define a translation of FO(M)-formulas into Δ_0(Maj)-formulas. The translation is defined by relativizing quantifications by a new variable x, i.e., $\exists y$ and M y are translated as $(\exists y < x)$ and $(\text{Maj}\, y < x)$, respectively. It is easy to verify that for any sentence $\psi \in$ FO(M), the corresponding formula $\psi^*(x)$ defines the set $\text{Sp}(\psi)$.

Assume then that $A \in \mathcal{R}^{Maj}$. By definition, there is formula $\psi(x) \in \Delta_0(\text{Maj})$ defining A over $\langle \mathbb{N}, \leq, +, \times\rangle$. Note that quantifications $(\text{Maj}\, y < u)$ can be expressed, e.g., by using the first-order Rescher quantifier R in FO(M). Therefore, we can construct a formula $\psi^*(x) \in \mathrm{FO(M)}$ such that, for all n, $\psi^*(x)$ defines the set $A \cap n$ over $\langle n, \leq, +, \times\rangle$. It is now easy to write a sentence $\varphi \in \mathrm{FO(M)}$ such that $\mathrm{Sp}(\varphi) = A$. □

In this section, we need the following more general versions of the quantifier Most^1:

$$\mathfrak{A} \models \mathrm{Most}^1_k \overline{X}\psi(\overline{X}) \Leftrightarrow |\psi^{\mathfrak{A}}| > 2^{k|\mathrm{Dom}(\mathfrak{A})|-1},$$

where $\overline{X} = X_1, \ldots, X_k$. By the same argument as in Theorem 3.5 of [1] it holds that the quantifier $\mathcal{R}^1_k$ defined by

$$\mathfrak{A} \models \mathcal{R}^1_k\overline{X}, \overline{Y}(\psi(\overline{X}), \varphi(\overline{Y})) \Leftrightarrow |\psi^{\mathfrak{A}}| > |\varphi^{\mathfrak{A}}|,$$

can be defined in the logic $\mathrm{FO}(\mathrm{Most}^1_k)$ on ordered structures. On the other hand, the following lemma shows that in some cases the quantifiers Most^1_k can be already expressed in terms of the quantifier Most^1.

Lemma 8.4. *Suppose that $\tau = \{<, P_1, \ldots, P_m\}$, where P_i is unary for $1 \leq i \leq m$. Then on τ-structures*

$$\mathrm{FO}(\mathrm{Most}^1_k)_{k\in\mathbb{Z}_+} \equiv \mathrm{FO}(\mathrm{Most}^1).$$

Proof. It suffices to show that $\mathrm{FO}(\mathrm{Most}^1_k)_{k\in\mathbb{Z}_+}[\tau] \leq \mathrm{FO}(\mathrm{Most}^1)[\tau]$, i.e., that for every sentence $\varphi \in \mathrm{FO}(\mathrm{Most}^1_k)_{k\in\mathbb{Z}_+}[\tau]$ there is an equivalent sentence $\psi \in \mathrm{FO}(\mathrm{Most}^1)[\tau]$. The proof uses the fact that, for all $k \in \mathbb{Z}_+$, the first-order k-ary majority quantifier M^k can be defined in the logic FO(M) with the help of the predicates $+$ and $\times$ (see [15]).

Let $\sigma = \{<, +, \times, c_1, \ldots, c_m\}$ be a vocabulary, where each c_i is a constant symbol. For a τ-structure $\mathfrak{A} = \langle n, <, P_1^{\mathfrak{A}}, \ldots, P_m^{\mathfrak{A}}\rangle$, let $\mathfrak{A}^*$ be the following σ-structure

$$\mathfrak{A}^* = \langle 2^n, <, +, \times, c_1^{\mathfrak{A}^*}, \ldots, c_m^{\mathfrak{A}^*}\rangle,$$

where $c_i^{\mathfrak{A}^*}$ is the integer ($<2^n$) whose length n binary representation corresponds to $P_i^{\mathfrak{A}}$. We shall next show that for any sentence $\varphi \in \mathrm{FO}(\mathrm{Most}^1_k)_{k\in\mathbb{Z}_+}[\tau]$ there is a sentence $\varphi^* \in \mathrm{FO}(\mathrm{M}^k)_{k\in\mathbb{Z}_+}[\sigma]$ such that for all τ-structures $\mathfrak{A}$

$$\mathfrak{A} \models \varphi \Leftrightarrow \mathfrak{A}^* \models \varphi^*.$$

The sentence φ^* is defined by the following inductive translation:

$$\begin{aligned}
(x_i < x_j)^* &\equiv x_i < x_j \\
(P_i x_j)^* &\equiv \mathrm{Bit}(c_i, x_j) \\
(X_i x_j)^* &\equiv \mathrm{Bit}(y_i, x_j) \\
(\exists x_i \psi(x_i))^* &\equiv \exists x_i(x_i < n \wedge \psi^*(x_i)) \\
(\mathrm{Most}^1_k \overline{X}\, \psi(\overline{X}))^* &\equiv \mathrm{M}^k\, \overline{y}\, \psi^*(\overline{y}).
\end{aligned}$$

Above, $\mathrm{Bit}(c_i, x_j)$ and $x_i < n$ are abbreviations for definable formulas. Since the quantifiers M^k are definable in the logic FO(M) over initial segments of arithmetic, there is a sentence $\psi \in \mathrm{FO(M)}[\sigma]$ equivalent to φ^*. Now, by essentially replacing first-order variables by second-order variables, we can write a sentence $\psi' \in \mathrm{FO}(\mathrm{Most}^1)[\tau]$ such that for every τ-structure $\mathfrak{A}$

$$\mathfrak{A} \models \psi' \Leftrightarrow \mathfrak{A}^* \models \psi.$$

Note that, by the above ψ' is equivalent to φ and we are done. The translation is defined by replacing every existential first-order quantification by existential monadic second-order quantification and every M-quantification by Most^1-quantification. Sums and products are converted into sums and products on binary representation of the numbers. Note that we do not need to assume built-in predicates $+$ and $\times$ in the case of $\mathrm{FO}(\mathrm{Most}^1)$ since they are definable over ordered structures. □

The proof of Lemma 8.4 implies also the following fact that will be useful later.

