# On the Existential Arithmetics with Addition and Bitwise Minimum

Mikhail R. Starchak(✉)

St. Petersburg State University, St. Petersburg, Russia
m.starchak@spbu.ru

**Abstract.** This paper presents a similar approach for existential first-order characterizations of the languages recognizable by finite automata, by Parikh automata, and by multi-counter machines over the alphabet $\{0, 1, ..., k-1\}^n$ for some $k \geq 2$. The set of $k$-FA-recognizable relations coincides with the set of relations, which are existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$, where $\&_k$ corresponds to the bitwise minimum of base $k$. In order to obtain an existential first-order description of $k$-Parikh automata languages, we extend this structure with the predicate $EqNZB_k(x, y)$ which is true if and only if $x$ and $y$ have the same number of non-zero bits in $k$-ary encoding. Using essentially the same ideas, we encode computations of $k$-multi-counter machines and thus show that every recursively enumerable relation over the natural numbers is existentially definable in the aforementioned structure supplemented with concatenation $z = x \frown_k y \rightleftharpoons z = x + k^{l_k(x)} y$, where $l_k(x)$ is the bit-length of $x$ in base $k$. This result gives us another proof of DPR-theorem.

**Keywords:** Bitwise minimum · Büchi arithmetic · Parikh automata · Existential definability · Recursively enumerable sets · DPR-theorem · Concatenation

## 1 Introduction

In a recent paper [11], Haase and Różycki considered definability problems in $k$-Büchi arithmetic, an extension of Presburger arithmetic with a relation $V_k$ such that $V_k(x, y)$ if and only if $x$ is the largest power of $k$ that divides $y$. They proved that there are relations which are definable in $k$-Büchi arithmetic ($k$-definable) and not definable by any existential formula of the corresponding language. By a slight modification of a theorem of Villemaire [24, Corollary 2.4], they show that every $k$-definable relation can actually be expressed via some $\exists\forall$-formula, whereas Villemaire constructs a $\exists\forall\exists$-formula.

Büchi arithmetic of base $k \geq 2$ can be considered as a first-order characterization of the languages, recognizable by finite-state automata over the alphabet $\{0, 1, ..., k-1\}^n$ (called $k$-FA-recognizable). Interpreting the words of this language as tuples $(x_1, ..., x_n)$ of natural numbers in base $k$ encoding, we obtain the Büchi-Bruyère theorem [3,5], which states that every relation $R \subseteq \mathbb{N}^n$ is $k$-FA-recognizable if and only if it is $k$-definable. A second-order version of this theorem

O. Kupferman and P. Sobocinski (Eds.): FoSSaCS 2023, LNCS 13992, pp. 176–195, 2023.
https://doi.org/10.1007/978-3-031-30829-1_9

(which was proved independently by Büchi [5], Elgot [9], and Trakhtenbrot [22]) says that every relation is 2-FA-recognizable iff it is weak monadic second-order (WMSO-)definable in the structure $\langle\mathbb{N}; S\rangle$, where $S$ is a unary function symbol for the successor function over the natural numbers. The WMSO-theory of $\langle\mathbb{N}; S\rangle$ is usually denoted by WS1S.

Coming back to the Villemaire's result, we see that his encoding of $k$-FA via $\exists\forall\exists$-formulas of the language of $k$-Büchi arithmetic uses a unique bounded universal quantifier. A similar construction often appears in logical descriptions of abstract machines. For example, Klaedtke and Rueß considered in [16] various definability and decidability properties for WMSO-formulas with successor $S$ and cardinality constraints of the form $|X_1| + ... + |X_r| < |Y_1| + ... + |Y_s|$; the corresponding WMSO-theory of $\mathbb{N}$ was denoted by WS1S$^{\text{card}}$. They introduced Parikh automata, an extension of finite automata, and obtained an analogue of Büchi's Theorem, namely every relation recognizable by a Parikh automaton over the alphabet $\{0, 1\}^n$ is existentially WMSO-definable in $\mathbb{N}$ with $S$ and cardinality constraints, and vice versa. Here, only second-order variables are existentially quantified, while the formula, which describes a computation of a given Parikh automaton, still contains a universally quantified first-order variable (see [16, Theorem 10], where the universal quantifier $\forall x$ can be bounded by the maximal element of the existentially quantified second-order variable $U$).

Note that while WS1S is decidable, WS1S$^{\text{card}}$ is already undecidable, and its decidable fragments [16, Theorem 16] were obtained as a consequence of decidability of the emptiness problem for Parikh automata. Translating these undecidability results into first-order context, Bès showed [2, Proposition 3.8] in particular that the graph of multiplication function is definable in the structure $\langle\mathbb{N}; 0, 1, +, V_2, \mathit{EqNonZeroBits}, =\rangle$, where $\mathit{EqNonZeroBits}(x, y)$ is true iff $x$ and $y$ have the same number of non-zero bits in their binary representations. This implies undecidability of the first-order theory of this structure, but it is not known, for example, whether the existential first-order theory is decidable. In the concluding section [2], Bès remarks that *"it would be interesting to study the expressive power of fragments of FO arithmetic which include predicates like EqNonZeroBits"*. We will further shorten the name of this predicate to $\mathit{EqNZB}$.

The Davis-Putnam-Robinson theorem (DPR-theorem) [8] was a milestone in the undecidability proof of the Hilbert's Tenth Problem. This theorem states that every relation $R \subseteq \mathbb{N}^n$ is recursively enumerable (r.e.) if and only if it is existentially first-order definable in the structure $\langle\mathbb{N}; 0, 1, +, \cdot, \mathit{exp}, =\rangle$ (these relations are also called *exponential diophantine*). As the starting point, the proof uses the result of Davis [7], which states that every r.e. set is $\exists\forall\exists$-definable in the structure $\langle\mathbb{N}; 0, 1, +, \cdot, =\rangle$ with one bounded universal quantifier. It is important for us that elimination of this quantifier in the proof of DPR-theorem involves multiplication, factorial, binomial coefficients, and does not seem useful when we try to eliminate bounded universal quantifier in weaker structures. However in 1976, Matiyasevich presented an alternative proof of DPR-theorem [19] by purely existential encoding of computations of Turing machines, which thus gives us another approach for eliminating bounded universal quantifier [20, Section 6.1].

It is easy to modify the final steps of Matiyasevich's proof in order to obtain an existential formula of the language with 0, 1, addition, bitwise minimum &, and concatenation $\frown$, where $t = x \frown y \rightleftharpoons t = x + 2^{l(x)}y$ and $l(x)$ is the bit-length of $x$. Kummer's lemma [18] then plays a crucial role, since it gives an exponential diophantine representation of bitwise minimum (see also an exponential diophantine representation of *masking* relation $\preccurlyeq$ in [14]). Note that it is not difficult to define & in the structure $\langle \mathbb{N}; 0, 1, +, V_2, = \rangle$ by a formula with one bounded universal quantifier, whereas there is an existential formula that defines $V_2$ in $\langle \mathbb{N}; 0, 1, +, \&, = \rangle$. This suggests the question whether every 2-FA-recognizable relation is existentially first-order definable in $\langle \mathbb{N}; 0, 1, +, \&, = \rangle$.

In Theorem 1, we show that every relation is actually $k$-FA-recognizable if and only if it is existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$, where $\&_k$ corresponds to the binary bitwise minimum operation of base $k$. The same approach is applied in Theorem 2 to obtain an existential first-order characterization of the languages, recognizable by Parikh automata over the alphabet $\{0, 1, ..., k-1\}^n$. In this case, the structure must be extended by the binary predicate $EqNZB_k$, which is true for those pairs of natural numbers $(x, y)$ such that $x$ and $y$ have the same number of non-zero bits of base $k$.

Applying essentially the same ideas as in Theorem 1, we are able to show in Theorem 3 that every relation $R \subseteq \mathbb{N}^n$ is recognizable by multi-counter machines over the alphabet $\{0, 1, ..., k-1\}^n$ if and only if it is existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, \frown_k, = \rangle$, where $z = x \frown_k y \rightleftharpoons z = x + k^{l_k(x)}y$ and $l_k(x)$ is the bit-length of $x$ in base $k$. Since such machines recognize exactly r.e. sets, this provides yet another [14,19,20] proof of DPR-theorem by purely existential arithmetization of abstract machines.

## 2 Definitions and the main example

This section recalls some basic definitions from logic and automata theory, which will be used in the sequel. Then we illustrate the main idea of the existential characterisations constructed in Sections 3 and 4.

### 2.1 Definability and automata

**First-order definability.** The domain of all the structures considered in this paper will be the set of natural numbers $\mathbb{N} = \{0, 1, 2, ...\}$, and we will consider existential definability in some extensions of $\langle \mathbb{N}; 0, 1, +, = \rangle$.

Denote by $L_\sigma$ the first-order language of some signature $\sigma$. An $L_\sigma$-formula $\varphi$ is existential if it has the form $\exists \overline{x} \psi(\overline{x}, \overline{y})$, where $\psi(\overline{x}, \overline{y})$ is a quantifier-free $L_\sigma$-formula. Here, $\overline{x}$ denotes a list of variables $x_1, ..., x_n$. We say that an $n$-ary relation $R$ over $\mathbb{N}$ is *first-order (FO-)definable in the structure* $\langle \mathbb{N}; \sigma \rangle$ if there exists an $L_\sigma$-formula $\varphi(\overline{x})$ such that for every $\overline{a} \in \mathbb{N}^n$ we have $R(\overline{a})$ if and only if $\varphi(\overline{a})$. When the formula $\varphi(\overline{x})$ is existential, the corresponding relation is called *existentially first-order (∃FO-)definable*, and similarly for the case of quantifier-free formulas, universal formulas and other quantifier prefixes. We will subsequently write the prefix “FO” in the cases where we also discuss second-order definability, and in general it will be omitted.

