On Undecidability of Subset Theory for Some Monoids

S M Dudakov
Department of Applied Mathematics and Cybernetics, Tver State University, Zhelyabova str., 33, Tver, 170100, Russia
E-mail: sergeydudakov@yandex.ru

Abstract. Early we (with B. N. Karlov) have proved the following claim for the infinite cyclic monoid \(A\). Let \(\text{exp}A\) be an algebra of finite subsets of \(A\) with the same operation, \(\text{exp}A\) must be a monoid again. So the theory of \(\text{exp}A\) is equivalent to elementary arithmetic. Thus, the theory of the monoid \(\text{exp}A\) is undecidable. Here we consider an arbitrary commutative cancellative monoid \(A\) with an element of infinite order, and generalize the previous claims to the corresponding monoid \(\text{exp}A\).

1. Introduction
Monoids (semigroups with the neutral element) are the most general kind of associative algebras. A lot of traditional universes are monoids: numbers, polynomials, matrices with addition or multiplication, words with concatenation, functions with composition etc. Monoids are tightly connected with various concepts of computation theory (see [1, 2]), they can be used to describe algorithms or automata. So algorithmic problems of monoid theory are actively investigated (see [3, 4]).

Investigations of formal theories are among the central problems of mathematical logic. These problems are not only of great theoretical value but have practical significance. One of its applications is database query languages. Usually such languages are variants of logic languages, while databases themselves are finite structures. This concept of relational databases was introduced by E. F. Codd in [5]. Since in real systems database items are encoded by some mathematical objects (numbers, words and so on), there are some “natural” operations or relations on such objects. For example, those can be arithmetical operations, word concatenation, or comparisons. Hence, a real database is a finite structure embedded into some infinite universe (see [6]). Therefore, a database query planner must operate with some logic language on a given universe.

Modern database management systems allow to construct aggregate types and use database items of such types. In such a manner we can define arrays, maps, sets consisting of numbers, words, Boolean values etc. These aggregates are finite due to “natural” restrictions of storage capacity. So we have a complex structure, which can contain not only atomic objects but aggregates, for example, finite sets of such objects.

Another way, which leads to the same concept, is a determinization process of automata (see [1]). The universal method is to consider sets of non-deterministic automaton states as
states of new deterministic automaton. If the original automaton is presented as semigroup (see [7]), so its deterministic version corresponds to semigroup of subsets.

We have to note that such construction of the subset algebra is not equivalent to the monadic second order logic for the original algebra. The second order language (see [8]) admits first order variables to denote first order objects (elements of the original algebra). But in the first order theory of the subset algebra we don’t have such variables generally. The described difference is important because there exist examples (constructed in [9]), where the first order theory of the subset algebra is algorithmically simpler than the theory of the original algebra. For second order logic it is impossible.

Algorithmic properties of subset algebras and its theories are very different. As we mentioned in the previous paragraph, the theory of the finite subset algebra can be decidable, while the theory of the original one is not (see [9]). And vice versa, there are algebras with decidable theories such that the corresponding subset algebras have undecidable theories. Such algebras appear when we investigate languages theory [1]: every language is a set of words, which are elements of free monoid (with concatenation). So the concatenation of entire languages can be considered as a generalization of the word concatenation onto sets of word. In this way, some result were established in [10–12].

In particular, one of these results is the following: if \( \mathfrak{F} \) is the free cyclic monoid (such as the set of natural numbers with addition), then the theory of finite subsets of \( \mathfrak{F} \) is algorithmically equivalent to elementary arithmetic. It was proved in [11], Corollary 1. The natural question appears: can we generalize this result to some wider class of monoids? Or, may be, the free cyclic monoid is a rare exception?

In this paper we show how to generalize the mentioned result from [11]. We establish such result for monoids those are simultaneously commutative, cancellative and have elements of infinite order. Instances of such monoids are the set of natural numbers with multiplication, the set of polynomials with multiplication, arbitrary linear space with addition over a field of characteristic zero, and many other classic algebras. In particular, every Abelian group that is not a torsion group satisfies these conditions.

2. Definitions and Basic Properties

The following basic concepts of monoid theory can be found in the book [13].

A monoid \( \mathfrak{A} = (A, *, e) \) is a non-empty set \( A \) with a binary operation \( * \) on it. Elements of the monoid \( \mathfrak{A} \) are elements of the set \( A \). The operation \( * \) is called usually “multiplication”, it must be associative: \( a * (b * c) = (a * b) * c \) for every \( a, b, c \in \mathfrak{A} \), and \( e \) must be the (necessarily unique) neutral element: \( a * e = e * a = a \) for every \( a \in \mathfrak{A} \).