Corollary 8.5. *Let $A \subseteq \mathbb{N}^*$. Then $A \in \mathrm{Sp}(\mathrm{FO}(\mathrm{Most}^1))$ iff $\{2^n \mid n \in A\} \in \mathrm{Sp}(\mathrm{FO(M)})$.*

Lemma 8.4 also has the following corollary showing that, over vocabularies of the form $\{<, P_1, \ldots, P_m\}$, the logic $\mathrm{FO}(\mathrm{Most}^1)$ is closed under logical reductions I for which the target structure $I(\mathfrak{A})$ has size linear in $|\mathrm{Dom}(\mathfrak{A})|$.

Corollary 8.6. *Suppose that $\tau = \{<, P_1, \ldots, P_m\}$, where each P_i is unary and σ is a vocabulary. Let I be an interpretation, definable in terms of $\mathrm{FO}(\mathrm{Most}^1)[\tau]$-formulas, mapping τ-structures $\mathfrak{A}$ to σ-structures $I(\mathfrak{A})$ such that for all $\mathfrak{A}$*

$$\mathrm{Dom}(I(\mathfrak{A})) = \{(i, j) \mid 0 \leq i \leq k-1 \text{ and } j \in \mathrm{Dom}(\mathfrak{A})\},$$

for some fixed $k \in \mathbb{N}^*$. *Then for any sentence* $\varphi \in \mathrm{FO}(\mathrm{Most}^1)[\sigma]$ *there is a sentence* $\varphi^* \in \mathrm{FO}(\mathrm{Most}^1)[\tau]$ *such that for all* $\mathfrak{A}$ *(with* $|\mathrm{Dom}(\mathfrak{A})| \geq k$*)*

$$\mathfrak{A} \models \varphi^* \Leftrightarrow I(\mathfrak{A}) \models \varphi.$$

Proof. We define φ^* using induction on φ. As the domain of the structure $I(\mathfrak{A})$ consists of pairs $(i, j) \in \mathrm{Dom}(\mathfrak{A})^2$ such that $0 \leq i \leq k-1$, each first-order variable x over $I(\mathfrak{A})$ is replaced by a pair (x_1, x_2) of variables. Second-order variables X are replaced by k-tuples $(X_0, \ldots, X_{k-1})$ of second-order variables. The idea is that if X is interpreted by the set $A \subseteq \{(i, j) \mid 0 \leq i \leq k-1 \text{ and } j \in \mathrm{Dom}(\mathfrak{A})\}$, then the interpretation of X_i encodes the set $A \cap \{(i, j) \mid j \in \mathrm{Dom}(\mathfrak{A})\}$.

Let us then define φ^*: for atomic σ-formulas φ, the formula φ^* is defined using the corresponding $\mathrm{FO}(\mathrm{Most}^1)[\tau]$-formulas which exist by the assumption. For example, for each $R \in \sigma$ there is a formula $\pi_R((x_1^1, x_2^1), \ldots, (x_1^l, x_2^l)) \in \mathrm{FO}(\mathrm{Most}^1)[\tau]$, where l is the arity of R, such that the interpretation of R in $I(\mathfrak{A})$ is given by

$$\{(\bar{a}_1, \ldots, \bar{a}_l) \in A^{2l} \mid \mathfrak{A} \models \pi_R(\bar{a}_1, \ldots, \bar{a}_l)\}.$$

The boolean connectives are translated in the trivial way. The remaining cases are defined below:

$$\begin{aligned}
(x = y)^* &\equiv x_1 = y_1 \wedge x_2 = y_2 \\
(Xy)^* &\equiv \bigvee_{0 \leq i \leq k-1} (y_1 = i \wedge X_i y_2) \\
(\exists x \psi)^* &\equiv \exists x_1 \exists x_2 (0 \leq x_1 \leq k-1 \wedge \psi^*(x_1, x_2)) \\
(\mathrm{Most}^1\, X\, \psi(X))^* &\equiv \mathrm{Most}_k^1\, \bar{X} \psi^*(\bar{X}). \qquad \Box
\end{aligned}$$

Definition 8.7. Let n be a positive integer. Denote by $\mathrm{ld}(n)$ its dyadic length, i.e., we have

$$n = \sum_{i=0}^{\mathrm{ld}(n)-1} n_i 2^i,$$

with $n_i \in \{1, 2\}$. We denote by w_n the dyadic notation for n, i.e., the word $n_0 n_1, \ldots, n_{\mathrm{ld}(n)-1}$.

Dyadic notation provides a one-to-one and onto correspondence between words and positive integers and avoids problems with leading zeroes. Let $w \in \{1, 2\}^*$ and n an integer such that $w_n = w$. Denote by P_w the unary relation over $\{0, \ldots, \mathrm{ld}(n) - 1\}$ defined by $i \in P_w$ iff the digit of weight 2^i of n is 2. We denote by $\mathfrak{A}_w$ the word structure $\langle \mathrm{ld}(n), <, P_w \rangle$.

Definition 8.8. A language $L \subseteq \{1, 2\}^+$ is definable in $\mathrm{FO}(\mathrm{Most}^1)$ if there is $\psi \in \mathrm{FO}(\mathrm{Most}^1)[\{<, P\}]$, where P is unary, such that for all words w

$$\mathfrak{A}_w \models \psi \Leftrightarrow w \in L.$$

For $A \subseteq \mathbb{N}$, denote by $L_2(A)$ the language $\{w_n \mid n \in A\}$ and let

$$\mathcal{L}_2(\mathcal{R}^\sharp) = \{L_2(A) \mid A \in \mathcal{R}^\sharp\}.$$

We are now ready to state the main result of this section. Below we restrict attention to binary strings. The result can be then generalized easily to strings of arbitrary finite alphabets (see Corollary 8.10).

Theorem 8.9. *Let* $L \subseteq \{1, 2\}^+$. *Then L is definable in* $\mathrm{FO}(\mathrm{Most}^1)$ *iff* $L \in \mathcal{L}_2(\mathcal{R}^\sharp)$.

