On properties of subsets algebras

Sergey Dudakov

Tver State University

2022-11-07

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Origin of the problem

Boris Karlov

Let R be the class of regular languages over some alphabet. Let us consider the theory of $(R, \&, \cup, *)$. Is such theory decidable?

Theory $(R, \cup)$

This theory is decidabe, the system is a boolean algebra

Theory of $(R, *)$

Boris Karlov

- There is an infinite axiomatization
- A finite axiomatization is impossible
- The theory is decidable and PSPACE-complete

Theories of $(R, \cup, ^*)$ and $(R, \&, ^*)$

Dudakov & Karlov

- It is possible to interpret computations of counter machines
- The addition and multiplication of naturals are definable
- The elementary arithmetic can be interpreted

Theories of $(R, \cup, ^*)$ and $(R, \&, ^*)$

Inverse modeling

- Every regular language is a finite automaton
- Actions on automata can be defined in the elementary arithmetic
- The theory of $(R, \cup, \&, ^*)$ can be interpreted in the elementary arithmetic

Theory of $(R, \&)$

- A direct interpretation of counter machines is inevident

Different view

For an alphabet Σ there is an algebra of words $(\Sigma^*, \&)$

Every language is a subset of Σ^*

The language concatenation is a point-wise concatenation of word sets:

$$L_1 \& L_2 = \{w_1 \& w_2 : w_1 \in L_1, w_2 \in L_2\}$$

Theory of $(R, \&)$ is a special case

Let $\mathfrak{A} = (A, f_1, \ldots, f_n)$ be an algebra

Then operations $f_1, \ldots, f_n$ can be used for subsets of A:

$$f(A_1, \ldots, A_k) = \{f(a_1, \ldots, a_k) : a_i \in A_i\}$$

We have subsets algebras $(A', f_1, \ldots, f_n)$, where A' is a class of subsets closed under $f_1, \ldots, f_n$

Examples

The algebra of all subsets $\exp^* \mathfrak{A}$, the algebra of finite subsets $\exp \mathfrak{A}$ etc.

Some instances are trivial

The algebra of one-element subsets is isomorphic to the original:

$$\{a\} + \{b\} = \{a + b\}$$

Examples

Other example

For the additive monoid of naturals $(\omega, +)$ the algebra of non-empty intervals $[0, a]$ is isomorphic to the original $(\omega, +)$:

$$[0, a] + [0, b] = [0, a + b]$$

Question

What about other cases?

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Monadic second-order logic (MSO)

MSO admits variables and quantifiers on subsets of the domain

$$(\forall X)(\exists a)(X(a) \wedge \neg f(a) = a)$$

Weak MSO

Second-order variables denote only finite subsets

Interpretation

The algebra of (finite) subsets is interpretable in MSO (WMSO):

$$Y = f(X_1, \ldots, X_k) \equiv (\forall a)(Y(a) \leftrightarrow (\exists a_1, \ldots, a_k)(X_1(a_1) \wedge \cdots \wedge X_k(a_k) \wedge a = f(a_1, \ldots, a_k))$$

Corollary

The algebra of all (finite) subsets is a part of (weak) monadic second-order logic

Is there an opposite embedding?

Second-order logic admits first-order variables and the membership relation $a \in A$

There is no evident method to define this relation in the subsets algebra

Generally It Is Impossible

Dudakov

There is an algebra with undecidable theory, but the subsets algebra has decidable theory

For MSO and WMSO such case is impossible

Example

Let $K \subseteq 2P$, P be the set of all primes

$\mathfrak{A}_K = (A, f)$, f is a one-one function

For every $n \in K$ or $n \notin 2P$ there are infinitely many a such that $f^n(a) = a$, for every $n \in 2P \setminus K$ there is no such a

Example

Then the algebra $\exp \mathfrak{A}_K$ is isomorphic to $\mathfrak{A}_{2P}$, and its theory is decidable

The theory of $\mathfrak{A}_K$ can be undecidable for corresponding K

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Main result

Let $\Sigma = \{a\}$ be a one-letter alphabet

So the algebra of regular (or finite) languages $(R, \&)$ over Σ admits an interpretation of the elementary arithmetic