A monoid \( \mathfrak{A} \) is commutative if \( a * b = b * a \) for all \( a, b \in \mathfrak{A} \).

An element \( a \) of a monoid has an infinite order if all powers \( a^0 = e, a^1 = a, a^2, \ldots \) are pairwise distinct. Otherwise, the element \( a \) is of finite order.

An element \( a \) of a commutative monoid \( \mathfrak{A} \) is cancellative if \( b = c \) whenever \( b * a = c * a \) for each \( b, c \in \mathfrak{A} \). A monoid \( \mathfrak{A} \) is cancellative if every element of \( \mathfrak{A} \) is cancellative.

An element \( a \) of a commutative monoid is invertible if \( a * b = e \) for some \( b \). This element \( b \) is unique and is denoted by \( a^{-1} \).

On subsets of a monoid \( \mathfrak{A} \) we can also define the binary operation: if \( x, y \subseteq \mathfrak{A} \), then

\[ x * y = \{ a * b : a \in x, b \in y \}. \]

If the set \( x \) contains a unique element \( a \), then we write \( a * y \) instead of \( x * y \) or \( \{ a \} * y \). For instance, we get \( x * \emptyset = \emptyset, \{ e \} * y = e * y = y \). The last equality means that the set \( E = \{ e \} \) is the neutral element for the operation \( * \) on subsets of \( \mathfrak{A} \). The operation \( * \) on subsets is associative (commutative) whenever the operation \( * \) has corresponding properties. Also, it is clear that the
product $x \ast y$ is a finite set whenever the sets $x$ and $y$ are finite. Therefore, for any commutative monoid $\mathbb{A} = (A, \ast, e)$ there is the commutative monoid $\exp \mathbb{A} = (\Pi_{\text{fin}}(A), \ast, E)$, where $\Pi_{\text{fin}}(A)$ is the set of all finite subsets of $\mathbb{A}$.

If a monoid $\mathbb{A}$ is cancellative, then the function $b \mapsto a \ast b$ on $\mathbb{A}$ is injective for any fixed element $a$. So for cardinalities we have $|x| = |a \ast x|$ for each $x \in \exp \mathbb{A}$ and $a \in \mathbb{A}$. Also, for every $x, y \in \exp \mathbb{A}$, $y \neq \emptyset$, the equality $x \ast y = \bigcup_{a \in x} a \ast y$ holds, so $|x \ast y| \geq |x|$.

In any commutative monoid the divisibility relation is definable:

$$x \mid y \equiv (\exists z)z \ast x = y.$$ 

We can define the set $Q$ of invertible elements:

$$Q(x) \equiv (\exists y)x \ast y = e.$$ 

The divisibility relation is transitive and reflexive, so the mutual divisibility relation

$$x \sim y \equiv x \mid y \land y \mid x$$

is an equivalency. Also, the last relation can be defined as $x$ and $y$ are distinguished by some invertible multiplier:

$$x \sim y \equiv (\exists z)(Q(z) \land x = z \ast y).$$

The empty set $\emptyset$ is a zero of the monoid $\exp \mathbb{A}$ and has corresponding definition:

$$x = \emptyset \equiv (\forall y)x \ast y = x$$

because $\emptyset \ast y = \emptyset$ for all $y$, but $x \ast y \neq x$ if $x \neq \emptyset$ and $y = \emptyset$.

Everywhere in the following we consider an arbitrary commutative cancellative monoid $\mathbb{A}$ with at least one element of infinite order. Hence, there is the commutative monoid $\exp \mathbb{A}$. We consider only non-zero elements of the monoid $\exp \mathbb{A}$, i.e. non-empty sets. These elements form a submonoid of $\exp \mathbb{A}$ because $x \ast y \neq \emptyset$ whenever the sets $x$ and $y$ are not empty.

Further, we write $xy$ everywhere instead of $x \ast y$. Also, we use letters $a, \ldots, k$ to denote elements of an original monoid $\mathbb{A}$ whereas letters $t, \ldots, z$ are used to denote elements of the corresponding monoid $\exp \mathbb{A}$.

It is easy to prove the next claim.

**Proposition 1.** Invertible elements of the monoid $\exp \mathbb{A}$ are sets of the form $\{a\}$ exactly, where $a$ is an invertible element of $\mathbb{A}$.