Proof. Assume that $A \subseteq \mathbb{N}^*$ and that $L_2(A)$ is definable in $\mathrm{FO}(\mathrm{Most}^1)$. We shall show that $A \in \mathcal{R}^\sharp$. We construct a $\Delta_0(\mathrm{C})$-formula $\theta(n)$ defining A. The proof of the claim is analogous to the proof of Lemma 3.1 in [9] and similar to the translation used in Lemma 8.4, where binary notation was used instead of dyadic notation. Therefore, we refer to [9] for details on the other cases of the translation and just provide a translation for the quantifier Most^1. Note that subsets of $l = \mathrm{ld}(n)$ correspond exactly to integers ($\leq 2n$) from the interval $[2^l - 1, 2^{l+1} - 2]$. We translate $\mathrm{Most}^1\, X \psi(X)$ as

$$(\exists y \leq n+1)\left[(\exists^{=y} x \leq 2n)(2^l - 1 \leq x \leq 2^{l+1} - 2 \wedge \psi^*(x)) \wedge y > 2^{l-1}\right],$$

where $\psi^*(x)$ is the translation of $\psi(X)$. We use above the fact that $\mathcal{R}^\sharp$ is closed under polynomial bounded quantifications [18].

Assume then that $A \in \mathcal{R}^\sharp = \mathcal{R}^{Maj}$. We need to show that $L_2(A)$ is definable in $\mathrm{FO}(\mathrm{Most}^1)$. By Proposition 8.3, there is a sentence $\varphi \in \mathrm{FO}(\mathrm{M})$ such that for all $n \in \mathbb{N}$

$$n \in A \text{ iff } \langle n, <, +, \times \rangle \models \varphi.$$

We construct a sentence $\psi \in \mathrm{FO}(\mathrm{Most}^1)[\{<, P\}]$ such that

$$\mathfrak{A}_{w_n} \models \psi \text{ iff } \langle n, <, +, \times \rangle \models \varphi.$$

We recall the following notation from [9]. Let $n \in \mathbb{N}$ and $l = \mathrm{ld}(n)$. We associate to each integer $u < n$ the following pair of unary relations $(1_u, 2_u)$ over l defined by $i \in 1_u$ ($i \in 2_u$) holds iff the letter of index i is 1 in w_u (resp. 2). Similarly, we associate to each first-order variable x over n a tuple (X_1, X_2) of unary second-order variables. Next we define some formulas that will be used in the translation. Denote by $N_{<max}(X_1, X_2)$ a formula which for every pair (A, B) of unary relations over the domain l expresses:

$$\mathfrak{A}_{w_n} \models N_{<max}(A, B) \Leftrightarrow \exists x < n \text{ such that } (1_x, 2_x) = (A, B).$$

We shall use formulas $\Delta_<(X_1, X_2, Y_1, Y_2)$, $\Delta_+(X_1, X_2, Y_1, Y_2, Z_1, Z_2)$ and $\Delta_\times(X_1, X_2, Y_1, Y_2, Z_1, Z_2)$, to translate the arithmetic predicates. The idea is of course that, e.g.,

$$\mathfrak{A}_{w_n} \models \Delta_+(1_a, 2_a, 1_b, 2_b, 1_c, 2_c) \text{ iff } \langle n, <, +, \times \rangle \models a + b = c.$$

These formulas can be constructed easily by using the formulas defining addition and multiplication of binary numbers (see Section 7). In other words, it suffices to define a translation from dyadic notation of integers to binary notation. Suppose that $w \in \{1, 2\}^k$ and n is an integer such that $w_n = w$. Now n can be represented as a sum of two k-bit binary numbers, namely, 1^k, i.e., the string of k repetitions of 1, and $i_k \dots i_1$, where $i_l = 1$ iff the lth bit of w is 2.

The translation is now defined as follows:

$$\begin{aligned}
(\exists x \phi(x))^* &\equiv \exists X_1 \exists X_2 (N_{<max}(X_1, X_2) \wedge \phi^*(X_1, X_2)) \\
(\mathrm{M}\, x\, \phi(x))^* &\equiv \mathcal{R}_2^1\, X_1X_2, X_1X_2\ (N_{<max}(X_1, X_2) \wedge \phi^*, N_{<max}(X_1, X_2) \wedge \neg\phi^*) \\
(x < y)^* &\equiv \Delta_<(X_1, X_2, Y_1, Y_2) \\
(x + y = z)^* &\equiv \Delta_+(X_1, X_2, Y_1, Y_2, Z_1, Z_2) \\
(xy = z)^* &\equiv \Delta_\times(X_1, X_2, Y_1, Y_2, Z_1, Z_2).
\end{aligned}$$

The translation above gives us a sentence φ^*, containing occurrences of the quantifier $\mathcal{R}_2^1$, such that for all $n \in \mathbb{N}^*$

$$\mathfrak{A}_{w_n} \models \varphi^* \text{ iff } \langle n, <, +, \times \rangle \models \varphi.$$

Recall that the quantifier $\mathcal{R}_2^1$ can be defined in terms of Most_2^1 on ordered structures and, by Lemma 8.4, the quantifier Most_2^1 can be already expressed using the quantifier Most^1. Hence, we can replace φ^* by an equivalent sentence $\psi \in \mathrm{FO}(\mathrm{Most}^1)$ $[\{<, P\}]$. $\square$

Since by [8] it holds that $\mathcal{L}_2(\mathcal{R}^\sharp) = \mathrm{LINCH}$, we have shown that the logic $\mathrm{FO}(\mathrm{Most}^1)$ captures the class LINCH on binary strings. Using Corollary 8.6, we can generalize this result to strings over arbitrary alphabets. This can be stated in a bit more general form as follows:

Corollary 8.10. *Let $\tau = \{<, P_1, \dots, P_m\}$, where each P_i is unary. Then the logic* $\mathrm{FO}(\mathrm{Most}^1)$ *captures the class* LINCH *on τ-structures.*