In this paragraph, we focus on definability in the structure $\langle \mathbb{N}; 0, 1, +, V_k, = \rangle$, where $k \geq 2$ is an integer, and $V_k$ is a binary relation such that $V_k(x, y)$ if and only if $x$ is the largest power of $k$ dividing $y$. Büchi arithmetic of base $k$ is the first-order theory of this structure. The relations definable in this structure are called *$k$-definable.* Recall that for every multiplicatively independent integer $l \geq 2$ (i.e., $k^a \neq l^b$ for every positive integers $a, b$), $V_l$ is not definable in $\langle \mathbb{N}; 0, 1, +, V_k, = \rangle$ [23,24] (see also a generalization of this result by Bès [1]). In the following, we consider some fixed base $k$. Let $\&_k$ be the binary bitwise minimum operation of base $k$, where we assume that the natural number of smaller bit-length is supplemented with a sufficient number of leading zeros. For example, we have $120202 \,\&_3\, 21201201 = 100201$. It is not difficult to prove the following lemma.

**Lemma 1.** *Every relation is $k$-definable if and only if it is definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$.*

*Proof.* In order to define bitwise minimum, for every $j \in [0..k-1]$ we use the relation $X_{k,j}(x, y)$, which is defined as *“$x$ is a power of $k$ and the coefficient of this power of $k$ in the representation of $y$ in base $k$ equals $j$”.* There is a simple existential formula for this relation in [4,11,24]:

$$X_{k,j}(x, y) \rightleftharpoons V_k(x, x) \wedge \exists z \exists t \exists u (y = z + jx + t \wedge z < x \wedge (t = 0 \vee (V_k(u, t) \wedge x < u))),$$

where $x < y \rightleftharpoons \exists z (y = x + z + 1)$. Therefore, the graph of bitwise minimum can be expressed by a formula with a universal quantifier

$$z = x \&_k y \rightleftharpoons \forall t \bigwedge_{(i,j) \in [0..k-1]^2} \left( X_{k,i}(t, x) \wedge X_{k,j}(t, y) \Leftrightarrow X_{k,\min(i,j)}(t, z) \right).$$

For the converse, by using monus $z = x - y \rightleftharpoons (z = 0 \wedge x < y) \vee (x = z + y)$, define the set of powers of $k$ by the formula $P_k(x) \Leftrightarrow (kx - 1) \&_k x = x \wedge \neg x = 0$. Finally, we have $V_k(x, y) \Leftrightarrow P_k(x) \wedge \bigvee_{j \in [1..k-1]} (kx - 1) \&_k y = jx$. □

We see that $X_{k,j}(x, y)$ can be defined in $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$ by the quantifier-free formula $P_k(x) \wedge y \&_k x = jx$. Let $\lambda_k(x)$ be the greatest power of $k$ less or equal to $x$ when $x > 0$, and $\lambda_k(0) = 1$. Formally, we have the definition $y = \lambda_k(x) \Leftrightarrow (x = 0 \wedge y = 1) \vee (P_k(y) \wedge y \leq x \wedge x < y)$. Now an analogue of bitwise negation can be defined as follows: $\sim_k (y, x) = (k\lambda_k(y) - 1) - x \&_k (k\lambda_k(y) - 1)$. Here, $\sim_k (y, x)$ has the same bit-length as $y$, and we assume that $\&_k$ has a higher precedence than $+$ or monus. For our purposes, it is useful to include in the signature a binary function symbol for bitwise maximum

$$\begin{aligned} z = x|_k y \Leftrightarrow\ & (x < y \wedge z = \sim_k (y, \sim_k (y, x) \&_k \sim_k (y, y)) \vee \\ & (y \leq x \wedge z = \sim_k (x, \sim_k (x, x) \&_k \sim_k (x, y)). \end{aligned}$$

We will write $\frac{x}{k^n}$ with some fixed natural number $n$ for the function whose graph is quantifier-free definable by the formula $y = \frac{x}{k^n} \Leftrightarrow k^n y \leq x \wedge x < k^n(y+1)$. The function $\mathbf{1}_k(y)$ gives a natural number of the same bit-length with $y$, but with all $k$-ary digits equal to one: $x = \mathbf{1}_k(y) \Leftrightarrow (k-1)x = k\lambda_k(y) - 1$. For notational convenience, let us introduce a binary predicate symbol $\preccurlyeq_k$ such that $x \preccurlyeq_k y \rightleftharpoons x \&_k y = x$. The following lemma summarizes these definability results and will be implicitly used in the next sections.

**Lemma 2.** *The predicates $P_k$, $V_k$, $X_{k,j}$, $<$, $\leq$ and the graphs of functions $-$, $\lambda_k$, $\sim_k$, $\mathbf{1}_k$, $|_k$, and $\dot{\overline{k^n}}$ for every fixed $n \geq 1$ are $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$.*

The existential encoding of $k$-automata in Subsection 2.2 uses a $\exists$-definable function, which echoes a construction that was applied by Matiyasevich [19] in his arithmetization of Turing machines. For every $a \in [1..k-1]$ the function $\Theta_{k,a}(x)$ substitutes 1 for every digit of $x$ equal to $a$, and 0 otherwise. Then, the graph of this function is defined as follows:

$$\begin{aligned} y = \Theta_{k,a}(x) \Leftrightarrow \exists x_1 \ldots \exists x_{k-1} \Big( \bigwedge_{1 \leq i < j \leq k-1} & x_i \&_k x_j = 0 \wedge \\ & (x_1 + \ldots + x_{k-1}) \preccurlyeq_k \mathbf{1}_k(x) \wedge \\ & x_1 + 2x_2 + \ldots + (k-1)x_{k-1} = x \wedge y = x_a \Big). \end{aligned} \tag{1}$$

Note that each digit in the $k$-ary representation of every quantified variable in (1) is either 0 or 1. Moreover, if we denote $\bar{\mathbf{1}}_k(x) \rightleftharpoons x \&_k \mathbf{1}_k(x)$ then the sum $x_1 + \ldots + x_{k-1}$ is exactly $\bar{\mathbf{1}}_k(x)$. In the case of digit zero, the function $\Theta_{k,0}$ has an extra parameter that specifies the number of leading zeros, which must be replaced by ones:

$$y = \Theta_{k,0}(t, x) \Leftrightarrow y = \mathbf{1}_k(t) - \bar{\mathbf{1}}_k(x). \tag{2}$$

In particular, when $\lambda_k(t) < \lambda_k(x)$, we always have $\Theta_{k,0}(t,x) = 0$ and otherwise we obtain, for example, $\Theta_{3,0}(100000, 1020) = 110101$.

*Remark 1.* In Subsection 2.2 and Section 3 it is convenient to write $\Theta_{k,a}(t,x)$ instead of $\Theta_{k,a}(x)$ when $a \in \{1, \ldots, k-1\}$. In Section 4 there is no need to consider auxiliary zeros, and we use $\Theta_{k,a}$ with a single parameter assuming that $\Theta_{k,0}(x) \rightleftharpoons \Theta_{k,0}(x,x)$.

We conclude this paragraph by defining a set of natural numbers $\bar{\mathbf{1}}_k(\mathbb{N}) = \{\bar{\mathbf{1}}_k(x) \mid x \in \mathbb{N}\}$. This definition will be useful in the next paragraph.

**Second-order definability.** Similarly to Bès [2], let us denote by $\mathcal{F}$ the set of *finite* subsets of $\mathbb{N}$ and also define a function $cod_k : \mathcal{F}^n \to \mathbb{N}^n$ which maps every tuple $(X_1, \ldots, X_n) \in \mathcal{F}^n$ to the tuple of non-negative integers $cod_k(\overline{X}) = (\sum_{i \in X_1} k^i, \ldots, \sum_{i \in X_n} k^i)$. We see that the image of $cod_k$ is $\bar{\mathbf{1}}_k(\mathbb{N})$. This function establishes a connection between first-order definability and weak monadic second-order (WMSO-)definability in $\langle \mathbb{N}; S \rangle$ in the following way.

Recall that WMSO-language $L_\sigma^{WMSO}$ allows to quantify over finite subsets of the domain, and its signature $\sigma$ has auxiliary binary predicate symbol $\in$ for the membership relation $x \in X$. Again, let the domain of our structures be the set of natural numbers $\mathbb{N}$. Then a relation $R \subseteq \mathcal{F}^n$ is *WMSO-definable in the structure* $\langle \mathbb{N}; \sigma \rangle$ if there exists a $L_\sigma^{WMSO}$-formula $\varphi(X_1, ..., X_n)$ such that $R(\overline{A}) \Leftrightarrow \varphi(\overline{A})$ for every $\overline{A} \in \mathcal{F}^n$. As was explicitly shown by Villemaire [23, Theorem 3.3], every relation $R \subseteq \mathcal{F}^n$ is WMSO-definable in the structure $\langle \mathbb{N}; S \rangle$ if and only if $cod_2(R)$ is FO-definable in $\langle \mathbb{N}; 0, 1, +, V_2, = \rangle$.