**Proof.** Such elements are invertible: $\{a\}\{a^{-1}\} = \{e\} = E$.

Let us consider any set $y = \{a, b, \ldots\}$ of the monoid $\exp \mathbb{A}$. If $y$ is invertible, then we get $yz = E = \{e\}$ for some $z$. Hence, for any $c \in z$ we have $ac = e = bc$ and $a = b$ due to cancellation in $\mathbb{A}$. So $y$ must have one element exactly.

If $a$ is not invertible in $\mathbb{A}$, then $\{a\}$ is not invertible in $\exp \mathbb{A}$ because $\{a\}x$ doesn’t contain $e$, so $\{a\}x \neq E$.

Therefore, each invertible element of $\exp \mathbb{A}$ is $\{a\}$ for a suitable invertible $a$. \qed

Another simple claim is

**Proposition 2.** If $u, v \in \exp \mathbb{A}$ and $e \in u$, then $v \subseteq uv$.

**Proof.** Let $u = \{e\} \cup u'$. Then,

$$uv = \{e\}u \cup u'v = v \cup u'v$$

that follows the claim. \qed
3. Definability of Powers
The main goal of our paper is to interpret elementary arithmetic in the monoid \( \exp \mathfrak{A} \), where \( \mathfrak{A} \) is a commutative cancellative monoid with an element of infinite order. To do that we sequentially define some relations and establish its properties.

The first ones are used to distinguish sets of one or two elements:
\[
R_1(x) \equiv (\forall u)(xu = x^3 \rightarrow u = x^2);
\]
\[
R_2(x) \equiv (\exists u)(u \neq x^2 \land xu = x^3 \land (\forall v)(xv = x^3 \rightarrow v = u \lor v = x^2)).
\]

Proposition 3. The formula \( R_1(x) \) is true in the monoid \( \exp \mathfrak{A} \) if and only if the set \( x \) consists of one element exactly.

Proof. If \( x = \{a\} \), then the equality \( xu = x^3 \) follows \( ab = a^3 \) for all \( b \in u \). So we have \( b = a^2 \) due to cancellation. Therefore, \( u = \{a^2\} = x^2 \).

Let us suppose the set \( x \) contains at least two different elements \( a \) and \( b \). Then, consider the set \( u = x^2 \setminus \{ab\}. \) Evidently, \( xu \subseteq x^3 \).

Now we must show the inclusion \( x^3 \subseteq xu \). Let us consider an arbitrary item of \( x^3 \). This item is of the form \( fcd \), where \( f, c, d \in x \). There are three possible cases.

- In the case \( cd \neq ab \) we have \( cd \in u \) and \( fcd = f(cd) \in xu \).
- The second case is \( cd = ab \) and \( f \neq a \). Then, we can transform \( fcd = fab = a(fb) \). Since \( f \neq a \), we can conclude \( fb \neq ab \) using cancellation. The last inequality follows \( fb \in u \) and \( fcd = a(fb) \in xu \).
- The last case is \( cd = ab \) and \( f = a \). Thus, we have the equality \( fcd = caba = ba^2 \). According to cancellation we have \( a^2 \neq ab \) and \( fcd = ba^2 \in xu \).

Hence, we have proved \( fcd \in xu \) in any case, so \( x^3 \subseteq xu \). Consequently, \( xu = x^3 \).

Therefore, there exists \( u \) such that \( u \neq x^2 \) and \( xu = x^3 \), so the formula \( R_1(x) \) is false. \( \square \)

Proposition 4. Let the formula \( R_2(x) \) be true in the monoid \( \exp \mathfrak{A} \). Then, the set \( x \) consists of two elements exactly.

Proof. By the definition of the relations \( R_1 \) and \( R_2 \), it follows immediately that if \( R_2(x) \) is true then \( R_1(x) \) is false. Hence, if the formula \( R_2(x) \) is true, then \( x \) can’t contain one element exactly due to Proposition 3.

Now let us assume that a set \( x \) contain at least three different items: \( x = \{a, b, c, \ldots\} \), where \( a, b, \) and \( c \) are pairwise distinct. Consider two sets: \( v_1 = x^2 \setminus \{ab\} \) and \( v_2 = v_1 \setminus \{ac\} \). We have \( ab \neq ac \) due to cancellation in \( \mathfrak{A} \), so the following proper inclusions hold: \( v_2 \subseteq v_1 \subseteq x^2 = x^3 \).

Now if we prove the inclusion \( x^3 \subseteq xv_2 \), then we obtain \( xv_2 = xv_1 = x^3 \). The last equalities follow the falsehood of the formula \( R_2(x) \) because the sets \( v_1, v_2, \) and \( x^3 \) are pairwise distinct.

