On the Expressiveness of Büchi Arithmetic

Jakub Różycki [1] Christoph Haase [2]

[1]University of Warsaw, Poland; [2]University of Oxford, UK

April 13, 2021

Table of contents

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.
Büchi arithmetic is the structure $(\mathbb{N}, +, V_p(\cdot, \cdot))$.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.
Büchi arithmetic is the structure $(\mathbb{N}, +, V_p(\cdot, \cdot))$.

Theorem (Büchi, 1960)

Let L be a language over an alphabet $\Sigma = \{0, 1 \ldots p - 1\}$.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.
Büchi arithmetic is the structure $(\mathbb{N}, +, V_p(\cdot, \cdot))$.

Theorem (Büchi, 1960)

Let L be a language over an alphabet $\Sigma = \{0, 1 \ldots p - 1\}$. Further assume that any element of L represents an integer.

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.
Büchi arithmetic is the structure $(\mathbb{N}, +, V_p(\cdot, \cdot))$.

Theorem (Büchi, 1960)

Let L be a language over an alphabet $\Sigma = \{0, 1 \ldots p-1\}$. Further assume that any element of L represents an integer.
Then L is regular if and only if it is represented by a formula ϕ of Büchi arithmetic,

What is Büchi arithmetic?

Presburger arithmetic: $(\mathbb{N}, +)$.
Fix a base $p > 1$.
Define a relation V_p, such that
$V_p(x, y) \iff \exists k : x = p^k$ and $p^k | y$ and $p^{k+1} \nmid y$.
Büchi arithmetic is the structure $(\mathbb{N}, +, V_p(\cdot, \cdot))$.

Theorem (Büchi, 1960)

Let L be a language over an alphabet $\Sigma = \{0, 1 \ldots p-1\}$. Further assume that any element of L represents an integer.
Then L is regular if and only if it is represented by a formula ϕ of Büchi arithmetic, i.e. $x \in L \iff \phi(x)$.

Our motivation

How many quantifiers do we need to express every formula of Büchi arithmetic?

Our motivation

How many quantifiers do we need to express every formula of Büchi arithmetic?

Theorem (Ginsburg, Spanier, 1964 (1))

The $\exists^*$ fragment of Presburger arithmetic is expressively complete.

Our motivation

How many quantifiers do we need to express every formula of Büchi arithmetic?

Theorem (Ginsburg, Spanier, 1964 (1))

The $\exists^*$ fragment of Presburger arithmetic is expressively complete.

Definition

The $\exists^*$ fragment (or $\forall^*, \exists^*\forall^*$...) of logical theory is *expressively complete* if and only if for every first-order logic formula ϕ of the logic there exists a formula ψ with quantifier prefix $\exists^*$ (or $\forall^*, \exists^*\forall^*$...) such that $\phi(\boldsymbol{x}) \iff \psi(\boldsymbol{x})$.

Our results

Theorem

The $\exists^*\forall^*$ fragment of Büchi arithmetic is expressively complete.

Our results

Theorem

The $\exists^*\forall^*$ fragment of Büchi arithmetic is expressively complete.

Theorem

The $\exists^*$ fragment of Büchi arithmetic is not expressively complete.

Our results

Theorem

The $\exists^*\forall^*$ fragment of Büchi arithmetic is expressively complete.

Theorem

The $\exists^*$ fragment of Büchi arithmetic is not expressively complete.

Theorem

If L is a regular language of polynomial growth, then there exists an $\exists^*$ formula of Büchi arithmetic ϕ such that $\phi(x) \iff x \in L$.

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Theorem

Let $L \subset \mathbb{N}$ be defined by a formula of existential Büchi arithmetic. Then one of the following is satisfied:

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Theorem

Let $L \subset \mathbb{N}$ be defined by a formula of existential Büchi arithmetic. Then one of the following is satisfied:

(1) There exists a constant $c \in (0,1)$ such that for all $k \in \mathbb{N}$ $d_L(k) \geq c \cdot p^k$.

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Theorem

Let $L \subset \mathbb{N}$ be defined by a formula of existential Büchi arithmetic. Then one of the following is satisfied:

(1) There exists a constant $c \in (0, 1)$ such that for all $k \in \mathbb{N}$ $d_L(k) \geq c \cdot p^k$.

(2) There exists a polynomial q such that $d_L(k) \leq q(k)$.