Note that $cod_k$ is bijective only in the case $k = 2$ when we have $\mathbf{1}_2(\mathbb{N}) = \mathbb{N}$. In the case when $k > 2$, we can transfer FO-definability results for extensions of $k$-Büchi arithmetic to their WMSO-definability analogues using the function $\overline{cod}_k : \mathbb{N} \to \mathcal{F}^{k-1}$ which maps every $x \in \mathbb{N}$ to the tuple $\overline{cod}_k(x) = (cod_k^{-1}(\Theta_{k,1}(x)), ..., cod_k^{-1}(\Theta_{k,k-1}(x)))$. This function can obviously be extended such that $\overline{cod}_k : \mathbb{N}^n \to \left(\mathcal{F}^{k-1}\right)^n$. We use $\overline{cod}_k$ to establish a relationship between $\exists$FO-definability in $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, = \rangle$ and $\exists$WMSO-definability in $\langle \mathbb{N}; S \rangle$ extended with cardinality constraints of the form $|X_1| + ... + |X_r| < |Y_1| + ... + |Y_s|$. Section 3 focuses on the existential definability in these structures and recognizability by Parikh automata [16]. We say that $R \subseteq \mathcal{F}^n$ is *existentially ($\exists$) WMSO-definable in the structure* $\langle \mathbb{N}; \sigma \rangle$ if there exists an $L_\sigma^{WMSO}$-formula $\exists \overline{Y} \varphi(\overline{X}, \overline{Y})$, where $\varphi(\overline{X}, \overline{Y})$ may include arbitrary first-order quantifiers, such that for every $\overline{A} \in \mathcal{F}^n$ we have $R(\overline{A})$ if and only if $\exists \overline{Y} \varphi(\overline{A}, \overline{Y})$.

The following lemma shows that it is sufficient to extend $\langle \mathbb{N}; S \rangle$ with the relation $EqCard(X, Y) \rightleftharpoons |X| = |Y|$ to reason about $\exists$WMSO-definability in $\mathbb{N}$ with successor $S$ and cardinality constraints.

**Lemma 3.** *Every cardinality constraint $|X_1| + ... + |X_r| < |Y_1| + ... + |Y_s|$ is existentially WMSO-definable in the structure $\langle \mathbb{N}; S, EqCard \rangle$.*

*Proof.* Let us first define the graph of $\cap$ using a formula with one universal first-order quantifier $\forall x (x \in Z \Leftrightarrow x \in X \wedge x \in Y)$ (and analogously, the graphs of union $Z = X \cup Y$ and difference $Z = X \setminus Y$) and the empty set $X = \emptyset \Leftrightarrow \forall x (\neg x \in X)$.

Now it is not difficult to see that

$$\begin{aligned} |X_1| + ... + |X_r| < |Y_1| + ... + |Y_s| \Leftrightarrow \exists U \exists V \exists X_1' ... \exists X_r' \exists Y_1' ... \exists Y_s' \Big( \\ \bigwedge_{1 \leq i < j \leq r} X_i' \cap X_j' = \emptyset \wedge \bigwedge_{1 \leq i \leq r} EqCard(X_i, X_i') \wedge \\ \bigwedge_{1 \leq i < j \leq s} Y_i' \cap Y_j' = \emptyset \wedge \bigwedge_{1 \leq i \leq s} EqCard(Y_i, Y_i') \wedge \\ \bigcup_{1 \leq i \leq r} X_i' = U \wedge \bigcup_{1 \leq i \leq s} Y_i' = V \wedge U \cap V = U \wedge \neg(V \setminus U = \emptyset) \Big). \end{aligned} \tag{3}$$

□

The following fact is an analogue of Villemaire's theorem [23]. Note that when $k = 2$ the function $\overline{cod}_2$ is exactly $cod_2^{-1}$.

**Proposition 1.** *(i) If a relation $R \subseteq \mathcal{F}^n$ is existentially WMSO-definable in the structure $\langle \mathbb{N}; S, EqCard\rangle$ then $cod_k(R)$ is existentially FO-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, =\rangle$.*

*(ii) If a relation $R \subseteq \mathbb{N}^n$ is $\exists$FO-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, =\rangle$ then $\overline{cod}_k(R)$ is $\exists$WMSO-definable in $\langle \mathbb{N}; S, EqCard\rangle$.*

The proof of this proposition is rather straightforward and follows along similar lines as the proof of Villemaire's theorem. Only notice that in order to deal with universal FO-quantifiers in *(i)*, we apply Corollary 1 from Subsection 2.2.

Klaedtke and Rueß show in [16] that every relation $R \subseteq \mathcal{F}^n$ is existentially WMSO-definable in the structure $\langle \mathbb{N}; S, EqCard\rangle$ if and only if it is recognizable by some Parikh automaton over the alphabet $\{0, 1\}$. By reduction to the emptiness problem for Parikh automata, they show that satisfiability of existential WMSO-formulas in the structure $\langle \mathbb{N}; S, EqCard\rangle$ is decidable. The next paragraph gives the necessary definitions.

**Automata languages.** Büchi-Bruyère's theorem [4,5] states that every relation is first-order definable in the structure $\langle \mathbb{N}; 0, 1, +, V_k, =\rangle$ if and only if it is recognizable by a finite $k$-automaton. Haase and Różycki [11] prove that this statement is however not true if we consider *existential* first-order definability in $\langle \mathbb{N}; 0, 1, +, V_k, =\rangle$. We first recall some automata-theoretic definitions and then show that substituting $\&_k$ for $V_k$ yields the desired existential description of $k$-recognizable sets.

Let $\Sigma$ be some alphabet and $\Sigma^*$ denote the set of words of finite length over $\Sigma$ with a unique empty word $\epsilon$ of length 0. Then a *(non-deterministic) finite $\Sigma$-automaton ($\Sigma$-FA)* is a 4-tuple $\mathcal{A} = (Q, q_0, F, \delta)$, where $Q = \{q_0, ..., q_s\}$ is a finite set of states with initial state $q_0$ and the set $F \subseteq Q$ of finial states; $\delta : Q \times \Sigma \to 2^Q$ is the transition function, where $2^Q$ is the power set of $Q$. A configuration of $\mathcal{A}$ is a pair $(q, x)$, where $q \in Q$ is a current state and $x \in \Sigma^*$ is an unused part of an input word. A transition relation $\to$ over configurations of $\mathcal{A}$ is defined such that $(q, ax) \to (q', x)$ if and only if $q' \in \delta(q, a)$. A sequence of transitions between configurations is called a *computation of $\mathcal{A}$*. We say that $x = x_0 x_1 \cdots x_t \in \Sigma^{t+1}$ is accepted by a given $\Sigma$-FA $\mathcal{A}$ if there is an accepting computation of $\mathcal{A}$ for $x$, that is, a sequence $(q_0, x_0 x_1 ... x_t) \to (q', x_1 ... x_t) \to \cdots \to (q'', x_t) \to (q_f, \epsilon)$ for some $q_f \in F$. The set of all words $x \in \Sigma^*$ accepted by $\Sigma$-FA $\mathcal{A}$ defines the language recognizable by this automaton. This language is denoted by $L(\mathcal{A})$.

A *finite $k$-automaton ($k$-FA)* is defined as a $\Sigma_k^n$-FA, where every letter from $\Sigma_k^n$ is an $n$-tuple of digits from $\Sigma_k = \{0, 1, ..., k-1\}$. To each language $L \subseteq (\Sigma_k^n)^*$ there corresponds a relation $R_L$ over $\mathbb{N}^n$ in the following way: $R_L = \{\sum_{i=0}^{t} x_i k^i \mid x_0 \cdots x_t \in L\}$. An $n$-ary relation $R$ over $\mathbb{N}$ is called *$k$-FA-recognizable* if there exists a $k$-FA $\mathcal{A}$ such that for every $\overline{a} \in \mathbb{N}^n$ we have $R(\overline{a}) \Leftrightarrow R_{L(\mathcal{A})}(\overline{a})$. For technical convenience, the notion of $k$-recognizability is commonly defined [4,23,24] for deterministic $k$-FA ($k$-DFA), where for every state $q$ and letter $a \in \Sigma_k^n$ it holds that $|\delta(q, a)| \leq 1$. Since $\Sigma$-FA and $\Sigma$-DFA recognize the same class of languages [17], i.e. the class of regular languages over the alphabet $\Sigma$, this restriction does not change the class of recognizable relations. In our logical characterization of $k$-FA-recognizable relations we will not benefit from such restrictions on the transition function.

The definition of $\Sigma$-FA can be extended by adjoining to every letter of $\Sigma$ a vector $v \in D$, where $D$ is a finite subset of $\mathbb{N}^m$, and imposing certain restrictions on the accepting sequences of transitions to obtain *Parikh finite automata* (*$\Sigma$-PFA*). That is, for some $m > 0$ and a finite set $D \subseteq \mathbb{N}^m$, a $\Sigma$-PFA is a pair $(\mathcal{A}, \varphi)$, denoted by $\mathcal{A}_\varphi$, where $\mathcal{A}$ is a $(\Sigma \times D)$-FA and $\varphi(x_1, ..., x_m)$ is an existential $L_{\langle 0,1,+,=\rangle}$-formula. It is convenient to think of a configuration of $\Sigma$-PFA as an $(m+2)$-tuple $(q, x, y_1, ..., y_m)$ where the pair $(q, x)$ is the same as in the definition of configurations of $\Sigma$-FA, and $(y_1, ..., y_m)$ is a vector from $\mathbb{N}^m$. A transition relation between two configurations of $\Sigma$-PFA $\mathcal{A}_\varphi$ is now defined as follows: $(q, ax, y_1, ..., y_m) \to (q', x, y_1+d_1, ..., y_m+d_m)$ if and only if $q' \in \delta(q, a, d_1, ..., d_m)$. A word $x = x_0x_1 \cdots x_t \in \Sigma^{t+1}$ is accepted by $\mathcal{A}_\varphi$ if there is a computation $(q_0, x_0x_1 \cdots x_t, 0, ..., 0) \to (q', x_1 \cdots x_t, y_1', ..., y_m') \to \cdots \to (q'', x_t, y_1'', ..., y_m'') \to (q_f, \epsilon, y_1, ..., y_m)$ for some $q_f \in F$ and the formula $\varphi(y_1, ..., y_m)$ is true. We denote by $L(\mathcal{A}_\varphi)$ the language recognizable by $\Sigma$-PFA $\mathcal{A}_\varphi$.