Therefore, the formula \( R_2(x) \) is true only if \( x \) contains two elements exactly.

At last, let us prove the inclusion \( x^3 \subseteq xv_2 \). The set \( v_2 \) must contain all products \( a \gamma \) (where \( \gamma \in x \)) from \( x^2 \) except for \( ab \) and \( ac \). Also, according to cancellation the set \( v_2 \) must contain \( bc \): if \( bc = ab \) then \( a = c \), if \( bc = ac \) then \( a = b \), both cases are impossible. Let us consider an arbitrary triple product \( cdf \in x^3 \), where \( c, d, f \in x \). If \( cdf \) is not equal to any triple product with \( a \), then \( cdf \in xv_2 \). Otherwise, we consider all the possible triple products with \( a \):

- \( abc = a(bc) \in xv_2 \);
- if \( b^2 = ac \), then \( abb = ab^2 = a(ac) = ca^2 \in xv_2 \);
- if \( b^2 \neq ac \), then \( abb = ab^2 \in xv_2 \), because \( b^2 \neq ab \) due to cancellation;
- \( ab \gamma = b(a \gamma) \in xv_2 \) for any \( \gamma \notin \{b, c\} \).
• products of the form $ac^\gamma$ are considered analogously to the products $ab^\gamma$;
• $a^\gamma b^\delta = \gamma(a^\delta b) \in xv_2$, where $\gamma, \delta \notin \{b, c\}$.

Thus, we have proved the needed inclusion $x^3 \subseteq xv_2$.

Further, consider the binary relation $P$:

$$P(x, y) \equiv \neg Q(x) \land \neg Q(y) \land (\forall u, v)(y = uv \land \neg Q(v) \rightarrow \exists \ell y = uxt)$$

and the unary relation $L$:

$$L(x) \equiv R_2(x) \land (\forall u, v)(x = uv \rightarrow Q(u) \lor Q(v)) \land$$
$$\land (\forall y)(P(x, y) \rightarrow P(x, xy)) \land$$
$$\land (\forall y, z)(P(x, y) \land xy | z \rightarrow \neg z | y) \land$$
$$\land (\forall y, z, u)(P(x, y) \land P(x, z) \land y = zu \land R_1(u) \rightarrow Q(u)).$$

**Proposition 5.** Let the formula $L(x)$ be true in the monoid $\exp \mathfrak{A}$. By Proposition 4, it follows that $x = \{a, b\}$ for some different $a, b \in \mathfrak{A}$. Then,

(i) for all natural numbers $m > 0$ the formula $P(x, y)$ is true whenever $y \sim x^m$;
(ii) at least one item of the set $x$ has infinite order in the monoid $\mathfrak{A}$;
(iii) for all natural numbers $l > 0$ we have $a^l \neq b^l$;
(iv) for all natural numbers $m > 0$ the set $x^m$ contains exactly $m + 1$ elements of the form $a^kb^{m-k}$, where $k = 0, \ldots, m$.

**Proof.** The truth of $y \sim x^m$ means $y = x^m w$ for some invertible element $w$ of $\exp \mathfrak{A}$. We prove Claim (i) by induction. For $m = 1$ consider the relation $P(x, x^1 w)$. Since $x = \{a, b\}$, by Proposition 1, it follows that $x$ is not invertible. Thus, the element $x^1 w$ is not invertible too. Further, let $uv = x^1 w$, and $v$ be not invertible. Then, $vu^{-1}$ is not invertible also, hence, $u(vu^{-1}) = x$ and (1) follow $u$ to be invertible. Thus, we obtain $v = uv^{-1} w$ and $xw = ux(u^{-1} w)$. Therefore, we have proved the truth of $P(x, x^1 w)$. For every $m > 1$ the truth of $P(x, x^m w)$ can be easy concluded from (2) by induction.

To prove Claim (ii) let us suppose both elements of $x$ are of finite order. Thus, there exist finitely many non-equal products of the form $a^kb^n$. Let $M$ be the amount of all such products. For all natural $m > 0$ the power $x^m$ consists of such products only, so there exist at most $2M$ different sets of the form $x^m$. But $m$ itself can have infinitely many values, so there are natural numbers $m_1$ and $m_2$ such that $m_1 < m_2$ and $x^{m_1} = x^{m_2}$. It follows that $xx^{m_1} | x^{m_2}$. By Claim (i), we have the truth of $P(x, x^{m_1})$. Then, by (3), we can conclude that $x^{m_2} | x^{m_1}$ is false. Hence, we have got a contradiction with $x^{m_1} = x^{m_2}$. Therefore, our assumption is false, at least one item of $x$ must have infinite order.