The algebra of all languages $(R, \&)$ over Σ admits an interpretation of the second order arithmetic

Decomposition

Empty language

$X = \varnothing \equiv (\forall Y)X = f(X, Y, \ldots, Y)$

For non-empty subsets $X_1, \ldots, X_k$ the set $f(X_1, \ldots, X_k)$ is non-empty

The algebra $\exp \mathfrak{A}$ is the union of $\{\varnothing\}$ and the algebra $\exp_0 \mathfrak{A}$ of non-empty languages

Decomposition

Every non-empty language X is equal to $X = \{a^n\}\&Y$, where the language Y contains the empty word

The algebra of non-empty languages $\exp_0 \mathfrak{A}$ is the product $\mathfrak{A}_1 \times \exp_e \mathfrak{A}$, where $\mathfrak{A}_1$ is the algebra of one-word languages, $\exp_e \mathfrak{A}$ is the algebra of languages with the empty word

$\mathfrak{A}_1$ is isomorphic to the additive arithmetic of naturals: $a^n \& a^m = a^{n+m}$

The matter is $\exp_e \mathfrak{A}$

Base of Proof

The ternary relation $P_3(X, Y, Z)$ that is

- $X = \{\varepsilon, w\}$
- $Y = \{\varepsilon, w^n\}$
- $Z = \{\varepsilon, w, w^2, \ldots, w^n\}$ for some n

Combinatorial Reasoning

$X = \{\varepsilon, w\}$ iff there are exactly two languages $U = \{\varepsilon, w^2\}$ and $V = \{\varepsilon, w, w^2\}$ such that $XU = XV = X^3$.

If $X = \{\varepsilon, w\}$, then $Y = X^n$ iff every non-trivial decomposition $Y = U\&V$ can be continued: $Y = U\&X\&V'$.

Interpretation of Arithmetic

It is enough to interpret the addition and the divisibility relation

- A domain is the class of languages of the form $\{\varepsilon, a^n\}$
- A natural number n corresponds to $\{\varepsilon, a^n\}$
- Let us fix $X_0 = \{\varepsilon, a\}$
- The domain is defined as $(\exists Z)P_3(X_0, Y, Z)$

Interpretation of Arithmetic

- $n + m = k$ corresponds to

$$\{\varepsilon, a, \ldots, a^n\} \& \{\varepsilon, a, \ldots, a^m\} = \{\varepsilon, a, \ldots, a^k\}$$

$$Y_1 + Y_2 = Y_3 \equiv (\exists Z_1, Z_2)(P_3(X, Y_1, Z_1) \wedge P_3(X, Y_2, Z_2) \wedge P_3(X, Y_3, Z_1 \& Z_2))$$

- $n|m$ corresponds to

$$Y_1 | Y_2 \equiv (\exists Z)(P_3(X, Y_1, Z_1) \wedge P_3(Y_1, Y_2, Z_2))$$

Corollaries

Let $(\omega, +)$ be the additive monoid of naturals. Then the theory of $\exp(\omega, +)$ is undecidable

Disjunctive polynomials: $\alpha_0 \vee \alpha_1 x \vee \cdots \vee \alpha_n x^n$, $\alpha x^i \vee \beta x^i = (\alpha \vee \beta) x^i$, $\alpha x^i \cdot \beta x^j = (\alpha \cdot \beta) x^{i+j}$. The multiplicative theory of disjunctive polynomials is undecidable

Further problem

An alphabet was one-letter

The previous result depends on the commutativity of the concatenation

For multiletter alphabets other interpretations are needed

Solution

To define some subalgebra of one-letter languages in the algebra of multiletter languages

$x = \{\varepsilon, c\}$, $c \in \Sigma$ iff [words x and uv commute iff words u and v commute]

A language commutes with $\{\varepsilon, c\}$ iff this language is one-letter

Final Result

Let Σ be an arbitrary alphabet

The algebra of all/regular/finite languages over Σ with the concatenation admits an interpretation of the elementary arithmetic

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Generalization

The algebra of all words with the concatenation is the free monoid

Can the previous result be generalized to other monoids?