In order to deal with definability over the natural numbers, we again consider $\Sigma_k^n$-PFA, which we call a *$k$-Parikh finite automata* (*$k$-PFA*). The $k$-PFA-recognizable relations $R \in \mathbb{N}^n$ are defined analogously. The prefixes $\Sigma$- and $k$- will be sometimes omitted when the exact alphabet $\Sigma$ or value of $k$ is not significant.

The original definition of Parikh automata [16] uses semi-linear sets $C \subseteq \mathbb{N}^t$ instead of existential formulas of Presburger arithmetic, but it is well-known [10] that these definitions of PFA are equivalent. The main result by Klaedtke and Rueß [15, Theorems 12 and 15] states that every relation $R \subseteq \mathcal{F}^n$ is ∃WMSO-definable in the structure $\langle \mathbb{N}; S, \mathit{EqCard} \rangle$ if and only if the relation $\mathit{cod}_2^{-1}(R)$ is 2-PFA-recognizable. The "only if" part of this WMSO-characterization follows from the fact that the class of languages recognizable by PFA is closed under union, intersection, left and right quotients [15, Property 4] and that *EqCard* with its negation are recognizable by 2-PFA. Since it is easy to construct $k$-PFA for the predicate $\mathit{EqNZB}_k$ and for its negation, the following proposition can be proved in a similar way.

**Proposition 2.** *If some relation $R \subseteq \mathbb{N}^n$ is existentially FO-definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, \mathit{EqNZB}_k, = \rangle$ then it is $k$-PFA-recognizable.*

Based on Parikh's theorem [21], Klaedtke and Rueß proved decidability of the emptiness problem for PFA, and thus decidability of the existential WMSO-theory of $\langle \mathbb{N}; S, \mathit{EqCard} \rangle$. They also proved that the universality problem for Parikh automata is undecidable. In contrast to finite automata, *deterministic* Parikh automata, where for every $(q, a) \in Q \times \Sigma_k^n$ there exists at most one pair $(q', \overline{d}) \in Q \times D$ such that $q' \in \delta(q, (a, \overline{d}))$, are less powerful than PFA. The paper by Cadilhac, Finkel and McKenzie [6] provides some explicit examples of languages recognizable by PFA but not by any deterministic PFA. These authors continued the study of other properties of PFA and, in particular, proved undecidability of the regularity property for PFA. This result will be used in Section 3.

### 2.2 Existential characterization of $k$-FA-recognizable languages

In this section we illustrate the main idea of the existential characterisation from Section 3. Our aim now is to prove the following theorem.

**Theorem 1.** *For an integer $k \geq 2$ every relation is $k$-FA-recognizable if and only if it is existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$.*

*Proof.* Let $\mathcal{A} = (Q, q_0, F, \delta)$ be a $k$-FA. We are going to prove existential definability of the relation $R_{L(\mathcal{A})}$ in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$ by encoding the existence of an accepting computation of $\mathcal{A}$ when the input word is the $k$-ary representation of $\overline{x} = x_1, ..., x_n$. To this end, let us first introduce new variables $\overline{q} = q_0, ..., q_s$ for every state $q_i \in Q$; for a state $p \in Q$, we denote by $\nu(p)$ its number from $[0..s]$. The following restriction on $\overline{q}$ expresses the fact that at each step of a computation the automaton $\mathcal{A}$ has a unique state from $Q$:

$$K_k(t, \overline{q}) \rightleftharpoons \bigwedge_{0 \leq i < j \leq s} q_i \&_k q_j = 0 \wedge q_0 + \ldots + q_s = \mathbf{1}_k(t) \wedge 1 \preccurlyeq_k q_0 \wedge \bigvee_{p \in F} t \preccurlyeq_k q_{\nu(p)}. \quad (4)$$

Here $t$ will be another existentially quantified variable that will be a power of $k$. This variable corresponds to a configuration $(p, \epsilon)$ for some $p \in F$, and formula (4) also requires that the computation starts in the state $q_0$. It is obvious that $t$ must be greater than $x_i$ for every $i \in [1..n]$; this restriction will appear in the resulting formula below.

In order to express the fact that each step of a computation is performed in accordance with the transition function $\delta : Q \times \varSigma_k^n \to 2^Q$, we introduce a predicate $\varDelta_{(p,\overline{a})}$. For every pair $(p, \overline{a}) \in Q \times \varSigma_k^n$, we have

$$\varDelta_{(p,\overline{a})}(t, \overline{q}, \overline{x}) \rightleftharpoons \left( q_{\nu(p)} \&_k \mathop{\&_k}_{i \in [1..n]} \varTheta_{k,a_i}(t, x_i) \right) \preccurlyeq_k \left( \mathop{\Big|_k}_{\widetilde{p} \in \delta(p,\overline{a})} \frac{q_{\nu(\widetilde{p})}}{k} \right), \quad (5)$$

where, by definition, $\mathop{\Big|_k}_{y \in \emptyset} y = 0$. From this formula we see that at each step of an accepting computation there are either no configurations with the state $p$ and a word starting with the letter $\overline{a} = (a_1, ..., a_n)$, or in the next configuration the state will be from $\delta(p, \overline{a})$. By combining formulas (4) and (5), we conclude that

$$R_{L(\mathcal{A})}(\overline{x}) \Leftrightarrow \exists t \exists \overline{q} \Big( P_k(t) \wedge \bigwedge_{i \in [1..n]} x_i < t \wedge K_k(t, \overline{q}) \wedge \bigwedge_{(p,\overline{a}) \in Q \times \varSigma_k^n} \varDelta_{(p,\overline{a})}(t, \overline{q}, \overline{x}) \Big). \quad (6)$$

It remains to use formulas (1) and (2), Büchi-Bruyère's theorem and Lemmas 1 and 2. □

**Corollary 1.** *If a relation is definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$ then it is existentially definable in this structure.*

This result for $k = 2$ can be transferred to the second-order case similarly to Proposition 1. Thus, we obtain a corollary, which was essentially proved by Elgot [9, Theorem 5.3 (b)].

**Corollary 2.** *If a relation $R \in \mathcal{F}^n$ is WMSO-definable in the structure $\langle \mathbb{N}; S \rangle$ then it is existentially WMSO-definable in this structure.*

## 3 First-order characterization of Parikh automata

The aim of this section is to prove the converse statement to Proposition 2 and thus obtain an existential first-order characterization of Parikh automata languages. Parikh map over the natural numbers can be defined as a function $\Phi_k : \mathbb{N} \to \mathbb{N}^k$ such that $\Phi_k(x) = (\#_{k,0}(x), ..., \#_{k,k-1}(x))$, where every function $\#_{k,i}$ counts the number of occurrences of the digit $i$ in $k$-ary representation of $x$. For such counting functions we have the following lemma.

**Lemma 4.** *Let $R(x_1, ..., x_n)$ be a relation that is existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, = \rangle$, and let $\overline{a}$ be some vector from $\{0, ..., k-1\}^n$. Then the relation $R(\#_{k,a_1}(x_1), ..., \#_{k,a_n}(x_n))$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, = \rangle$.*

*Proof.* It is sufficient to define the relations $\#_{k,a}(x) = d$ for integers $d \geq 0$ and $\#_{k,a}(x) + \#_{k,b}(y) = \#_{k,c}(z)$ by some existential formulas. For the first relation we have the formula $EqNZB_k(\Theta_{k,a}(x), k^d - 1)$, and for the second one there is the following first-order analogue to formula (3):

$$\#_{k,a}(x) + \#_{k,b}(y) = \#_{k,c}(z) \Leftrightarrow \exists x' \exists y' (EqNZB_k(x' + y', \Theta_{k,c}(z)) \wedge \\ x' \&_k y' = 0 \wedge EqNZB_k(\Theta_{k,a}(x), x') \wedge EqNZB_k(\Theta_{k,b}(y), y')).$$

It remains to use existential definability of the graph of $\Theta_{k,i}$ in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$.

Note that every function $\#_{k,i}$ can be represented in terms of Subsection 2.1 as $\#_{k,i}(x) = |cod_k^{-1}(\Theta_{k,i}(x))|$, and thus this lemma can also be proved using Lemma 3 and the first part of Proposition 1. □

Let $D$ be some finite subset of $\mathbb{N}^m$, and let $M(D)$ be the maximum integer occurring in $D$. The same as Klaedtke and Rueß [16], we encode vectors from $D$ of a given $k$-Parikh automaton by introducing $M(D) + 1$ new variables $y_{i,0}$,...,$y_{i,M(D)}$ for each coordinate $y_i$. For every $i \in [1..m]$, these variables will be pairwise *disjoint* (i.e. $y_{i,j_1} \&_k y_{i,j_2} = 0$ for $j_1 \neq j_2$) and their representation in base $k$ will contain only zeros and ones. For this reason, we use only $\#_{k,1}$ in our encoding and denote $\#_k \rightleftharpoons \#_{k,1}$.