Now we have to prove Claim (iii). Let us assume that $a^l = b^l$ for some natural number $l > 0$. Then, for any natural number $q \geq l$ we have $a^qb^q = a^{q+l}b^{q-l}$. So an arbitrary product $a^{m-s}b^s$ must be equal to some product $a^{m-r}b^r$, where $r < s$. For every natural $m \geq l$ the power $x^m$ consists of products $a^{m-s}b^s = a^{m-r}b^r$. Since $r < s$, we have $m - r > m - l$ and $x^m = a^{m-l}x_m$, where the set $x_m$ contains only products $a^p b^q$ with $p + q < l$. There exist finitely many products of the last form, hence, there exist finitely many different $x_m$. Thus, there must exist $x_s$ such that $x_m = x_s$, infinitely often. In particular, we can select $x_m = a^{m-l}x_s$ and $x^{m+n} = a^{m+n-l}x_s$ for some $n > 0$, then, we get $x^{m+n} = \{a^n\} x_s$. By Claim (i), it follows that the formulas $P(x, x^m)$ and $P(x, x^{m+n})$ are true. Since $R_1(\{a^n\})$ is true, we can use (4), so $\{a^n\}$ is invertible. The inequality $n > 0$ follows $xx^m | x^{m+n}$. Now we can apply (3), then, $x^m$ is not
divisible by $x^{m+n}$. The last follows that $\{a^n\}$ is not invertible. This contradiction proves the falsehood of the assumption $a^i = b^j$.

At last, let us prove Claim (iv). According to Claim (ii) we can suppose that $a$ has infinite order in the monoid $\mathfrak{A}$. We note earlier that the power $x^m$ consists of all products of the form $a^k b^{m-k}$, where $k = 0, 1, \ldots, m$. If we suppose that there are equal products for different $k$ (i.e. $a^k b^{m-k} = a^{k'} b^{m-k'}$ for $k_1 < k_2$), then we obtain $b^{k_2-k_1} = a^{k_2-k_1}$ using cancellation. It contradicts Claim (iii).

Now we can prove the inverse of Claim (i) in the previous proposition.

**Proposition 6.** Let $L(x)$ be true in the monoid $\exp \mathfrak{A}$. Then, $P(x, y)$ follows that $y \sim x^m$ for some natural number $m > 0$.

**Proof.** The part (1) of the $L$ definition means $R_2(x)$. So using Proposition 4 we have $x = \{a, b\}$ for some $a \neq b$.

The truth of $P(x, y)$ implies immediately that the element $y$ is not invertible. It is clear that $y = Ey$. From the definition of $P$ we obtain $y = Ey = x^1 w_1$ for some $w_1$. If $w_1$ is not invertible, then we again use the equality $y = x^1 w_1$ to obtain $y = x^1 w_2 = x^2 w_3$ for some $w_2$, and so on. We can do it while $w_n$ is not invertible, so we get $y = x^m w_m$ for some $w_m$. Later we show that the number $m$ can’t grow infinitely. Hence, we can select the maximal $m$ such that there is the presentation $y = x^m w_m$. If $w_m$ is not invertible, then analogously we can obtain $y = x^{m+1} w_{m+1}$, it contradicts the maximality of $m$. Therefore, $w_m$ is invertible, and we have proved $y \sim x^m$.

Now we need to prove the used claim: there is an upper bound of $m$ such that $y = x^m w_m$. Let us suppose this bound doesn’t exist. So there exist infinitely many natural numbers $m$ such that $y = x^m w_m$. The power $x^m$ consists of $m + 1$ elements exactly, it is followed by Claim (iv) of Proposition 5. But for cardinality of sets we have the inequality $|x^m| \leq |x^m w_m| = |y|$ that means $|y| \geq m + 1$. The monoid $\exp \mathfrak{A}$ consists of finite sets, so the inequality $|y| \geq m + 1$ can’t be true for infinitely many $m$. Therefore, the assumption is false.

If we combine the last two propositions, then we obtain

**Corollary 7.** Let $L(x)$ be true in the monoid $\exp \mathfrak{A}$. Then, $P(x, y)$ is true if and only if $y \sim x^m$ for some natural number $m > 0$.

The previous claims are useful if the monoid $\exp \mathfrak{A}$ actually contains elements $x$ those satisfy $L(x)$. So we need to prove such $x$ exists.