Proof. Denote by I_{bin} and I_{bin}^{-1} the interpretations such that I_{bin} maps a τ-structure $\mathfrak{A}$ to a word structure $\mathcal{W}_{\mathfrak{A}}$ corresponding to $\mathrm{bin}(\mathfrak{A})$ and $I_{bin}^{-1}(\mathcal{W}_{\mathfrak{A}}) = \mathfrak{A}$ for all $\mathfrak{A}$. The interpretations I_{bin} and I_{bin}^{-1} are first-order definable assuming built-in ordering and arithmetic [20] and thus $\mathrm{FO}(\mathrm{Most}^1)$-definable over ordered structures. Let K be a class of τ-structures such that $K^* \in \mathrm{LINCH}$, where

$$K^* = \{I_{bin}(\mathfrak{A}) \mid \mathfrak{A} \in K\}.$$

By Theorem 8.9, K^* can be defined by some $\varphi \in \mathrm{FO}(\mathrm{Most}^1)$ over binary words. Since for all τ-structures $\mathfrak{A}$ it holds that $|I_{bin}(\mathfrak{A})| = m|\mathfrak{A}|$, we may apply Corollary 8.6 to get a sentence $\varphi^* \in \mathrm{FO}(\mathrm{Most}^1)[\tau]$ such that for all τ-structures $\mathfrak{A}$

$$\mathfrak{A} \models \varphi^* \Leftrightarrow I_{bin}(\mathfrak{A}) \models \varphi,$$

and hence φ^* defines K. The other direction is analogous. $\square$

Remark 8.11. It is known that if $\mathrm{Sp(FO)} \neq \mathrm{Sp(FO(M))}$, then $\mathrm{LINH} \neq \mathrm{E}$. In [21] Schweikardt asked if the opposite has any serious complexity theoretic consequences. Note that $\mathrm{Sp(FO)} = \mathrm{Sp(FO(M))}$ would imply that $\mathrm{LINH} = \mathrm{LINCH}$. Now since LINCH contains problems complete for each level of the counting hierarchy, we would have that $\mathrm{PH} = \mathrm{CH}$ and that CH would collapse to its second level by Toda's Theorem [22].

9. Separation of $\mathrm{FO(Most^1)}$ and $\mathrm{FO(Most^2)}$

Define Sp_0 similarly as Sp, but over the empty vocabulary, i.e., $\mathrm{Sp}_0(\varphi) = \{n \in \mathbb{N} \mid \langle n \rangle \models \varphi\}$ and $\mathrm{Sp}_0(\mathcal{L}) = \{\mathrm{Sp}_0(\varphi) \mid \varphi \in \mathcal{L}\}$. Since we can existentially quantify linear orders in $\mathrm{FO(Most^2)}$ and the logic can define arithmetic on ordered structures, we have $\mathrm{Sp(FO(Most^2))} = \mathrm{Sp_0(FO(Most^2))}$. We will prove in this section $\mathrm{Sp(FO(M))} \subsetneq \mathrm{Sp(FO(Most^1))}$. Combined with the results in the preceding sections (the first inclusion follows by Theorems 5.4 and 6.2 and the second inclusion by Theorem 7.4), this gives us

$$\begin{aligned}\mathrm{Sp(FO)} &\subseteq \mathrm{Sp}_0\left(\mathrm{FO(Most^1)}\right) \subseteq \mathrm{Sp(FO(M))}\\ &\subsetneq \mathrm{Sp}\left(\mathrm{FO(Most^1)}\right) \subseteq \mathrm{Sp}\left(\mathrm{FO(Most^2)}\right) = \mathrm{Sp}_0\left(\mathrm{FO(Most^2)}\right).\end{aligned}$$

In particular, $\mathrm{FO(Most^1)} < \mathrm{FO(Most^2)}$.

Let MLFP be the extension of first-order logic by the monadic least fixed point operator. On the initial segments of arithmetic, it is known that $\mathrm{FO(M)} \leq \mathrm{MLFP} \leq \mathrm{MSO} \leq \mathrm{FO(Most^1)}$ (for the first inclusion see Lemma 5.4 in [23]).

Let us fix some reasonable coding $\varphi \mapsto \mathrm{code}(\varphi)$ of FO(M)-sentences as binary words. Given a binary word $w = w_0 \dots w_{n-1}$, let $N(w) = \sum_{i<n} w_i 2^{n-i-1}$. For all $\varphi \in \mathrm{FO(M)}$, let $\mathrm{varcount}(\varphi)$ be the number of different variables occuring in φ. For binary words w_0 and w_1, let $w_0\#w_1$ be a binary word where all bits of w_0 and w_1 are doubled and 01 inserted in between. Then w_0 and w_1 are recoverable in linear time and the length of the word $w_0\#w_1$ is linear in $\max(|w_0|, |w_1|)$.

Recall that the complexity of the model checking problem $\langle n, \leq, +, \times\rangle \models \varphi$ is

$$O(n^{O(\mathrm{varcount}(\varphi))}|\mathrm{code}(\varphi)|)$$

for $\varphi \in \mathrm{FO}$ [24]. This can be easily verified also for FO(M). Let us fix a big enough k so that $\langle n, \leq, +, \times\rangle \models \varphi$ can be checked in time $O(n^{k(\mathrm{varcount}(\varphi))}|\mathrm{code}(\varphi)|)$ for $\varphi \in \mathrm{FO(M)}$. We consider the following spectrum:

$$\begin{aligned}S = \{n \in \mathbb{N} \mid\; & n = N(10^m\#w\#\mathrm{code}(\varphi)), \varphi \in \mathrm{FO(M)}, m \in \mathbb{N},\\ & \langle N(w), \leq, +, \times\rangle \models \varphi, n \geq N(w)^{k(\mathrm{varcount}(\varphi))}|\mathrm{code}(\varphi)|\}\end{aligned}$$

Lemma 9.1. $S \in \mathrm{Sp(MLFP)}$.

Proof. By the arguments above, checking $n = N(10^m\#w\#\mathrm{code}(\varphi)) \in S$, can be done in time linear to n, i.e., we can recognize S in deterministic linear time relative to n. By [23] the computations can be done in MLFP. $\square$

Theorem 9.2. $\mathrm{Sp(FO(Most^1))} \not\subseteq \mathrm{Sp(FO(M))}$.