**Theorem 2.** *For every integer $k \geq 2$ a relation $R \subseteq \mathbb{N}^n$ is k-PFA-recognizable if and only if it is $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, = \rangle$.*

*Proof.* The "if" direction of this theorem is Proposition 2. In the proof of the "only if" direction, suppose we are given a $k$-Parikh automaton $\mathcal{A}_\varphi$ for some finite set $D \in \mathbb{N}^m$, where $\mathcal{A} = (Q, q_0, F, \delta)$ is a FA over the language $\Sigma_k^n \times D$ and $\varphi$ is an existential $L_{\langle 0,1,+,= \rangle}$-formula. We are going to construct an existential $L_{\langle 0,1,+,\&_k, EqNZB_k, = \rangle}$-formula $\psi$ such that $R_{L(\mathcal{A}_\varphi)}(\overline{a})$ if and only if $\psi(\overline{a})$ for every $\overline{a} \in \mathbb{N}^n$. Again, $\psi(\overline{x})$ will encode the existence of an accepting computation of $\mathcal{A}_\varphi$ when the input word is the $k$-ary representation of $\overline{x}$.

The sequence of states from an accepting computation of $\mathcal{A}$ can be encoded using the predicate $K_k(t, \overline{q})$, defined by the existential $L_{\langle 0,1,+,\&_k,= \rangle}$-formula (4).

We modify formula (5) so that it works with the alphabet $\Sigma_k^n \times D$. To this end, let us introduce $m(M(D)+1)$ variables $\overline{y} = y_{1,0},...,y_{1,M(D)},...,y_{m,0},...,y_{m,M(D)}$ such that for every $i \in [1..m]$ it holds that $\theta_k(t, y_{i,0}, ..., y_{i,M(D)})$, where

$$\theta_k(t, y_0, ..., y_M) \rightleftharpoons \bigwedge_{0 \le i < j \le M} y_i \&_k y_j = 0 \wedge y_0 + ... + y_M = \mathbf{1}_k(t).$$

Now for every $(p, \overline{a}, \overline{d}) \in Q \times \Sigma_k^n \times D$ we have:

$$\Delta_{(p,\overline{a},\overline{d})}(t, \overline{q}, \overline{x}, \overline{y}) \rightleftharpoons \Big( q_{\nu(p)} \&_k \mathop{\&_k}_{i \in [1..n]} \Theta_{k,a_i}(t, x_i) \&_k \mathop{\&_k}_{j \in [1..m]} y_{j,d_j} \Big) \preccurlyeq_k \Bigg( \mathop{\Big|_k}_{\widetilde{p} \in \delta(p,\overline{a},\overline{d})} \frac{q_{\nu(\widetilde{p})}}{k} \Bigg).$$

Recall that the expression with bitwise maximums $\Big|_k$ evaluates to zero when $\delta(p, \overline{a}, \overline{d}) = \emptyset$.

By combining all the parts of the existential definition of $R_{L(\mathcal{A}_\varphi)}$, we get the following analogue to formula (6):

$$R_{L(\mathcal{A}_\varphi)}(\overline{x}) \Leftrightarrow \exists t \exists \overline{q} \exists \overline{y} \Bigg( P_k(t) \wedge \bigwedge_{i \in [1..n]} x_i < t \wedge K_k(t, \overline{q}) \wedge \\ \bigwedge_{i \in [1..m]} \theta_k(t, y_{i,0}, ..., y_{i,M(D)}) \wedge \bigwedge_{(p,\overline{a},\overline{d}) \in Q \times \Sigma_k^n \times D} \Delta_{(p,\overline{a},\overline{d})}(t, \overline{q}, \overline{x}, \overline{y}) \wedge \\ \varphi\Big( \sum_{c \in [1..M(D)]} c \#_k(y_{1,c}), ..., \sum_{c \in [1..M(D)]} c \#_k(y_{m,c}) \Big) \Bigg).$$

It remains to apply Lemma 4 to obtain the desired existential formula. □

This result gives us the following statement concerning decidability of fragments of the first-order theory of the structure $\langle \mathbb{N}; 0, 1, +, \&_k, \mathit{EqNZB}_k, = \rangle$.

**Corollary 3.** *The existential theory of $\langle \mathbb{N}; 0, 1, +, \&_k, \mathit{EqNZB}_k, = \rangle$ is decidable and the $\forall\exists$-theory of this structure is undecidable.*

*Proof.* The first part of the corollary is just a variation on the automata-theoretic techniques that were formalized by Hodgson [12]. It follows from the decidability of the emptiness problem for PFA. Undecidability of the universality problem, combined with Theorem 2, imply undecidability already for the problem of deciding $\forall\exists$-formulas with a single universal quantifier. □

Haase and Różycki [11, Conclusion] ask whether the property of $\exists$-definability is decidable for the relations definable in the structure $\langle \mathbb{N}; 0, 1, +, V_k, = \rangle$. Using Theorem 1, this problem can be reformulated so that we consider only existentially definable sets, but now the signatures are different. Namely, the question is whether we can decide if a set $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, V_k, \&_k, = \rangle$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, V_k, = \rangle$. A similar question can be answered in the negative for the structure with $\&_k$ and $\mathit{EqNZB}_k$.

**Proposition 3.** *The problem of deciding whether a set existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, = \rangle$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, = \rangle$ is undecidable.*

This follows from Theorems 1 and 2, and from undecidability of the regularity property for Parikh automata, which was proved by Cadilhac, Finkel and McKenzie [6, Proposition 7].

Parikh automata are closely related to multi-counter machines (MCM): they recognize exactly the same languages as reversal-bounded MCM [15, Section A.3] (see also [6, Subsection 3.3]). Recall that a MCM is *reversal-bounded* (the notion was introduced by Ibarra [13]) if there exists a pair of integers $(r, s)$ such that in every accepting computation the value of each counter increases and decreases at most $r$ times and the input head reverses at most $s$ times. Theorem 2 now gives an existential first-order characterization of this restricted version of MCM. It is clear that the model of PFA is more suitable for our logical descriptions. However, as we will see in the next section, the behaviour of MCM can be described in a similar way when the structure is extended with concatenation.

# 4 Multi-counter machines and DPR-theorem

## 4.1 Two-way multi-counter machines

Same as Ibarra [13], we define a *two-way multi-counter machine* $\mathcal{M}$ over an alphabet $\Sigma$ ($\Sigma$*-MCM*) with two special symbols $\vdash, \dashv$ as a tuple $(m, Q, q_0, F, \delta)$. Here, $m \geq 0$ is the number of the counters of $\mathcal{M}$, the triple $(Q, q_0, F)$ has its standard meaning, and $\delta$ is a function from $Q \times (\Sigma \cup \{\vdash, \dashv\}) \times \{0,1\}^m$ to $2^{Q \times \{-1,0,1\}^{m+1}}$. Every computation of $\mathcal{M}$ starts with an input $x \in \Sigma^*$ written on the tape between the delimiters: $\vdash x \dashv$, and the input head of $\mathcal{M}$ reading the left delimiter $\vdash$. A configuration of $\mathcal{M}$ on an input $\vdash x \dashv$ is given by an $(m+3)$-tuple $(q, \vdash x \dashv, i, y_1, ..., y_m)$ denoting the fact that $\mathcal{M}$ is in state $q$, the read-only input head scans the $i$-th symbol of the input, and $y_1$,...,$y_m$ are some non-negative integer values of the counters. The relation $\rightarrow$ over configurations is defined such that $(q, \vdash x \dashv, i, y_1, ..., y_m) \rightarrow (q', \vdash x \dashv, i + \Delta, y_1 + d_1, ..., y_m + d_m)$ if and only if $(q', \Delta, d_1, ..., d_m) \in \delta(q, a, [y_1 > 0], ..., [y_m > 0])$, where $a$ is the $i$-th symbol of the input and $[y > 0]$ returns 1 if $y > 0$, and 0 otherwise. A natural restriction on $\delta$ prevents the cases when: (1) $[y_j > 0] = 0$ and $d_j = -1$; (2) $i = 0$ and $\Delta = -1$; (3) the $i$-th symbol of the input is $\dashv$ and $\Delta = 1$.

We say that $x \in \Sigma^*$ is accepted by a given $\Sigma$-MCM if for the input word $\vdash x \dashv$ there is a computation $(q_0, \vdash x \dashv, 0, 0, ..., 0) \rightarrow ... \rightarrow (q_f, \vdash x \dashv, 0, 0, ..., 0)$ for some $q_f \in F$. The set of all the words $x \in \Sigma^*$ accepted by a $\Sigma$-MCM $\mathcal{M}$ defines the language recognized by this machine, which we denote by $L(\mathcal{M})$. In order to properly relate $\Sigma$-MCM with definability over $\mathbb{N}$, we again assume that $\Sigma = \Sigma_k^n$ for $k \geq 2$. Every $x \in \Sigma^*$ is now an element of $\mathbb{N}^n$ in the inverse base $k$ representation. An $n$-ary relation $R$ over $\mathbb{N}$ is called *k-MCM-recognizable* if there exists a $\Sigma_k^n$-MCM $\mathcal{M}$ such that for every $\overline{a} \in \mathbb{N}^n$ we have $R(\overline{a}) \Leftrightarrow R_{L(\mathcal{M})}(\overline{a})$.