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Theorem

Let $L \subset \mathbb{N}$ be defined by a formula of existential Büchi arithmetic. Then one of the following is satisfied:

(1) There exists a constant $c \in (0, 1)$ such that for all $k \in \mathbb{N}$ $d_L(k) \geq c \cdot p^k$.

(2) There exists a polynomial q such that $d_L(k) \leq q(k)$.

Corollary

Existential Büchi arithmetic is not fully expressive in Büchi arithmetic.

Density function

Let $L \subset \mathbb{N}$. We introduce a function $d_L(k) := \#\{L \cap [p^{k-1}, p^k)\}$.

Theorem

Let $L \subset \mathbb{N}$ be defined by a formula of existential Büchi arithmetic. Then one of the following is satisfied:

(1) There exists a constant $c \in (0, 1)$ such that for all $k \in \mathbb{N}$ $d_L(k) \geq c \cdot p^k$.

(2) There exists a polynomial q such that $d_L(k) \leq q(k)$.

Corollary

Existential Büchi arithmetic is not fully expressive in Büchi arithmetic.

Proof. For the language $L = (01|10)^*$ we have $d_L(k) \approx 2^{\frac{k}{2}}$. Thus, for any polynomial q and constant c for big enough k we have $q(k) \leq d_L(k) \leq c \cdot p^k$.

Converting formulas into automata

Any formula $\phi(\boldsymbol{x})$ of existential Büchi arithmetic can be presented as a disjunction of linear Diophantine equations with valuation constraints, each of the form:

Converting formulas into automata

Any formula $\phi(\boldsymbol{x})$ of existential Büchi arithmetic can be presented as a disjunction of linear Diophantine equations with valuation constraints, each of the form:

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c} \wedge \bigwedge_{i \in I} V_p(x_i, y_i)$$

Converting formulas into automata

Any formula $\phi(\boldsymbol{x})$ of existential Büchi arithmetic can be presented as a disjunction of linear Diophantine equations with valuation constraints, each of the form:

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c} \wedge \bigwedge_{i \in \boldsymbol{I}} V_p(x_i, y_i)$$

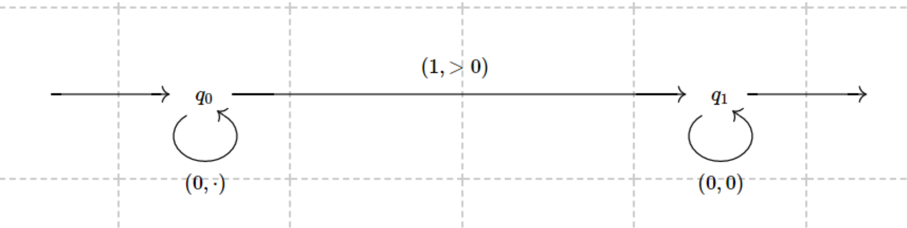
where $x_i, y_i \in \boldsymbol{x}$.
We focus on building an automaton for any Diophantine equation with valuation constraints.

Converting formulas into automata

Any formula $\phi(\boldsymbol{x})$ of existential Büchi arithmetic can be presented as a disjunction of linear Diophantine equations with valuation constraints, each of the form:

$$\boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c} \wedge \bigwedge_{i \in I} V_p(x_i, y_i)$$

where $x_i, y_i \in \boldsymbol{x}$.
We focus on building an automaton for any Diophantine equation with valuation constraints.



Automaton for linear equations

Fix $S : \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c}$. Define $A(S) = (Q, \Sigma_p^d, \delta, \boldsymbol{q}_0, F)$ such that:

Automaton for linear equations

Fix $S : \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c}$. Define $A(S) = (Q, \Sigma_p^d, \delta, \boldsymbol{q}_0, F)$ such that:

- $Q = \mathbb{Z}^d$
- $\boldsymbol{q}_0 = 0$
- $\delta(\boldsymbol{q}, \boldsymbol{u}) = p \cdot \boldsymbol{q} + \boldsymbol{A} \cdot \boldsymbol{u}$
- $F = \{\boldsymbol{c}\}$

Fact

The number of states which can reach the accepting state is finite.

Automaton for linear equations

Fix $S : \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c}$. Define $A(S) = (Q, \Sigma_p^d, \delta, \boldsymbol{q}_0, F)$ such that:

- $Q = \mathbb{Z}^d$
- $\boldsymbol{q}_0 = 0$
- $\delta(\boldsymbol{q}, \boldsymbol{u}) = p \cdot \boldsymbol{q} + \boldsymbol{A} \cdot \boldsymbol{u}$
- $F = \{\boldsymbol{c}\}$

Fact

The number of states which can reach the accepting state is finite. Therefore above automaton restricted to such states is finite.