Proof. Because $\mathrm{MLFP} \leq \mathrm{MSO} \leq \mathrm{FO(Most^1)}$, the claim holds if $S \notin \mathrm{Sp(FO(M))}$. Assume therefore $S \in \mathrm{Sp(FO(M))}$, i.e., there is $\theta \in \mathrm{FO(M)}$ such that $S = \mathrm{Sp}(\theta)$. Let

$$\begin{aligned}D = \{n \in \mathbb{N} \mid\; & \text{if } n = N(\mathrm{code}(\varphi)) \text{ for some } \varphi \in \mathrm{FO(M)},\\ & \text{then } \langle n, \leq, +, \times\rangle \not\models \varphi\}.\end{aligned}$$

For all $\varphi \in \mathrm{FO(M)}$, we have $N(\mathrm{code}(\varphi)) \in \mathrm{Sp}(\varphi) \iff N(\mathrm{code}(\varphi)) \notin D$. Hence $D \notin \mathrm{Sp(FO(M))}$.

Define $f(n, m) = N(10^m\#w_n\#w_n)$, where w_n is the binary representation of n. Let

$$D' = \{2^n \mid (\forall m \leq n)(f(n, m) < 2^n \to f(n, m) \notin S)\}.$$

We claim that $D' \in \mathrm{Sp(FO(M))}$. The FO(M)-sentence defining the spectrum first universally quantifies m and then calculates $h = f(n, m)$. It then checks $h \notin S$ using θ where all quantifications are bounded by h.

If $n \in D$ and $n = N(\mathrm{code}(\varphi))$ for some $\varphi \in \mathrm{FO(M)}$, then $\langle n, \leq, +, \times\rangle \not\models \varphi$. Then for all $m \in \mathbb{N}$, $f(n, m) = N(10^m\#\mathrm{code}(\varphi)\#\mathrm{code}(\varphi)) \notin S$ and so $2^n \in D'$. If $n \neq N(\mathrm{code}(\varphi))$ for all $\varphi \in \mathrm{FO(M)}$, we also have $2^n \in D'$.

If $n \notin D$, then $n = N(\text{code}(\varphi))$ for some $\varphi \in \text{FO(M)}$ and $\langle n, \leq, +, \times \rangle \models \varphi$. Then $f(n, m) \in S$ if m is chosen so large that

$$f(n, m) \geq N(\text{code}(\varphi))^{k(\text{varcount}(\varphi))}|\text{code}(\varphi)| = n^{k(\text{varcount}(\varphi))}|\text{code}(\varphi)|.$$

Certainly, we must have

$$n^{k(\text{varcount}(\varphi))}|\text{code}(\varphi)| \leq n^{k|\text{code}(\varphi)|}|\text{code}(\varphi)| \leq n^{k(\lfloor \log_2 n \rfloor + 1)}(\lfloor \log_2(n) \rfloor + 1).$$

When n is big enough, we can choose m so that $n^{k(\text{varcount}(\varphi))}|\text{code}(\varphi)| \leq f(n, m) < 2^n$ and so get $2^n \notin D'$.

Because $\{2^n \mid n \in D\}$ and D' differ only on finite number of elements, by Corollary 8.5, D is in $\text{Sp}(\text{FO}(\text{Most}^1))$ and thus $\text{Sp}(\text{FO}(\text{Most}^1)) \not\subseteq \text{Sp}(\text{FO(M)})$. $\square$

Remark 9.3. The proof above can be used also to separate LINCH (linear time counting hierarchy) and ECH (exponential time counting hierarchy). Separation of the classes LINH and EH, which also follows from a similar idea, is apparently shown in [25], which we however were not able to obtain.

10. Approximating CH in terms of $\text{FO}(\text{Most}^1)$

It is well known that MSO can define complete problems for every level of the polynomial hierarchy. In this section, we show that the analogous result holds for $\text{FO}(\text{Most}^1)$ and CH. Variants of the quantified boolean formula problem are known to be complete for each level of PH. In an analogous way, it is possible to construct complete sets for all levels of the counting hierarchy. It is worth noting that the result of this section, over string structures, is an easy corollary of the characterization of LINCH by the logic $\text{FO}(\text{Most}^1)$. However, in this section we show that also on unordered structures $\text{FO}(\text{Most}^1)$ can define classes of structures complete for every level of the counting hierarchy (see Proposition 10.6). For the completeness results (Theorem 10.3) we do need to assume built-in arithmetic.

Definition 10.1. Let $k \geq 1$ and define

$$F(\tilde{x}_1, \ldots, \tilde{x}_k) \in \text{MAJSAT}_\text{k},$$

iff $F(\tilde{x}_1, \ldots, \tilde{x}_k)$ is a boolean formula and

$$\mathcal{C}\tilde{x}_1 \ldots \mathcal{C}\tilde{x}_k F(\tilde{x}_1, \ldots, \tilde{x}_k)$$

is true, where $\mathcal{C}\tilde{x}$ is interpreted as "more than half of the partial truth assignments for the variables in $\tilde{x}$".

It is known that the problem MAJSAT_k is complete for the class $\text{C}_\text{k}\text{P}$ [6]. However, our goal in this section is to give a logical version of the proof of the completeness of MAJSAT_k for $\text{C}_\text{k}\text{P}$ arising from the logical characterization of CH in [1].

We shall first define an encoding of boolean formulas as finite structures (essentially as boolean circuits). We encode a formula $F(\tilde{x}_1, \ldots, \tilde{x}_k)$ as a certain acyclic directed graph $\mathfrak{A}_F$ over the vocabulary

$$\tau = \{E, I_1, \ldots, I_k, P_\neg, P_\vee, P_\wedge, v, \mathbf{1}, \mathbf{0}\},$$

where the predicate E is binary, I_i, $P_\neg$, $P_\vee$, and $P_\wedge$ are unary and v, $\mathbf{1}$, $\mathbf{0}$ are constants. The graph $\mathfrak{A}_F$ represents the syntactic structure of the formula F. The domain of $\mathfrak{A}_F$ contains exactly one element for every variable and every subformula of F. The interpretation of $E(x, y)$ is "x is an immediate subformula of y". The meaning of the predicates $P_\neg$, $P_\vee$, and $P_\wedge$ is obvious. The predicates I_i pick out the elements standing for the boolean variables in $\tilde{x}_i$. The constant v encodes the formula F and thus it has no out-going edges. The constants $\mathbf{1}$, $\mathbf{0}$ are the elements representing the boolean constants.

