Existential Definability with Addition and k-Regular Predicates

Mikhail R. Starchak

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

Keywords: Existential definability · Automatic structures · Büchi arithmetic · Quantifier elimination · Decidability

1 Existential Definability with Addition and Bitwise Minimum

For every $R \subseteq \mathbb{N}^n$, integer base $k \geq 2$, and $\Sigma_k = \{0, 1, ..., k-1\}$, the k-ary representations of vectors from R define a language $L_R \subseteq (\Sigma_k^n)^*$ in a natural way. A relation R is called k-regular if there is a finite automaton $\mathcal{A}$ over Σ_k^n that recognizes the language L_R. The Büchi-Bruyère's theorem [1] provides an FO-characterization of k-regular sets: they coincide with the sets definable in the structure $\langle \mathbb{N}; 0, 1, +, V_k, \leq \rangle$, where $V_k(x, y)$ is true whenever y is the largest power of k dividing x. As it was shown by Haase and Różycki [2], the $\exists\forall$-formulas of the corresponding language are expressive enough to define every k-regular set, but the $\exists$-formulas are less powerful. They give necessary conditions of $\exists$-definability in terms of densities of regular languages and, in particular, show that the set of all natural numbers with binary representations from the language $\{10, 01\}^*$ is not $\exists$-definable. The following two questions immediately arise in connection with these results: whether there is a "natural" k-regular relation R such that every k-regular predicate is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, R, \leq \rangle$, and how can we completely describe the expressive power of the existential k-Büchi arithmetic.

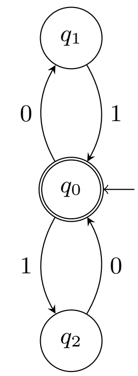
The first problem can be solved by using the techniques of Matiyasevich [4], which were applied for arithmetization of Turing machines. Let $\&_k$ be the binary *bitwise minimum operation of base* k, where we assume that the natural number of smaller bit-length is supplemented with a sufficient number of leading zeros. Then we have the following existential FO-characterisation of k-regular relations.

Theorem 1 ([7]). *For an integer $k \geq 2$ every relation is k-regular if and only if it is existentially definable in the structure $\langle \mathbb{N}; 0, 1, +, \&_k, \leq \rangle$.*

For every word $w = a_m ... a_0 \in \Sigma_k^*$, denote by $[\![w]\!]_k$ the integer $a_m k^m + ... + a_1 k + a_0$, and for a language $L \subseteq \Sigma_k^*$ define $[\![L]\!]_k \rightleftharpoons \{[\![w]\!]_k : w \in L\}$. We can now construct an existential definition of $[\![\{10, 01\}^*]\!]_2$ in $\langle \mathbb{N}; 0, 1, +, \&_2, \leq \rangle$. In our formula, the subscript 2 is omitted, the property "to be a power of 2" is denoted by P_2, and the binary function $\sim$ is an analogue of bitwise negation, where the first argument specifies the bit-length of the result. We also use the binary predicate symbol $\preccurlyeq$ for the *masking* relation such that $x \preccurlyeq y \rightleftharpoons x \& y = x$. The values of t, q_0, q_1, q_2 for the case when $x = 1100101_2$ are given in Figure (a).

···	0	0	0	1	1	0	0	1	0	1	x
···	0	1									t
···	0	1		1		1		1		1	q_0
···	0				1						q_1
···	0		1				1		1		q_2

(a)



(b)

$$\exists t \exists q_0 \exists q_1 \exists q_2 \Big(P_2(t) \wedge x < t \wedge q_0 + q_1 + q_2 = 2t - 1 \wedge$$
$$q_0 \& q_1 = 0 \wedge q_0 \& q_2 = 0 \wedge q_1 \& q_2 = 0 \wedge$$
$$q_0 \& 1 = 1 \wedge q_0 \& t = t \wedge q_0 \& x \preccurlyeq \frac{q_2}{2} \wedge q_0 \& \sim (\frac{t}{2}, x) \preccurlyeq \frac{q_1}{2} \wedge$$
$$q_1 \& x \preccurlyeq \frac{q_0}{2} \wedge q_1 \& \sim (\frac{t}{2}, x) \preccurlyeq 0 \wedge q_2 \& x \preccurlyeq 0 \wedge q_2 \& \sim (\frac{t}{2}, x) \preccurlyeq \frac{q_0}{2} \Big).$$

This formula describes the fact that the Σ_2-NFA from Figure (b) accepts the binary representation of x with some auxiliary leading zeros while reading it from left to right. It is now easy to obtain a $\exists$-definition of $[\![\{10, 01\}^*]\!]_2$ in $\langle \mathbb{N}; 0, 1, +, \&_2, \leq \rangle$. We can even prove somewhat converse: every 2-regular set is $\exists$-definable in the structure $\langle \mathbb{N}; 0, 1, +, [\![\{10, 01\}^*]\!]_2, \leq \rangle$.