Considered Monoids

Comutativity $xy = yx$

Cancellation $xy = xz \to y = z$

An element a of infinite order: the elements $a, a^2, a^3, \ldots$ are pairwise distinct

Generalization

Let $\mathfrak{A}$ be a commutative cancellative monoid with an element of infinite order. Then the theory of $\exp \mathfrak{A}$ admits an interpretation of the elementary arithmetic

Base of Proof

The basic reasoning is the same

Problems

- The free monoid is factorial: from $u_1v_1 = u_2v_2$ it follows that $u_1 = u_2w$ or $u_2 = u_1w$. But monoids can be non-factorial
- In the free monoid every element a has infinite order. But elements of finite order can exist

Base of Proof

Solution

To define a subclass of sets that has the same properties as factorial monoids and sets X of the form $\{e, a\}$, where a has an infinite order

- If Y is a power of X, then XY is a power of X
- If Y is a power of X, XY divides Z, then Z doesn't divide Y
- If Y and Z are powers of X, $Y = UZ$, and U contains a unique element, then U is invertible

Abelian Groups

An Abelian group is a commutative cancellative monoid

Corollary

Let an Abelian group $\mathfrak{A}$ contain an element of infinite order ($\mathfrak{A}$ is not a torsion group). So the elementary arithmetic can be interpreted in $\exp \mathfrak{A}$

Further Generalization

It is possible to eliminate the following conditions

- the cancellation
- the commutativity
- an element of infinite order

No Cancellation

Generally it is not possible

Counterexample

$(\omega, \max)$ is interpretable in $(\omega, <)$, but WMSO of $(\omega, <)$ is decidable (Rabin's Theorem)

No commutativity

May be

It is possible for groups

Theorem

If a group $\mathfrak{A}$ is not a torsion group, then in the theory of $\exp \mathfrak{A}$ the elementary arithmetic is interpretable

No Commutativity

Proof

Invertible elements in the monoid $\exp \mathfrak{A}$ are one-element subsets $X = \{a\}$ exactly

Let Z be the center of the centralizer of X. Then Z contains a, and if a is of infinite order, then the previous result on Abelian groups is applicable

Question

Does this result hold for torsion groups?

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Hardness

A direct generalization of the previous proofs is impossible for torsion groups since there are finitely many sets of the form $\{e, a^n\}$. All naturals can't be encoded by such sets

Another interpretation is needed

Torsion Groups of Unbounded Exponent

Exponent of a group is the least natural n such that $a^n = e$ for all a in the group

Example

The multiplicative group of roots of unity $\mathfrak{U} = (\mathbb{U}, \cdot)$, or the isomorphic additive group of rationals modulo 1

Compactness is not Applicable

An Abelian group of unbounded exponent is elementary equivalent to an Abelian group with an element of infinite order

For elementary equivalent systems $\mathfrak{A}$ and $\mathfrak{B}$ the systems $\exp\mathfrak{A}$ and $\exp\mathfrak{B}$ can be elementary nonequivalent

Compactness is not Applicable

Example

Let $\mathfrak{A}$ consist of non-intersecting finite cyclic groups of unbounded order, and $ab = e_1$ for a and b from distinct groups

Then there is $\mathfrak{B} \equiv \mathfrak{A}$, and $\mathfrak{B}$ contains an instance of infinite cyclic group

$\exp \mathfrak{A}$ and $\exp \mathfrak{B}$ are not elementary equivalent

In $\exp \mathfrak{A}$ every finite subset can be include into a finite subsystem, in $\exp \mathfrak{B}$ this doesn't hold.