Definition 10.2. Denote by $\text{MAJSAT}_\text{k}^\text{Str}$ the class

$$\text{MAJSAT}_\text{k}^\text{Str} = \{\mathfrak{A}_F \mid F \in \text{MAJSAT}_\text{k}\}.$$

Theorem 10.3. *In the presence of the built-in predicates $\{<, +, \times\}$, the class $\text{MAJSAT}_\text{k}^\text{Str}$ is complete for $\text{C}_\text{k}\text{P}$ under first-order reductions.*

Before going to the proof of Theorem 10.3 we recall the following result from [1]. Below, $qr(\varphi) \leq k$ means that the maximal nesting-depth of the quantifiers Most^i in φ is at most k.

Proposition 10.4. *Let $k \geq 1$ and $\{<, +, \times\} \subseteq \tau$ a vocabulary. Then*

$$\mathrm{C_kP}[\tau] = \{\mathrm{Mod}(\varphi) \mid \varphi \in \mathrm{FO(Most)}[\tau],\ qr(\varphi) \leq k\}.$$

Proof. See Proposition 4.5 in [1]. □

A simple modification of the proof of Proposition 10.4 actually gives the following normal-form for $\mathrm{C_kP}$.

Lemma 10.5. *Let $k \geq 1$ and $\{<, +, \times\} \subseteq \tau$ a vocabulary. Then*

$$\mathrm{C_kP}[\tau] = \{\mathrm{Mod}(\varphi) \mid \varphi = \mathrm{Most}^{i_1}\, Y_1, \ldots, \mathrm{Most}^{i_k}\, Y_k\, \psi \text{ and } \psi \in \mathrm{FO}\}.$$

Proof. The claim is proved using induction on k. We need only to modify the proof in the case $k = 1$. In [1] it is shown that $\mathrm{C_1P}[\tau]$ can be captured using sentences of the form

$$\exists \overline{x}\, \mathrm{Most}^i\, Y \psi.$$

However, inspection of the proof shows that we can get rid of the quantifier block $\exists \overline{x}$ in the formula on ordered structures by using, e.g., definable elements 0, 1 instead. These elements can be defined by using existential quantifiers placed after the Most^i-quantification. The proof of the inductive step remains the same. Finally, note that it suffices to prove the claim for binary strings, since the formula transformation induced by an interpretation from τ-structures to binary strings preserves the desired structure of sentences. □

Proof of Theorem 10.3. Since $\mathrm{MAJSAT}_k^{\mathrm{Str}}$ is easily seen to be in $\mathrm{C_kP}$, it suffices to show that every class in $\mathrm{C_kP}$ can be reduced to $\mathrm{MAJSAT}_k^{\mathrm{Str}}$. Let τ be a vocabulary and $K \subseteq \mathrm{C_kP}[\tau]$. By Lemma 10.5, there is a sentence

$$\varphi = \mathrm{Most}^{i_1}\, Y_1, \ldots, \mathrm{Most}^{i_k}\, Y_k\, \psi,$$

where $\psi \in \mathrm{FO}[\tau]$, such that $K = \mathrm{Mod}(\varphi)$. We may assume that ψ is of the form

$$Q_1 x_1, \ldots, Q_t x_t\, \theta(x_1, \ldots, x_t),$$

where Q_i is either $\exists$ or $\forall$ and $\theta(x_1, \ldots, x_t) = \bigwedge_{1 \leq i \leq r} C_i(x_1, \ldots, x_t)$ is in conjunctive normal-form, i.e., $C_i(x_1, \ldots, x_t)$ is a disjunction of atomic formulas and their negations.

Fix a structure $\mathfrak{A}$. The sentence φ and the structure $\mathfrak{A}$ gives rise to a boolean formula $\theta_\varphi(\mathfrak{A})$ as follows. We first assign a boolean variable $x_{Y,\overline{a}}$ for each second-order variable Y_j and $\overline{a} \in \mathrm{Dom}(\mathfrak{A})^{i_j}$. The formula $\theta_\varphi(\mathfrak{A})$ is now defined inductively by the following clauses:

1. For an atomic formula of the form $Y_j(\overline{x})$ and $\overline{a}$ interpreting $\overline{x}$, we let $\theta_{Y_j(\overline{x})}((\mathfrak{A}, \overline{a}))$ be the variable $x_{Y_j,\overline{a}}$.
2. For all the other atomic formulas $\chi(\overline{x})$ and their negations, $\theta_{\chi(\overline{x})}((\mathfrak{A}, \overline{a}))$ is either the boolean constant 1 or 0 according to whether $\mathfrak{A} \models \chi(\overline{a})$ or $\mathfrak{A} \not\models \chi(\overline{a})$.
3. For a formula of the form $\exists x \phi(x, \overline{y})$ ($\forall x \phi(x, \overline{y})$) we define $\theta_{\exists x \phi(x,\overline{y})}((\mathfrak{A}, \overline{a}))$ as the formula $\bigvee_{b \in \mathrm{Dom}(\mathfrak{A})} \theta_\phi((\mathfrak{A}, \overline{a}, b))$ ($\bigwedge_{b \in \mathrm{Dom}(\mathfrak{A})} \theta_\phi((\mathfrak{A}, \overline{a}, b))$).
4. A formula of the form $\mathrm{Most}^{i_j}\, Y_j\, \phi$ is translated as $C\tilde{x}_j\, \theta_\phi(\mathfrak{A})$, where $\tilde{x}_j$ is the set $\{x_{Y_j,\overline{a}} \mid \overline{a} \in \mathrm{Dom}(\mathfrak{A})^{i_j}\}$. □

The following result is easily obtained.

Claim 1. *For every structure $\mathfrak{A}$ the following are equivalent:*

(a) $\mathfrak{A} \models \varphi$,
(b) $\theta_\varphi(\mathfrak{A})$ *is true,*
(c) $\theta_\psi(\mathfrak{A})(\tilde{x}_1, \ldots, \tilde{x}_k) \in \mathrm{MAJSAT}_k$.