2 Existential Definability in Büchi Arithmetic

A characterisation of sets $S \subseteq \mathbb{N}$ that are existentially definable in k-Büchi arithmetic $\langle \mathbb{N}; 0, 1, +, V_k, \leq \rangle$ relies on the quantifier-elimination techniques developed by Semënov [5]. Having an existential formula, the bound variables are split into *ordinary* and *special* variables for the powers of k. The desired characterisation is based on the ordinary variable elimination procedure [6] and the following fundamental result by Semënov [5, Theorem 5]: every set $S \subseteq \mathbb{N}$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, P_k, \leq \rangle$ if and only if S can be represented as a finite union of sets that are definable via expressions of the form $v_0 w_1^* v_1 w_2^* v_2 ... w_n^* v_n \Sigma_{l,m,c}$, where for every fixed $l, m, c \in \mathbb{N}$, the pattern $\Sigma_{l,m,c}$ specifies the set of all k-ary representations of non-negative integers congruent to c modulo m with bit-length divisible by l. Here we assume that $\Sigma_{0,0,0} = \{\epsilon\}$.

In order to formulate the theorem clearly, define for positive integers l and m a set of k-regular languages $\mathscr{C}_{l,m}$ as follows. This class contains the languages $\{w\}$ and w^* for every word $w \in \Sigma_k$ of length at most l, and the languages $\Sigma_{l',m',c'}$ for every non-negative integers $l' \leq l$, $m' \leq m$, $c' \in [0..m' - 1]$.

Theorem 2 ([6]). *A k-regular set $R \subseteq \mathbb{N}$ is $\exists$-definable in $\langle \mathbb{N}; 0, 1, +, V_k, \leq \rangle$ if and only if there exist positive integers l and m such that R can be obtained by a finite number of applications of concatenation and union to $\mathscr{C}_{l,m}$.*

This theorem allows us to make progress in solving the open problem by Haase and Różycki [2, Conclusion] concerning decidability of the $\exists$-definability property for the structure $\langle \mathbb{N}; 0, 1, +, V_k, \leq \rangle$. To apply the $\{\cdot, \cup\}$-representation theorem by Hashiguchi [3, Theorem 6.1] and thus to answer this question in the affirmative, we need to construct an upper bound on the integers l and m depending on the number of states of a given Σ_k-DFA.

The language $L \coloneqq \{10, 01\}^*$ provides another interesting example. Let $L^{\complement}$ denote the complement of the language L. It is easy to see that $[\![L^{\complement}]\!]_2$ is definable by the expression

$$x \in (\Sigma_{0,0,0} \cup \Sigma_{1,1,0})11\big(\Sigma_{2,1,0} \cup 0\Sigma_{2,1,0}(1 \cup 0)\big) \cup \Sigma_{1,1,0}00\big(\Sigma_{2,1,0} \cup 0\Sigma_{2,1,0}(1 \cup 0)\big).$$

Since every set definable in $\langle \mathbb{N}; 0, 1, +, P_2, \leq \rangle$ is existentially definable in this structure, the set $[\![L^{\complement}]\!]_2$ cannot be defined here. These examples lead to the following more general problem about the nature of *existential* definability in Presburger arithmetic with some classes of k-regular predicates $\mathscr{R}$: how can we describe a hierarchy of classes of predicates between semi-linear and k-regular with respect to the $\exists$-definability in $\langle \mathbb{N}; 0, 1, +, \mathscr{R}, \leq \rangle$?

The techniques that are used in the proofs of Theorems 1 and 2 can be applied to obtain definability and decidability results [6,7] outside of the k-regular world. In my talk, there will be considered the structure $\langle \mathbb{N}; 0, 1, +, \&_k, EqNZB_k, \leq \rangle$, where $EqNZB_k(x, y)$ is true if and only if x and y have the same number of non-zero bits in k-ary encoding, and the structure $\langle \mathbb{N}; 0, 1, +, V_k, \lambda x.k^x, \leq \rangle$. In both cases, the existential theories are decidable whereas the $\exists\forall$-theories are undecidable.

Acknowledgements. This work presents the results of a research supported by the Russian Science Foundation, project 23-71-01041.

References

1. 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 (jan 1994). https://doi.org/10.36045/bbms/1103408547
2. Haase, C., Różycki, J.: On the expressiveness of Büchi arithmetic. In: Foundations of Software Science and Computation Structures (FoSSaCS) 2021. LNCS, vol. 12650, pp. 310–323. Springer International Publishing (2021). https://doi.org/10.1007/978-3-030-71995-1_16
3. Hashiguchi, K.: Representation theorems on regular languages. Journal of Computer and System Sciences **27**(1), 101–115 (aug 1983). https://doi.org/10.1016/0022-0000(83)90031-4
4. 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). https://doi.org/10.1007/BF01693980, english translation: Journal of Soviet Mathematics 14, 5 (1980), 1475–1486

5. Semënov, A.L.: On certain extensions of the arithmetic of addition of natural numbers. Mathematics of the USSR-Izvestiya **15**(2), 401–418 (1980). https://doi.org/10.1070/im1980v015n02abeh001252
6. Starchak, M.R.: Existential Büchi arithmetic and its decidable extensions, preprint
7. Starchak, M.R.: On the existential arithmetics with addition and bitwise minimum. In: Lecture Notes in Computer Science, pp. 176–195. Springer Nature Switzerland (2023). https://doi.org/10.1007/978-3-031-30829-1_9