Automaton for linear equations

Fix $S : \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c}$. Define $A(S) = (Q, \Sigma_p^d, \delta, \boldsymbol{q}_0, F)$ such that:

- $Q = \mathbb{Z}^d$
- $\boldsymbol{q}_0 = 0$
- $\delta(\boldsymbol{q}, \boldsymbol{u}) = p \cdot \boldsymbol{q} + \boldsymbol{A} \cdot \boldsymbol{u}$
- $F = \{\boldsymbol{c}\}$

Fact

The number of states which can reach the accepting state is finite. Therefore above automaton restricted to such states is finite.

Proof. Omitted.

Automaton for linear equations

Fix $S : \boldsymbol{A} \cdot \boldsymbol{x} = \boldsymbol{c}$. Define $A(S) = (Q, \Sigma_p^d, \delta, \boldsymbol{q}_0, F)$ such that:

- $Q = \mathbb{Z}^d$
- $\boldsymbol{q}_0 = 0$
- $\delta(\boldsymbol{q}, \boldsymbol{u}) = p \cdot \boldsymbol{q} + \boldsymbol{A} \cdot \boldsymbol{u}$
- $F = \{\boldsymbol{c}\}$

Fact

The number of states which can reach the accepting state is finite. Therefore above automaton restricted to such states is finite.

Proof. Omitted.

Now we define an automaton for a linear equation with valuation constraints as a product automaton of $A(S)$ and automata for V_p.

Counting loops

Definition

Let A be an automaton, $q \in Q(A)$ - a state and x - a variable. We define a counting function:

$$C_{q,x}(n) = \#\{\pi_x(w) : q \xrightarrow{w} q, w \in (\Sigma_p^d)^n\}$$

Counting loops

Definition

Let A be an automaton, $q \in Q(A)$ - a state and x - a variable. We define a counting function:

$$C_{q,x}(n) = \#\{\pi_x(w) : q \xrightarrow{w} q, w \in (\Sigma_p^d)^n\}$$

Proposition (Woods, (3))

Let $\phi_t(\boldsymbol{x})$ be a formula of Parametric Presburger Arithmetic. Then $\#\{\boldsymbol{x} : \phi_t(\boldsymbol{x})\}$ is an eventual quasi-polynomial.

Counting loops

Definition

Let A be an automaton, $q \in Q(A)$ - a state and x - a variable. We define a counting function:

$$C_{q,x}(n) = \#\{\pi_x(w) : q \xrightarrow{w} q, w \in (\Sigma_p^d)^n\}$$

Proposition (Woods, (3))

Let $\phi_t(\boldsymbol{x})$ be a formula of Parametric Presburger Arithmetic. Then $\#\{\boldsymbol{x} : \phi_t(\boldsymbol{x})\}$ is an eventual quasi-polynomial.

Counting loops

Lemma

Let S be a system of linear Diophantine equations with valuation constraints with the DFA $A = A(S)$. Let $q \in Q(A)$.

Counting loops

Lemma

Let S be a system of linear Diophantine equations with valuation constraints with the DFA $A = A(S)$. Let $q \in Q(A)$. There is an eventual quasi-polynomial f such that $C_{q,x}(n) = f(p^n)$ for all $n \in \mathbb{N}$.

Counting loops

Lemma

Let S be a system of linear Diophantine equations with valuation constraints with the DFA $A = A(S)$. Let $q \in Q(A)$. There is an eventual quasi-polynomial f such that $C_{q,x}(n) = f(p^n)$ for all $n \in \mathbb{N}$. Moreover, for all sufficiently large $n \in \mathbb{N}$, $f(p^n)$ is a linear eventual quasi-polynomial.

Counting loops

Lemma

Let S be a system of linear Diophantine equations with valuation constraints with the DFA $A = A(S)$. Let $q \in Q(A)$. There is an eventual quasi-polynomial f such that $C_{q,x}(n) = f(p^n)$ for all $n \in \mathbb{N}$. Moreover, for all sufficiently large $n \in \mathbb{N}$, $f(p^n)$ is a linear eventual quasi-polynomial.

Proof.