Proof. Analogous to the proof of Theorem 2 in [26]. □

Claim 2. *There is a first-order interpretation I such that for all $\mathfrak{A}$ with $|\mathrm{Dom}(\mathfrak{A})| \geq 2$*

$$\mathfrak{A} \models \varphi \textit{ iff } I(\mathfrak{A}) \in \mathrm{MAJSAT}_k^{\mathrm{Str}}.$$

Proof. The interpretation I is defined so that $I(\mathfrak{A})$ is a structure encoding the boolean formula $\theta_\psi(\mathfrak{A})(\tilde{x}_1, \ldots, \tilde{x}_k)$. The interpretation can be defined in a similar way as in Proposition 11.10 [20], where it was shown that SAT in NP-complete under so-called first-order projection reductions. □

It remains to show that the classes $\mathrm{MAJSAT}^{\mathrm{Str}}_{\mathrm{k}}$ can be defined in $\mathrm{FO}(\mathrm{Most}^1)$. Recall that for the completeness result (Theorem 10.3) we needed to assume built-in arithmetic. On the other hand, for the definability result below we do not need to make this assumption.

Proposition 10.6. *For every $k \geq 1$ the class* $\mathrm{MAJSAT}^{\mathrm{Str}}_{\mathrm{k}}$ *is definable in* $\mathrm{FO}(\mathrm{Most}^1)$.

Proof. Note first that the collection of τ-structures which correctly encode some boolean formula can be defined in the logic $\mathrm{FO}(\mathrm{Most}^1)$. It suffices to express that all structures in $\mathrm{MAJSAT}^{\mathrm{Str}}_{\mathrm{k}}$ are acyclic, which can be already expressed in MSO, and that the in-degrees and out-degrees of different types of elements are as wanted.

Thus it suffices to show that, given a structure $\mathfrak{A}_F$ encoding a boolean formula F, we can decide if $\mathfrak{A}_F$ belongs to $\mathrm{MAJSAT}^{\mathrm{Str}}_{\mathrm{k}}$ or not. Given sets $X_i \subseteq I_i^{\mathfrak{A}_F}$, it is easy to construct a formula $\varphi = \exists Y \psi$, ψ first-order, such that

$$(\mathfrak{A}_F, X_1, \ldots, X_k) \models \varphi \text{ iff}$$

F is true under the assignment induced by $X_1, \ldots, X_k$, i.e., a variable in $\tilde{x}_i$ is set to true iff the corresponding element in I_i is in the set X_i. The formula $\psi(Y)$ says that $v \in Y$ and that Y contains those subformulas of F, including variables, which are made true by the assignment $X_1, \ldots, X_k$. The class $\mathrm{MAJSAT}^{\mathrm{Str}}_{\mathrm{k}}$ can be now defined using the sentence

$$\chi = (\mathrm{Most}^1\, X_1 \subseteq I_1), \ldots, (\mathrm{Most}^1\, X_k \subseteq I_k)\, \varphi.$$

Note that the relativization of Most^1 can be easily expressed using the quantifier $\mathcal{R}^1$, i.e., a formula of the form $(\mathrm{Most}^1\, X \subseteq Y)\, \phi(X)$ can be written as

$$\mathcal{R}^1\, X, X\, (X \subseteq Y \wedge \phi(X), X \subseteq Y \wedge \neg\phi(X)).$$

Since, for example, $\mathbf{1}^{\mathfrak{A}} \notin I_i^{\mathfrak{A}}$, the formula χ is expressible in $\mathrm{FO}(\mathrm{Most}^1)$ by case 1 of Lemma 6.1. □

11. Conclusion

Let us summarize the results of this paper. In Sections 4–7, we have mainly studied the expressive power of logics over unary vocabularies. These results can be summarized in a succinct way as follows:

(i) $\mathrm{Sp}_0(\mathrm{MSO}(\mathrm{R})) =$ Presburger arithmetic,
(ii) $\mathrm{Sp}_0(\mathrm{MSO}(\mathrm{R}^n)_{n\in\mathbb{Z}_+}) = \Delta_0\text{-arithmetic} = \mathcal{R}$,
(iii) $\mathcal{R} \leq \mathrm{Sp}_0(\mathrm{FO}(\mathrm{Most}^1)) \leq \mathrm{Sp}(\mathrm{FO}(\mathrm{M})) = \mathcal{R}^\sharp$.

In Section 9, we showed that

$$\mathrm{Sp}(\mathrm{FO}(\mathrm{M})) \subsetneq \mathrm{Sp}(\mathrm{FO}(\mathrm{Most}^1)),$$

which was used to show that $\mathrm{FO}(\mathrm{Most}^1) < \mathrm{FO}(\mathrm{Most}^2)$. In Section 8, we showed that on strings the logic $\mathrm{FO}(\mathrm{Most}^1)$ captures the complexity class LINCH. For comparison, let us recall the following well-known characterizations:

(i) $\mathrm{FO}(+, \times) \equiv$ LH, i.e., the logarithmic-time hierarchy,
(ii) $\mathrm{MSO}(+) \equiv$ LINH,
(iii) $\mathrm{SO} \equiv$ PH.

The complexity classes LH, LINH, and PH can be defined in terms of alternating Turing machines running, respectively, in logarithmic, linear, and polynomial time with $O(1)$ alternations. For the first equivalence, built-in arithmetic is needed. The second equivalence holds on strings (or more generally unary vocabularies), and the last equivalence holds also on unordered structures.

The counting extensions of these hierarchies can be defined by changing the machine model to the so-called threshold turing machine introduced in [27]. The counting hierarchy corresponds to polynomial time and LINCH to linear time, both with $O(1)$ uses of the threshold operation allowed. It was observed in [28] that threshold turing machine time $O(t(n))$ with $O(1)$ thresholds corresponds to uniform threshold circuits of size $2^{O(t(n))}$ and depth $O(1)$ for every complexity function $t(n) = \Omega(\log n)$. It follows that the languages recognized in logarithmic time and $O(1)$ thresholds (LCH) correspond to languages in uniform TC^0. By combining the logical characterization of uniform TC^0 [15] with the logical characterizations of LINCH (Theorem 8.9 and Corollary 8.10) and CH [1], we have

(i) $\mathrm{FO(M)}(+, \times) \equiv \mathrm{LCH}$,
(ii) $\mathrm{FO}(\mathrm{Most}^1) \equiv \mathrm{LINCH}$,
(iii) $\mathrm{FO}(\mathrm{Most}^k)_{k\in\mathbb{Z}^+} \equiv \mathrm{CH}$.

Analogously to above, the arithmetic predicates $+$ and $\times$ are needed for the first equivalence. The second equivalence holds on strings (unary vocabularies), and needs the built-in ordering. The last equivalence holds also on unordered structures.