**Proposition 8.** Let $g,a \in \mathfrak{A}$, the element $g$ be invertible, and the element $a$ be of infinite order. Then, for the set $x = g\{e, a\}$ the formula $L(x)$ is true in the monoid $\exp \mathfrak{A}$.

**Proof.** At first, consider the condition $R_2(x)$ from (1). Let $u = g^2\{e, a^2\}$. Then,

$$xu = g^3\{e, a\} \{e, a^2\} = g^3\{e, a, a^2, a^3\} = x^3.$$

If we suppose $g^2\{e, a^2\} = u = x^2 = g^2\{e, a, a^2\}$, then multiplying by $g^{-2}$ we obtain the equality $\{e, a^2\} = \{e, a, a^2\}$ and $a \in \{e, a^2\}$. Both cases $a = e$ and $a = a^2$ mean the finite order of $a$. It contradicts the proposition assumption.

Now let $xv = x^3$ that means $gv \cup gav = g^3\{e, a, a^2, a^3\}$. So $gv \subseteq g^3\{e, a, a^2, a^3\}$ and $v \subseteq g^2\{e, a, a^2, a^3\}$. It is enough to check all subsets of $g^2\{e, a, a^2, a^3\}$ to prove that $v$ must be equal to $x^2$ or $u$.

Consider the second part of line (1). Let $uv = x$ or $(g^{-1} u)v = g^{-1} x$ for suitable $u$ and $v$. The neutral element $e$ of $\mathfrak{A}$ belongs to the set $g^{-1} x$, hence, for some invertible $c \in \mathfrak{A}$ we have $c \in g^{-1} u$ and $c^{-1} \in v$. Then, $e$ belongs to the sets $u' = c^{-1} g^{-1} u$ and $v' = cv$. By Proposition
Now we are ready to do the last steps and to construct an interpretation of elementary arithmetic.

4. Interpretation of Elementary Arithmetic

Now we are ready to do the last steps and to construct an interpretation of elementary arithmetic in the monoid \( \exp \mathfrak{A} \). Let us introduce the following two relations:

\[
D(x, y, z) \equiv P(x, y) \land R_2(z) \land z y = y^2; \\
C(x, z) \equiv (\exists y) D(x, y, z).
\]

2, it follows that \( u', v' \subseteq u'v' = g^{-1}uv = g^{-1}x \). Let us assume that both sets \( u' \) and \( v' \) contain non-neutral elements \( b \) and \( d \) correspondingly. As \( u', v' \subseteq g^{-1}x = \{e, a\} \), so we have \( b, d \in \{e, a\} \) and \( b = d = a \). Thus, we obtain \( bd \in u'v' = g^{-1}x = \{e, a\} \). If \( bd = e \), then \( a^2 = e \) and \( a \) has finite order. If \( bd = a \), then \( a^2 = a \) and again \( a \) has finite order. Both cases lead to the contradiction, hence, our assumption is wrong, \( u' \) or \( v' \) must be equal to \( \{e\} \), and elements \( u = cu'u' \) or \( v = c^{-1}v' \) is invertible.

To prove another parts of the L definition we establish the following fact: \( P(x, y) \) is true if and only if \( y \sim x^m \) for some natural number \( m > 0 \).

If \( P(x, y) \) is true, then we can use the same methods as in the proof of Proposition 6 and obtain \( y = x^m w_m \) for natural numbers \( m > 0 \) while \( w_m \) is not invertible. But \( x^m = g^m \{e, a, a^2, \ldots, a^m\} \), \( a \) has infinite order, hence, the cardinality of \( x^m \) is \( m + 1 \). This cardinality must be less or equal to the cardinality of \( y \), so \( m \) can’t grow infinitely. Then, for some \( m \) we must have \( y = x^m w_m \) for some invertible \( w_m \), i.e. \( y \sim x^m \).

Now let \( y \sim x^m \) and \( y = x^m w \) for some natural number \( m > 0 \) and some invertible \( w \). We have demonstrated yet that the cardinality of \( x^m w \) is \( m + 1 > 1 \), so \( x \) and \( y \) are not invertible due to Proposition 1. Let \( uv = y = x^m w \) for non-invertible \( v \), then, \( (w^{-1} g^{-m} u) v = g^{-m} x^m = \{e, a\}^m \).