Torsion Groups of Infinite Exponent

Two-elements sets

Can be defined the same way

Exceptions

The previous method can be used for elements of order 5 and greater. For elements of less orders implicit definitions can be used

Powers of Two-Elements Sets

Can be defined the same way

Group of Unity Roots

In $\exp \mathfrak{U}$ the elementary arithmetic can be interpreted

For every positive n there is the unique subgroup of order n, every subgroup is cyclic

Group of Unity Roots

The domain is the sets of finite subgroups, a natural number n is interpreted as the subgroup of order n

To interpret the elementary arithmetic we define

- Divisibility
- Co-prime relation
- Multiplication of co-primes
- Linear order
- Multiplication of arbitrary naturals

Group of Unity Roots

Divisibility

Subgroups inclusion

Co-prime relation

There is a unique common subgroup

Multiplication of co-primes

Subgroups product

Group of Unity Roots

Linear order

Subgroups are generated by $X = \{e, c^n\}$ and $Y = \{e, c^m\}$.
Then $\langle Y \rangle < \langle X \rangle$ $(n < m)$, iff there is a power of $Z = \{e, c\}^k = \{e, c, \ldots, c^k\}$, $k = n - 1$, such that ZX is a power of $\{e, c\}$:

$$ZX = \{e, c, \ldots, c^{2n-1}\} = \{e, c\}^{2n-1},$$

and ZY is not a power:

$$ZY = \{e, c, \ldots, c^{n-1}, c^m, \ldots, c^{m+n-1}\}$$

Group of Unity Roots

Powers of primes

They are not products of co-primes

Multiplication of powers of some prime

$p^n p^m = p^k$ iff p^k is the greatest power of p that is less than $p^n(p^m + 1)$.

Multiplication of arbitrary naturals

is defined by the decomposition into primes

Arbitrary Abelian Groups of Unbounded Exponent

A combination of previous methods

A domain is the set of pairs $\{e, a\}$ and $\{e, a\}^n$.

Difference: $\{e, a\}$ was fixed, and now it can vary

The base is the same relation P_3.

Arbitrary Abelian Groups of Unbounded Exponent

Problem

For P_3 we need an infinite amount of sets $\{e, a\}^n$. For torsion groups there are finitely many such sets

Solution

"Transform" pair $(\{e, a\}, \{e, a\}^n)$ into $(\{e, b\}, \{e, b\}^n)$ where c is of greater order

Arbitrary Abelian Groups of Unbounded Exponent

Transformation

Combinatorial reasoning

Three-items sets

A set X contains exactly three items $\{e, a, b\}$ iff there are exactly seven sets U_i such that $XU_i = X^3$.

Arbitrary Abelian Groups of Unbounded Exponent

Equality

For sets $\{e, a\}$ and $\{e, b\}$ (with some restrictions for a and b)

$$\{e, a\} \cdot \{e, b\} \cdot \{a, b\} = \{e, a, b\} \cdot \{a, b, ab\}$$

$$\{e, a\} \cdot \{e, b\} \cdot \{e, ab\} = \{e, a, ab\} \cdot \{e, b, ab\}$$

There is no other cases for the last three sets in both equalities

Arbitrary Abelian Groups of Unbounded Exponent

Equality

Powers $\{e,a\}^n$ and $\{e,b\}^m$ are equal $(n=m)$ iff there are three sets $\{e,c\}$, $\{e,p,q\}$, $\{e,r,s\}$ such that

$$\{e,a\}\cdot\{e,b\}\cdot\{e,c\}=\{e,p,q\}\cdot\{e,r,s\}$$

and

$$\{e,a\}^n\cdot\{e,b\}^m\cdot\{e,c\}^k=\{e,p,q\}^\ell\cdot\{e,r,s\}^i$$

for some i,k,ℓ

1 Origin of the problem

2 Subset algebra and second-order logic

3 Results on Languages

4 Generalization

5 Torsion groups

6 Open Questions

Torsion Groups of Finite Exponent

Does the previous result hold for Abelian groups of finite exponent?

Non-cancellative Monoids

When does the previous result hold for non-cancellative monoids?

Non-commutative monoids

When does the previous result hold for non-commutative monoids?

Axiomatization

Is there an axiomatization for monoids of the form $\exp \mathfrak{A}$ or $\exp^* \mathfrak{A}$?

Thank you!