Let us conclude by discussing some open problems and directions for further study. Monadic second-order logic and many of its fragments have been studied extensively. In the same spirit, it would be interesting to isolate fragments of $\mathrm{FO}(\mathrm{Most}^1)$ that are relevant, e.g., from the computational perspective. Related to this we note that, on unordered relational structures, any sentence of the form

$$\mathrm{Most}^1 X_1, \ldots, \mathrm{Most}^1 X_k \psi,$$

where ψ is first-order, has asymptotic probability 0 or 1 by Corollary 5.11 in [1]. However, it is quite easy to construct a formula of the form $\exists x\psi$, where $qr(\psi) = 1$ (no nesting of the quantifier Most^1), which is true in almost all graphs of odd cardinality and false in all graphs of even cardinality.

An interesting problem left unanswered is: is $\mathrm{FO}(\mathrm{Most}^1)[\tau] > \mathrm{MSO}(\mathrm{R}^k)_{k\in\mathbb{Z}^+}$ over some vocabulary τ. A different kind of open question is to determine whether the quantifier $\mathcal{R}^1$ is definable in $\mathrm{FO}(\mathrm{Most}^1)$. It is possible that $\mathcal{R}^1$ is not definable in $\mathrm{FO}(\mathrm{Most}^1)$ but we still have $\mathrm{FO}(\mathrm{Most}^1) \equiv \mathrm{FO}(\mathcal{R}^1)$. Over ordered structures, the quantifier $\mathcal{R}^1$ is definable in $\mathrm{FO}(\mathrm{Most}^1)$ by the same argument as in Theorem 3.5 [1].

Acknowledgments

The authors thank Lauri Hella for valuable comments and suggestions. We are also grateful to the anonymous referees for their valuable comments which helped us to improve the presentation of the results considerably.

References

[1] J. Kontinen, A logical characterization of the counting hierarchy, ACM Trans. Comput. Log. 10 (2009), Article 7, 21 pp.
[2] R. Fagin, Generalized first-order spectra and polynomial-time recognizable sets, in: Complexity of computation (Proc. SIAM-AMS Sympos. Appl. Math., New York, 1973), SIAM–AMS Proc., Am. Math. Soc., Providence, R.I., vol. VII, 1974, pp. 43–73.
[3] L.J. Stockmeyer, The polynomial-time hierarchy, Theoret. Comput. Sci. 3 (1976) 1–22.
[4] R. Fagin, L.J. Stockmeyer, M.Y. Vardi, On monadic NP vs monadic co-NP, Inform. Comput. 120 (1995) 78–92.
[5] O. Matz, N. Schweikardt, W. Thomas, The monadic quantifier alternation hierarchy over grids and graphs, Inform. Comput. 179 (2002) 356–383.
[6] K. Wagner, The complexity of combinatorial problems with succint input representation, Acta Inform. 23 (1986) 325–356.
[7] J. Torán, Complexity classes defined by counting quantifiers, J. Assoc. Comput. Mach. 38 (1991) 753–774.
[8] A. Durand, M. More, Nonerasing, counting, and majority over the linear time hierarchy, Inform. Comput. 174 (2002) 132–142.
[9] M. More, F. Olive, Rudimentary languages and second-order logic, Math. Logic Quart. 43 (1997) 419–426.
[10] P. Lindström, First order predicate logic with generalized quantifiers, Theoria 32 (1966) 186–195.
[11] A. Andersson, On second-order generalized quantifiers and finite structures, Ann. Pure Appl. Logic 115 (2002) 1–32.
[12] J. Kontinen, Definability of second order generalized quantifiers, Arch. Math. Logic 49 (2010) 379–398.
[13] M. Presburger, Über die Vollständigkeit eines gewissen Systems der Arithmetik ganzer Zahlen, in welchem die Addition als einzige Operation hervortritt, Comptes Rendus du I congrés de Mathématiciens des Pays Slaves (1929) 92–101.
[14] K. Harrow, Sub-elementary Classes of Functions and Relations, Ph.D. thesis, New York University, Department of Mathematics, 1973.
[15] D.A.M. Barrington, N. Immerman, H. Straubing, On uniformity within NC^1, J. Comput. Syst. Sci. 41 (1990) 274–306.
[16] W. Hesse, E. Allender, D.A.M. Barrington, Uniform constant-depth threshold circuits for division and iterated multiplication, J. Comput. Syst. Sci. 65 (2002) 695–716.
[17] C. Wrathall, Rudimentary predicates and relative computation, SIAM J. Comput. 7 (1978) 194–209.
[18] H.-A. Esbelin, M. More, Rudimentary relations and primitive recursion: a toolbox, Theoret. Comput. Sci. 193 (1998) 129–148.
[19] N.D. Jones, A.L. Selman, Turing machines and the spectra of first-order formulas, J. Symbolic Logic 39 (1974) 139–150.
[20] N. Immerman, Descriptive Complexity, Graduate Texts in Computer Science, Springer-Verlag, New York, 1999.
[21] N. Schweikardt, Arithmetic, first-order logic, and counting quantifiers, ACM Trans. Comput. Log. 6 (2005) 634–671.
[22] S. Toda, PP is as hard as the polynomial-time hierarchy, SIAM J. Comput. 20 (1991) 865–877.
[23] N. Schweikardt, On the expressive power of monadic least fixed point logic, Theoret. Comput. Sci. 350 (2006) 325–344.
[24] M.Y. Vardi, On the complexity of bounded-variable queries, in: Proceedings of the Fourteenth ACM Symposium on Principles of Database Systems, ACM Press, 1995, pp. 266–276.
[25] J.H. Bennett, On Spectra, Ph.D. thesis, Princeton University, 1962.
[26] L. Hella, J.M. Turull-Torres, Complete problems for higher order logics, in: Computer Science Logic, Lecture Notes in Computer Science, vol. 4207, Springer, Berlin, 2006, pp. 380–394.
[27] I. Parberry, G. Schnitger, Parallel computation with threshold functions, J. Comput. Syst. Sci. 36 (1988) 278–302.
[28] E. Allender, The permanent requires large uniform threshold circuits, Chicago J. Theoret. Comput. Sci. (1999), Article 7, 19 pp (electronic).