The set \( \{e, a\}^m \) contains the neutral element \( e \), hence, there exists an invertible element \( c \in \mathfrak{A} \) such that \( c \in w^{-1} g^{-m} u \) and \( c^{-1} \in v \). Thus, both sets \( u' = c^{-1} w^{-1} g^{-m} u \) and \( v' = cv \) contain \( e \), and we have \( u' \subseteq u'v' = \{e, a\}^m \). Select the greatest natural number \( k \) such that \( a^k \in v' \). Let us note \( k > 0 \) because the sets \( v \) and \( v' \) are non-invertible, but the set \( \{e\} \) is invertible. Easy to see \( v' \subseteq \{e, a\}^k \), so we have \( \{e, a\}^m = u'v' \subseteq u'(e, a)^k \subseteq \{e, a\}^m \). The last inclusion holds because the set \( u'(e, a)^k \) can’t contain powers \( a^n \) for \( n > m \) and the set \( \{e, a\}^m \) contains all such powers. Then,

\[
\{e, a\}^m = u'(e, a)^k = c^{-1} w^{-1} g^{-m} u(e, a)(e, a)^{k-1}.
\]

Multiplying the last equality by \( g^m w \) we have

\[
y = x^m w = \{e, a\}^m g^m w = c^{-1} u(e, a)(e, a)^{k-1} = c^{-1} g^{-k} u(g(e, a))(g(e, a))^{k-1} = u x (c^{-1} g^{-k} x^{k-1})
\]

that means the truth of the implication in the \( P \) definition.

The proved claim implies (2) immediately.

Let us prove the part (4). If the formulas \( P(x, y) \) and \( P(x, z) \) are true, then we get \( y = x^{m_1} w_1 \) and \( z = x^{m_2} w_2 \) for some invertible \( w_1 \) and \( w_2 \) and some natural \( m_1 \) and \( m_2 \). By Proposition 1, the invertible elements \( w_1 \) and \( w_2 \) of \( \exp \mathfrak{A} \) are of the form \( \{g_1\} \) and \( \{g_2\} \) correspondingly for some invertible elements \( g_1 \) and \( g_2 \) of the monoid \( \mathfrak{A} \). So the equality \( y = z u \) means \( g_1 x^{m_1} = g_2 x^{m_2} u \). If the formula \( R_1(u) \) is true, then \( u = \{h\} \) for some \( h \in \mathfrak{A} \) and we have \( g_1 x^{m_1} = g_2 h x^{m_2} \). In particular, the set \( g_1 x^{m_1} \) contains \( g_1 g^{m_1} \), hence, \( g_1 g^{m_1} = g_2 h g^{m_2} a^k \in g_2 h x^{m_2} \) for some \( k \leq m_2 \) and \( h(g_1^{-1} g_2 g^{m_2-m_1} a^k) = e \). Therefore, \( h \) is invertible in the monoid \( \mathfrak{A} \), and \( u = \{h\} \) is invertible in \( \exp \mathfrak{A} \).

To prove (3) let again \( P(x, y) \) be true, so \( y = x^m w \) for some invertible \( w \). If we suppose the truth of both \( z y \mid z \) and \( x z \mid y \), then \( x x^m w u = z \) and \( x^m w = z v \) for some \( u \) and \( v \). So we have \( x^m w = x x^m w u w = x^{m+1} w u w \) and \( x^m = x^{m+1} w \). The last equality is impossible because the cardinality of the first set is less than of the second one.

\( \square \)
Proposition 9. Let \( g, a \in \mathcal{A} \), the element \( g \) be invertible, and the element \( a \) be of infinite order in the monoid \( \mathcal{A} \). Let \( L(x) \) be true in the monoid \( \exp \mathcal{A} \) for \( x = g \{ e, a \} \). Then,

(i) the formula \( D(x, x^n w, z) \) is true in the monoid \( \exp \mathcal{A} \) for every \( z = g^n \{ e, a^n \} w \), where \( n \) is an arbitrary natural number and \( w \) is an arbitrary invertible element of \( \exp \mathcal{A} \);

(ii) let \( z \in \exp \mathcal{A} \) be such that the formula \( C(x, z) \) is true. Then, there exists exactly one natural number \( n \) such that the formula \( D(x, x^n w, z) \) is true in the monoid \( \exp \mathcal{A} \) for some invertible element \( w \).

Proof. To prove Claim (i) we use Proposition 8, so the formula \( R_2(z) \) is true. To establish the equality \( zz'w = (x^n w)^2 \) let us consider

\[
zz'w = g^n \{ e, a^n \} w(g\{ e, a \})^n w = g^n \{ e, a^n \} g^n \{ a^k : k = 0, \ldots, n \} w^2 =
\]

\[
g^{2n} \{ a^k : k = 0, \ldots, n \} \cup \{ a^{n+k} : k = 0, \ldots, n \} w^2 =
\]

\[
g^{2n} \{ a^k : k = 0, \ldots, 2n \} w^2 = g^{2n} \{ e, a \} 2n w^2 = (x^n w)^2.
\]

The formula \( P(x, x^n w) \) is true due to Corollary 7.