Two-way multi-counter machines can simulate Turing machines (see e.g. [17]), and thus every relation $R$ over $\mathbb{N}^n$ is r.e. iff it is $k$-MCM-recognizable. The aim of this section is to use the same arguments as in the cases of $k$-FA and $k$-PFA in order to obtain an existential characterization of r.e. relations, and Theorem 3 gives us the desired result. The proof will be in some sense intermediate between the arithmetization of Turing machines by Matiyasevich [19] and the encoding of register machines by Jones and Matiyasevich in [14], but here we emphasize the role of concatenation in existential characterizations of multi-counter languages.

### 4.2 The role of concatenation in DPR-theorem

Matiyasevich's proof [19] implicitly gives us a description of every r.e. set via $\exists$-formulas of the first-order language with 0, 1, addition, bitwise multiplication $\&_2$, concatenation $\frown_2$, and equality. Here, $t = x \frown_k y \rightleftharpoons t = x + k^{l_k(x)}y = x + k\lambda_k(x)y$, where $l_k(x)$ is the length of $x$ in $k$-ary notation. This section aims to prove this theorem using the ideas from Subsection 2.2. Informally speaking, the main difference between the case of $k$-MCM and $k$-FA is that we now consider *byte*wise multiplication instead of *bit*wise from Theorem 1. Suppose a given $k$-MCM accepts $\overline{x} \in \Sigma_k^n$ and let $M$ be the maximum value of all the counters of some accepting computation for $\overline{x}$. If $u$ is a power of $k$ which is greater than the maximum of $k^M$ and all the $x_i$, then $l_k(u)$ will be the size of the byte in our encoding. Every non-negative integer can be represented as a sequence of bytes of size $l_k(u)$, which will be called *$u$-bytes*.

First, we introduce some auxiliary devices, which are required in our construction. Define the predicate $\Delta_k(u, t, x)$, which is true when $u$ is a power of $k$ greater than $k^2$, the variable $x$ has the same $u$-byte-length as $t$ and has the following form

$$x = 1\underbrace{000...0**}_{l_k(u)}...\underbrace{0..010..0}_{l_k(u)}...\underbrace{000...001}_{l_k(u)},$$

where $**$ is either 10 or 01, and for every two consecutive $u$-bytes $b_1, b_2$ in $x$ the only 1 in $b_2$ is either in the same place or one bit left/right of its position in $b_1$. Moreover, the two most significant bits in every $u$-byte are equal to zero. We will use this predicate to describe a position of the input head and values of the counters in configurations of a given $k$-MCM. Before we proceed with the existential definition of this relation, we need to introduce some auxiliary functions. The first one performs the right shift by $l_k(z)$ bits and can be defined via the formula $y = \frac{x}{z} \Leftrightarrow \exists v \exists u(\lambda_k(z) = u \wedge \lambda_k(v) \leq u \wedge x = u \frown_k y - u + v)$. The second function is $Copy_k(u, t, x)$ which maps to zero when $\lambda_k(u) < \lambda_k(x)$, and otherwise gives us the sequence of $u$-bytes of the same $u$-byte-length as $t$ such that each $u$-byte is equal to $x$. The following lemma gives the desired definition, and then we immediately prove existential definability of $\Delta_k(u, t, x)$.

**Lemma 5.** *The function $Copy_k$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, \frown_k, = \rangle$.*

*Proof.* We start with the predicate $Cpy_k(x, y)$ which is true whenever $y$ has the form $x \frown_k \dots \frown_k x$. Its definition is rather standard:

$$Cpy_k(x, y) \Leftrightarrow y = x \vee \exists z(y = x \frown_k z \wedge y = z \frown_k x).$$

The predicate $I_k(u,x) \Leftrightarrow x = 1 \vee \exists y(Cpy_k(\lambda_k(u), y) \wedge x = ky+1)$ is an another special case of $Copy_k$ which is true when $x$ is a sequence of $u$-bytes, each of which is equal to 1. Then, the minimum power of $k$ of the same $u$-byte-length as $x$ can be expressed as $y = \Lambda_k(u,x) \Leftrightarrow \exists v\,(I_k(u,v) \wedge v \le x \wedge v \frown_k u > x \wedge y = \lambda_k(v))$.

It is now clear that

$$
\begin{aligned}
y = Copy_k(u,t,x) \Leftrightarrow \lambda_k(u) < \lambda_k(x) \wedge y = 0 \vee \Lambda_k(u,y) = \Lambda_k(u,t) \ \wedge \\
\Big(\lambda_k(u) = \lambda_k(x) \wedge Cpy_k(x,y) \vee \lambda_k(u) > \lambda_k(x) \wedge \exists y' \exists y'' ( \\
Cpy_k(x + \lambda_k(u), y') \wedge Cpy_k(\lambda_k(u), y'') \wedge \lambda_k(y') = \lambda_k(y'') \wedge y = y' - y'')\Big).
\end{aligned}
$$

In this formula, the variables $y'$ and $y''$ are introduced in order to supplement every $u$-byte with a sufficient number of leading zeros. □

**Lemma 6.** *The relation $\Delta_k$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, \&_k, \frown_k, = \rangle$.*

*Proof.* We are going to prove the correctness of the following definition:

$$\Delta_k(u,t,x) \Leftrightarrow \exists z_1 \exists z_2 \exists x_1 \exists x_2 \exists x_3 \Big(P_k(u) \wedge k^3 \le u \wedge$$

$$z_1 = Copy_k(u,t,1) \wedge \lambda_k(z_1) = \lambda_k(x) \wedge x\&_k(ku-1) = 1 \wedge x \preccurlyeq_k \mathbf{1}_k(z_1) \wedge \tag{7}$$

$$x_1 = \frac{(kx)}{u} \wedge x_2 = \frac{x}{u} \wedge x_3 = \frac{x}{ku} \wedge x = \lambda_k(x) + x\&_k x_1 + x\&_k x_2 + x\&_k x_3 \wedge \tag{8}$$

$$x_1\&_k x_2 = 0 \wedge x_2\&_k x_3 = 0 \wedge x_2\&_k x_3 = 0 \wedge \tag{9}$$

$$z_2 = Copy_k(u,t,u) \wedge x\&_k(z_2 + \frac{z_2}{k}) = 0\Big). \tag{10}$$

Conjunction (7) expresses that $x$ is a sequence of the same number of $u$-bytes as $t$ that starts and ends with the $u$-byte 000...01, and in every $u$-byte there can only be zeros and ones. Condition (10) specifies that the two most significant bits in every $u$-byte of $x$ are equal to zero. Next, the variables $x_1, x_2, x_3$ correspond to the right shifts of $x$ one $u$-byte plus $D \in \{-1, 0, +1\}$. Let us prove that in every $u$-byte there is a unique 1 and that it has the same position plus $D \in \{-1, 0, +1\}$ compared to the previous $u$-byte.

From (8), we see that in every $u$-byte of $x$ there is at least one 1. Indeed, if $x \ne u$ then the first $u$-byte of $x_1$, or $x_2$, or $x_3$ must contain 1 (the least significant bit); thus, the second $u$-byte of $x$ is also non-zero, etc. This 1 in every $u$-byte is in the desired position since the values $x\&_k x_1$, $x\&_k x_2$, $x\&_k x_3$ describe the three cases in which the position in the next $u$-byte is the same plus $-1$, 0, $+1$, respectively.

Now we prove that there are no other non-zero bits in every $u$-byte of $x$. Assume for a contradiction that there is a $u$-byte in $x$ with more than one 1. Then, there are two consecutive $u$-bytes (which are depicted on the next page) such that the left $u$-byte has the only 1, and the right one has at least two 1. This pair exists because the most significant $u$-byte of $x$ equals 1. From the representation of $x$ in (8), we see that the bits $a$, $b$, $f$, $g$ are all equal to zero.

Next, since by (9) $x_1$, $x_2$ and $x_3$ are pairwise disjoint, among $c$, $d$ and $e$ there is only one 1. This contradicts our assumption.

$$\begin{aligned}
x &= \ldots\underbrace{0..000..\boxed{010}..000..00}_{l_k(u)}\underbrace{..*\,a*..*\,b\boxed{cde}f*..*\,g*..*}_{l_k(u)}\ldots\\
x_1 &= \ldots\underbrace{0..\,0\,0\,0..\;\;0\boxed{100}0\;\;..\,0\,0\,0\,..00}_{l_k(u)}\underbrace{..0c\boxed{de0}00..0}_{l_k(u)}\ldots\\
x_2 &= \ldots\underbrace{0..\,0\,0\,0..\;\;0\boxed{010}0\;\;..\,0\,0\,0\,..00}_{l_k(u)}\underbrace{..00\boxed{cde}00..0}_{l_k(u)}\ldots\\
x_3 &= \ldots\underbrace{0..\,0\,0\,0..\;\;0\boxed{001}0\;\;..\,0\,0\,0\,..00}_{l_k(u)}\underbrace{..00\boxed{0cd}e0..0}_{l_k(u)}\ldots
\end{aligned}$$

It remains to prove that for every $u$ and $x$ such that $\Delta_k(u,t,x)$ there exist non-negative integers from the definition above. This is obvious for $z_1$ and $z_2$; the existence of $x_1$, $x_2$, $x_3$ follows from the fact that there are at least two zeros between every pair of 1 in $x$. □

In our proof we check whether or not the $u$-bytewise minimum of two natural numbers equals zero. In order to express this property, let us introduce a function $U_k$ which modifies $x$ as follows. If $x$ can be split into consecutive $u$-bytes where the most significant bit is equal to zero, then $U_k(u,x)$ replaces every non-zero $u$-byte by 1. Otherwise, this function maps to zero. For example, when $x = 10\,000\,011\,000\,010$ we have $U_2(100,x) = 1\,000\,001\,000\,001$ and $U_2(1000,x) = 0$.