Proof continued

Counting loops

Lemma

Let $S, A = A(S)$ be the same as in previous lemma. Then either:

Counting loops

Lemma

Let $S, A = A(S)$ be the same as in previous lemma. Then either:

(i) There is $q \in Q(A)$ such that $C_{q,x}$ is an eventual quasi-polynomial f and $f(p^n)$ is a non-constant polynomial for infinitely many $n \in \mathbb{N}$;

Counting loops

Lemma

Let $S, A = A(S)$ be the same as in previous lemma. Then either:

(i) There is $q \in Q(A)$ such that $C_{q,x}$ is an eventual quasi-polynomial f and $f(p^n)$ is a non-constant polynomial for infinitely many $n \in \mathbb{N}$;

(ii) There is $d \geq 0$ such that $C_{q,x}(n) \leq d$ for all $q \in Q$ and $n \in \mathbb{N}$.

Counting loops

Lemma

Let $S, A = A(S)$ be the same as in previous lemma. Then either:

(i) There is $q \in Q(A)$ such that $C_{q,x}$ is an eventual quasi-polynomial f and $f(p^n)$ is a non-constant polynomial for infinitely many $n \in \mathbb{N}$;

(ii) There is $d \geq 0$ such that $C_{q,x}(n) \leq d$ for all $q \in Q$ and $n \in \mathbb{N}$.

Proof.

Counting loops

Lemma

Let S be a system of linear equations with valuation constraints with the associated DFA $A(S)$. Then either:

Counting loops

Lemma

Let S be a system of linear equations with valuation constraints with the associated DFA $A(S)$. Then either:

(i) $d_L(n) \geq c \cdot p^n$ for some fixed $c > 0$ and infinitely many $n \in \mathbb{N}$.

Counting loops

Lemma

Let S be a system of linear equations with valuation constraints with the associated DFA $A(S)$. Then either:

(i) $d_L(n) \geq c \cdot p^n$ for some fixed $c > 0$ and infinitely many $n \in \mathbb{N}$.

(ii) $d_L(n) = O(n^c)$ for some $c \geq 0$.

Counting loops

Lemma

Let S be a system of linear equations with valuation constraints with the associated DFA $A(S)$. Then either:

(i) $d_L(n) \geq c \cdot p^n$ for some fixed $c > 0$ and infinitely many $n \in \mathbb{N}$.

(ii) $d_L(n) = O(n^c)$ for some $c \geq 0$.

Proof.

Proof continued

Proof continued

Conclusions

We have proven that:

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.
- $\exists^*$ fragment of Büchi arithmetic is not fully expressive.

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.
- $\exists^*$ fragment of Büchi arithmetic is not fully expressive.

Further questions:

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.
- $\exists^*$ fragment of Büchi arithmetic is not fully expressive.

Further questions:

- Can we classify all languages of existential Büchi arithmetic using the density function?

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.
- $\exists^*$ fragment of Büchi arithmetic is not fully expressive.

Further questions:

- Can we classify all languages of existential Büchi arithmetic using the density function?
- Is it decidable to say whether a language is in existential Büchi arithmetic?

Conclusions

We have proven that:

- $\exists^*\forall^*$ fragment of Büchi arithmetic is fully expressive.
- $\exists^*$ fragment of Büchi arithmetic is not fully expressive.

Further questions:

- Can we classify all languages of existential Büchi arithmetic using the density function?
- Is it decidable to say whether a language is in existential Büchi arithmetic?
- Can we approach the generalized starheight problem using the languages that are in $\exists^*\forall^* \setminus \exists^*$ fragment of Büchi arithmetic?

Acknowledgements

This research was supported by the European Research Council.

erc

European Research Council

Established by the European Commission

References

[1] Ginsburg, S. and Spanier, E.H. *Bounded ALGOL-like languages* Transactions of the American Mathematical Society, 113(2), pp.333-368 (1964).

[2] Roger Villemaire. *The theory of* $(\mathbb{N}, +, V_k, V_l)$ *is undecidable*. Theor. Comput. Sci. 106(2), 337–349 (1992).

[3] K. Woods. *The unreasonable ubiquitousness of quasi-polynomials* Elect. J. Combin. 21(1), P1.44 (2014).

[4] A. Szilard, S. Yu, K. Zhang, J. Shallit. *Characterizing regular languages with polynomial densities*. Mathematical Foundations of Computer Science, MFCS. Lect. Notes Comp. Sci., vol. 629, pp. 494–503. Springer (1992).