**Lemma 7.** *The function $U_k$ is $\exists$-definable in $\langle\mathbb{N};0,1,+,\&_k,\frown_k,=\rangle$.*

*Proof.* Let us first define a predicate $\overline{U_k}$, which (in comparison with the function $U_k$) is also true for the cases when $y$ has $u$-bytes equal 1 while the corresponding $u$-bytes of $x$ are equal to zero. In $\overline{U_k}$ there are also no restrictions on the most significant bits of $u$-bytes. We have the definition

$$\begin{aligned}\overline{U_k}(u,x,y) \Leftrightarrow \exists t\exists t'\exists v\Big(\mathit{Cpy}_k(\lambda_k(u),t) \wedge t' \preccurlyeq_k t \wedge v = kt' - \frac{(kt')}{u} \wedge x \preccurlyeq_k v \wedge\\ y = v \&_k \mathit{Copy}_k(u,x,1)\Big).\end{aligned}$$

The $k$-ary representation of $v$ is a sequence of $u$-bytes which are either zero or equal to $ku-1$; moreover, for every unit in $x$ there is $(k-1)$ in $v$. Then we select the desired 1 in $y$ via a bitwise multiplication of $v$ by a sequence of $u$-bytes of the same $u$-byte-length as $x$, where all bytes are equal to 1.

In order to exclude extra non-zero $u$-bytes from $y$, we consider the difference $kx-y$. Recall that the definition of $U_k$ requires zeroness of the most significant bit in every $u$-byte. Thus, we have

$$\begin{aligned}y = U_k(u,x) \Leftrightarrow x\&_k \mathit{Copy}_k(u,x,u) > 0 \wedge y = 0 \vee\\ x\&_k \mathit{Copy}_k(u,x,u) = 0 \wedge \overline{U_k}(u,x,y) \wedge (k-1)y \preccurlyeq_k (kx-y).\end{aligned} \tag{11}$$

Consider the case when the most significant bits in $u$-bytes of $x$ are all zero. The least significant bit in every $u$-byte of $kx$ now equals 0, and the fact that there is a unique $y$ that satisfies the definition can be illustrated as follows:

$$...\underbrace{*...*1 \qquad 0... \qquad 0 \qquad 0}_{l_k(u)}...\underbrace{*...* \qquad 0}_{l_k(u)} \quad \overline{0} \quad \underbrace{0... \qquad 0 \qquad 0}_{l_k(u)}...$$

$$...\underbrace{0...00 \qquad 0... \qquad 0 \qquad 1}_{l_k(u)}...\underbrace{0...0 \qquad 1}_{l_k(u)} \quad \overline{0} \quad \underbrace{0... \qquad 0 \qquad 1}_{l_k(u)}...$$

$$...\underbrace{*...*0(k-1)...(k-1)(k-1)}_{l_k(u)}...\underbrace{*...*(k-2)}_{l_k(u)}\,\overline{(k-1)}\,\underbrace{(k-1)...(k-1)(k-1)}_{l_k(u)}...$$

These three lines represent the numbers $kx$, $y$, and $(kx-y)$, respectively. The left column demonstrates the general "correct" case. The middle and the right columns show why the existence of an extra non-zero $u$-byte in $y$ contradicts definition (11). □

We are now able to prove the main result of this section.

**Theorem 3.** *For every integer $k \geq 2$ a relation is $k$-MCM-recognizable if and only if it is $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, \frown_k, = \rangle$. Therefore, every relation $R \subseteq \mathbb{N}^n$ is r.e. iff it is $\exists$-definable in this structure.*

*Proof.* For a given $k$-MCM $\mathcal{M} = (m, Q, q_0, F, \delta)$ and an input vector $\overline{x} \in \mathbb{N}^n$ in $k$-ary notation, we are going to encode the existence of an accepting sequence of transitions between configurations of $\mathcal{M}$. First choose a variable $u$ such that $P_k(u) \wedge \bigwedge_{i \in [1..n]} k^4 x_i \leq u$; this choice specifies the size of bytes in our encoding. We multiply by $k^4$ since in $u$-byte there must be two bits for delimiters $\vdash, \dashv$ and at least two auxiliary zeros from the definition of $\varDelta_k$.

A sequence of states is encoded similarly to formula (4), that is,

$$K_k(u,t,\overline{q}) \rightleftharpoons \bigwedge_{0 \leq i < j \leq s} q_i \&_k q_j = 0 \wedge q_0 + ... + q_s = Copy_k(u,t,1) \wedge$$

$$1 \preccurlyeq_k q_0 \wedge \bigvee_{p \in F} \varLambda_k(u,t) \preccurlyeq_k q_{\nu(p)},$$

where $\overline{q} = q_0, ..., q_s$ and $t$ corresponds to the number of steps of an accepting computation of $\mathcal{M}$. Here we also require $q_0$ to be the initial state and the most significant $u$-byte of $t$ corresponds to a final configuration.

We now define a predicate $C_{\mathcal{M}}$ that encodes a sequence of configurations of $\mathcal{M}$. Similar to Matiyasevich [19], in this definition for every $x_i \in \overline{x}$ a sequence of copies of $x_i$ is decomposed into disjoint variables $\theta_{i,0}$,...,$\theta_{i,k-1}$ such that every $u$-byte of $\theta_{i,a}$ equals $\varTheta_{k,a}(x_i)$. Let $\overline{\theta}$ denote the list of variables $\theta_{1,0}, ..., \theta_{1,k-1}, \theta_{2,0}, ..., \theta_{n,k-1}, \theta_{\vdash}, \theta_{\dashv}$, where the extra variables $\theta_{\vdash}$, $\theta_{\dashv}$ encode the positions of the delimiters. The variable $h$ stores the positions of the input head of $\mathcal{M}$, and the list of variables $\overline{y} = y_1, ..., y_m$ corresponds to the values of the counters at each step of computation.

It is convenient to introduce a function $b_k$, which gives the smallest power of $k$ greater than every $x_i \in \overline{x}$. The graph of this function can be defined as

$$y = b_k(\overline{x}) \Leftrightarrow \bigvee_{i\in[1..n]} y = k\lambda_k(x_i) \wedge \bigwedge_{i\in[1..n]} y \geq k\lambda_k(x_i).$$

This function will be applied to encode the positions of the right delimiter $\dashv$. The following formula describes a sequence of configurations of $\mathcal{M}$.

$$\begin{aligned}
C_{\mathcal{M}}(u,t,\overline{q},\overline{x},\overline{\theta},h,\overline{y}) \rightleftharpoons P_k(u) \wedge \bigwedge_{i\in[1..n]} k^4 x_i \leq u \wedge u \leq t \wedge K_k(u,t,\overline{q})\wedge \\
\theta_{\vdash} = \mathit{Copy}_k(u,t,1) \wedge \bigwedge_{i\in[1..n]} \Big( \theta_{i,0} = \mathit{Copy}_k(u,t,k\varTheta_{k,0}(x_i + b_k(\overline{x}))\wedge \\
\bigwedge_{a\in[1..k-1]} \theta_{i,a} = \mathit{Copy}_k(u,t,k\varTheta_{k,a}(x_i))\Big) \wedge \theta_{\dashv} = \mathit{Copy}_k(u,t,kb_k(\overline{x}))\wedge \\
\varDelta_k(u,t,h) \wedge \bigwedge_{i\in[1..m]} \varDelta_k(u,t,y_i).
\end{aligned}$$

It is easy to see that $\theta_{\vdash}$, $\theta_{\dashv}$ are disjoint with the other variables from $\overline{\theta}$. For notational convenience, we subsequently assume that $\theta_{i,\vdash} \rightleftharpoons \theta_{\vdash}$ and $\theta_{i,\dashv} \rightleftharpoons \theta_{\dashv}$ for every $i \in [1..n]$, and the letters for the delimiters be the vectors $(\vdash, ..., \vdash)$ and $(\dashv, ..., \dashv)$ of length $n$.

We now proceed to the encoding of the fact that a given sequence of configurations is actually a sequence of transitions in $\mathcal{M}$. For a letter $(a_1, ..., a_n) \in \varSigma_k^n \cup \{\vdash, \dashv\}$, a state $p \in Q$, and a tuple $\overline{c} \in \{0,1\}^m$ such that the values of the counters from $Y_{\overline{c}} = \{i \in [1..m] \mid c_i = 0\}$ are equal to zero and from $[1..m] \setminus Y_{\overline{c}}$ are non-zero, the following formula is an analogue to definition (5):

$$\begin{aligned}
\varDelta_{(p,\overline{a},\overline{c})}(u,t,\overline{q},\overline{\theta},h,\overline{y}) \rightleftharpoons \Big( q_{\nu(p)} \&_k \underset{i\in[1..n]}{\&_k} U_k(u,(\theta_{i,a_i} \&_k h)) \&_k \\
\underset{i\in Y_{\overline{c}}}{\&_k} y_i \&_k \underset{i\in[1..m]\setminus Y_{\overline{c}}}{\&_k} U_k(u, y_i - \mathit{Copy}_k(u,t,1) \&_k y_i)\Big) \preccurlyeq_k \\
\underset{(\widetilde{p},d,\overline{d})\in\delta(p,\overline{a},\overline{c})}{\Big|_k} \Big( \frac{q_{\nu(\widetilde{p})}}{u} \&_k U_k(u, h \&_k \frac{(k^d h)}{u}) \&_k \underset{i\in[1..m]}{\&_k} U_k(u, y_i \&_k \frac{(k^{d_i} y_i)}{u})\Big).
\end{aligned}$$

The key difference with (5) is that now in order to compare two consecutive configurations we shift by one $u$-byte instead of one bit. It is obvious that the predicate $\varDelta_{(p,\overline{a},\overline{c})}$ makes sense when it is complemented with $C_{\mathcal{M}}$. In this case, for example, $U_k(u, h \&_k \frac{(k^d h)}{u})$ highlights the configurations for which in the following configuration the position of the input head shifts by $d$. Indeed, we obtain a sequence of $u$-bytes, each of which is equal to one if and only if the position of the unique 1 in the next $u$-byte is the same plus $d$, otherwise this $u$-byte is equal to zero.

It remains to define the relation $R_{L(\mathcal{M})}$ that corresponds to the language recognizable by $\mathcal{M}$. To this end, we have to consider every tuple $(p, \overline{a}, \overline{c})$ in $Q \times (\Sigma_k^n \cup \{\vdash, \dashv\}) \times \{0,1\}^m$ and apply already defined predicates $C_{\mathcal{M}}$ and $\Delta_{(p,\overline{a},\overline{c})}$.

$$R_{L(\mathcal{M})}(\overline{x}) \Leftrightarrow \exists u \exists t \exists \overline{q} \exists \overline{\theta} \exists h \exists \overline{y} \Big( C_{\mathcal{M}}(u, t, \overline{q}, \overline{x}, \overline{\theta}, h, \overline{y}) \wedge \bigwedge_{(p,\overline{a},\overline{c}) \in Q \times (\Sigma_k^n \cup \{\vdash, \dashv\}) \times \{0,1\}^m} \Delta_{(p,\overline{a},\overline{c})}(u, t, \overline{q}, \overline{\theta}, h, \overline{y}) \Big).$$

This completes the proof. □

Since by [14,19] the bitwise minimum operation $\&_2$ is existentially definable in $\langle \mathbb{N}; 0, 1, +, \cdot, exp, = \rangle$, we obtain DPR-theorem as a corollary.

**Corollary 4 (DPR-theorem).** *Every relation $R \subseteq \mathbb{N}^n$ is r.e. if and only if it is $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, \cdot, exp, = \rangle$.*

Let us fix $k = 2$ and omit mentioning $k$ in $\frown_k$ and $EqNZB_k$. Since we have $z = x \&_2 y \Leftrightarrow z \preccurlyeq y \wedge y \preccurlyeq x + y - z$ (see [14]), bitwise minimum is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, \preccurlyeq, \frown, = \rangle$. Next, exponential diophantiness of $\preccurlyeq$ follows from the fact that $x \preccurlyeq y$ iff $\binom{y}{x} \equiv 1 (\mathrm{mod}\ 2)$, where $\binom{y}{x}$ is a binomial coefficient. Factorial representation of binomial coefficients and Legendre's formula imply that

$$x \preccurlyeq y \Leftrightarrow s_2(y) = s_2(x) + s_2(y - x),$$

where $s_2(x)$ is the number of 1's in base 2 expansion of $x$. Therefore, the masking relation is definable by the formula $x \preccurlyeq y \Leftrightarrow EqNZB(y, x \frown (y - x))$ and we have the following result.

**Corollary 5.** *Every relation $R \subseteq \mathbb{N}^n$ is r.e. if and only if it is $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, EqNZB, \frown, = \rangle$.*

## 5 Conclusion

The purpose of this paper is to emphasize similarities in existential first-order characterizations of the languages recognizable by various abstract machines. Such descriptions in Sections 3 and 4 allowed us (in some sense) to answer the question of Bès [2, Open Problems] concerning the expressive power of fragments of FO-arithmetic with the predicate $EqNZB$.

Let us mention one natural question which is related to Theorems 1 and 3. Villemaire proves [23,24] that multiplication is definable in $\langle \mathbb{N}; 0, 1, +, V_k, V_l, = \rangle$ when $k$ and $l$ are multiplicatively independent. Bès strengthens this result [1] by showing that the same is true when $V_l$ is replaced by any $l$-recognizable relation $R_l$ that is not definable in $\langle \mathbb{N}; 0, 1, +, = \rangle$. It would be interesting to see whether multiplication is *existentially* definable in $\langle \mathbb{N}; 0, 1, +, \&_k, \&_l, = \rangle$, and more generally, to study $\exists$-definability in the structures $\langle \mathbb{N}; 0, 1, +, \&_k, R_l, = \rangle$.

**Acknowledgements.** The author is grateful to the anonymous reviewers for their useful suggestions and comments.

## References

1. Bès, A.: Undecidable extensions of Büchi arithmetic and Cobham-Semënov theorem. Journal of Symbolic Logic **62**(4), 1280–1296 (1997). https://doi.org/10.2307/2275643
2. Bès, A.: Expansions of MSO by cardinality relations. Logical Methods in Computer Science **9**(4) (2013). https://doi.org/10.2168/lmcs-9(4:18)2013
3. Bruyère V.: Entiers et automates finis. Mémoire de fin d'études, University of Mons, Belgium (1985)
4. Bruyère V., Hansel G., Michaux C., Villemaire R.: Logic and $p$-recognizable sets of integers. Bulletin of the Belgian Mathematical Society - Simon Stevin **1**(2), 191–238 (1994). https://doi.org/10.36045/bbms/1103408547
5. Büchi R.J.: Weak second-order arithmetic and finite automata. Mathematical Logic Quarterly **6**(1-6), 66–92 (1960). https://doi.org/10.1002/malq.19600060105
6. Cadilhac M., Finkel A., McKenzie P.: On the expressiveness of Parikh automata and related models. In: Proceedings of the Third Workshop on Non-Classical Models for Automata and Applications - NCMA 2011, pp. 103-119. Milan, Italy (2011)
7. Davis M.: Arithmetical problems and recursively enumerable predicates. Journal of Symbolic Logic **18**(1), 33–41 (1953). https://doi.org/10.2307/2266325
8. Davis M., Putnam H., Robinson J.: The decision problem for exponential diophantine equations. Annals of Mathematics **74**(3), 425–436 (1961). https://doi.org/10.2307/1970289
9. Elgot C.C.: Decision problems of finite automata design and related arithmetics. Transactions of the American Mathematical Society **98**(1), 21–51 (1961). https://doi.org/10.1090/s0002-9947-1961-0139530-9
10. Ginsburg S., Spanier E.: Semigroups, Presburger formulas, and languages. Pacific Journal of Mathematics **16**(2), 285–296 (1966). https://doi.org/10.2140/pjm.1966.16.285
11. Haase C., Różycki J.: On the expressiveness of Büchi arithmetic. In: Kiefer, S., Tasson, C. (eds) FOSSACS 2021, Lecture Notes in Computer Science, vol. 12650, pp. 310–323. Springer International Publishing (2021). https://doi.org/10.1007/978-3-030-71995-1_16
12. Hodgson B.R.: Décidabilité par automate fini. Annales des sciences mathématiques du Québec, **7**(1), 39–57 (1983).
13. Ibarra O.H.: Reversal-bounded multicounter machines and their decision problems. Journal of the ACM **25**(1), 116–133 (1978). https://doi.org/10.1145/322047.322058
14. Jones J.P., Matijasevič Yu.V.: Register machine proof of the theorem on exponential diophantine representation of enumerable sets. Journal of Symbolic Logic **49**(3), 818–829 (1984). https://doi.org/10.2307/2274135
15. Klaedtke F., Rueß H.: Parikh automata and monadic second-order logics with linear cardinality constraints. Tech. rep. 177, Universität Freiburg (2002)
16. Klaedtke F., Rueß H.: Monadic second-order logics with cardinalities. In: Baeten, J.C.M., Lenstra, J.K., Parrow, J., Woeginger, G.J. (eds) ICALP 2003, Lecture Notes in Computer Science, vol. 2719, pp. 681–696. Springer, Heidelberg (2003). https://doi.org/10.1007/3-540-45061-0_54
17. Kozen D.C.: Automata and Computability. Springer, New York (1997). https://doi.org/10.1007/978-1-4612-1844-9
18. Kummer E.E.: Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen. Journal für die reine und angewandte Mathematik, **44**, 93–146 (1852). https://doi.org/10.1515/crll.1852.44.93

19. Matiyasevich Yu.V.: A new proof of the theorem on exponential diophantine representation of enumerable sets (in Russian). Zapiski Nauchnykh Seminarov LOMI **60**, 75–92 (1976). (English translation: Journal of Soviet Mathematics **14**(5), 1475–1486 (1980) https://doi.org/doi:10.1007/BF01693980)
20. Matiyasevich Yu.V.: Hilbert's tenth problem. MIT Press, Massachusetts (1993)
21. Parikh R.J.: On context-free languages. Journal of the ACM **13**(4) 570–581 (1966). https://doi.org/10.1145/321356.321364
22. Trakhtenbrot B.A.: Finite automata and the logic of one-place predicates (in Russian). Sibirskiĭ Matematicheskiĭ Zhurnal **3**, 103–131 (1962).
23. Villemaire R.: Joining $k$- and $l$-recognizable sets of natural numbers. In: Finkel, A., Jantzen, M. (eds) STACS 1992, Lecture Notes in Computer Science, vol. 577, pp. 83–94. Springer, Heidelberg (1992). https://doi.org/10.1007/3-540-55210-3_175
24. Villemaire R.: The theory of $\langle \mathbb{N}; +, V_k, V_l \rangle$ is undecidable. Theoretical Computer Science **106**(2), 337–349 (1992). https://doi.org/10.1016/0304-3975(92)90256-f