Now let us establish Claim (ii). The formula \( C(x, z) \) follows \( D(x, y, z) \) for some \( y \). The formula \( D(x, y, z) \) contains \( P(x, y) \), hence, by Corollary 7, we conclude \( y = x^n w \) for some natural number \( n \) and invertible \( w \). Let us suppose there exists at least two different natural numbers \( n_1 \) and \( n_2 \) satisfying \( D(x, x^{n_i} w, z) \), \( i = 1, 2 \). We can assume \( n_1 < n_2 \), then, \( x^{n_1} w_1 = z = x^{n_1} w_2^1 \) and \( x^{n_2} w_2 = x^{2n_2} w_2^2 \). Futher,

\[
x^{2n_2} w_2^2 = x^{n_2} w_2 z = w_2 w_1^{-1} x^{n_2-n_1} x^{n_1} w_1 = w_2 w_1^{-1} x^{n_2-n_1} x^{2n_1} w_2^1 = w_2 w_1 x^{n_2+n_1}.
\]

Now we can cancel the equality by \( w_2 \) and obtain \( x^{2n_2} w_2 = x^{n_2+n_1} w_1 \). Remember, that both \( w_1 \) and \( w_2 \) have exactly one element (Proposition 1), the power \( x^m \) has exactly \( m + 1 \) elements (Claim (iv) of Proposition 5). So the last equality is possible only for \( 2n_2 = n_2 + n_1 \) that means \( n_1 = n_2 \). It contradicts our assumption \( n_1 < n_2 \).}

Introduce the following two relations:

\[
z_1 \leq_x z_2 : (\exists y_1, y_2) (D(x, y_1, z_1) \land D(x, y_2, z_2) \land y_1 \mid y_2);
\]

\[
z_1 \approx_x z_2 : z_1 \leq_x z_2 \land z_2 \leq_x z_1.
\]

Let us select an arbitrary \( x \in \exp \mathcal{A} \) satisfying the formula \( L(x) \). Then, we denote by \( C_x \) the following set:

\[
C_x = \{ z \in \exp \mathcal{A} : C(x, z) \}.
\]

Proposition 10. Let \( g, a \in \mathcal{A} \), the element \( g \) be invertible, the element \( a \) be of infinite order, and \( x = g \{ e, a \} \). Then, the relation \( \leq_x \) is reflexive and transitive on the set \( C_x \).

Proof. If \( z \in C_x \), then the formula \( D(x, y, z) \) is true for some \( y \) by definition, so \( z \leq_z z \) is true for \( y_1 = y_2 = y \).

To prove the transitivity of the relation \( \leq_x \) let us suppose \( z_1 \leq_x z_2 \) and \( z_2 \leq_x z_3 \) for elements \( z_1, z_2, \) and \( z_3 \) of \( C_x \). Then, we have the truth of the next four formulas: \( D(x, y_1, z_1), D(x, y_2, z_2), D(x, y_3, z_3)\), and \( D(x, y_3, z_3) \) for some \( y_1, y_2, y_3, y_3 \) such that \( y_1 \mid y_2 \) and \( y_2 \mid y_3 \). By Claim (ii) of Proposition 9, we conclude \( y_2 = x^n w \) and \( y'_2 = x^n w' \) for some invertible elements \( w \) and \( w' \), it follows \( y_2 \mid y'_2 \). Thus, we obtain \( y_1 \mid y_2, y_2 \mid y'_2 \), and \( y'_2 \mid y_3 \). Therefore, we get \( y_1 \mid y_3 \) that means \( z_1 \leq_x z_3 \).
Corollary 11. The relation $\approx_x$ is an equivalence on the set $C_x$, the factor order on $C_x$ by $\approx_x$ is isomorphic to natural numbers.

Let us denote by $\bar{n}$ the equivalence class consisting of elements $z$ such that $D(x, x^n w, z)$ is true for invertible elements $w$. By Claim (ii) of Proposition 9, it follows that such $n$ is unique for each $z \in C_x$.

Now we can define formulas, which interpret arithmetic relations:

$$
L^*(x) \equiv (\forall z)(C(x, z) \rightarrow L(z)); \\
A_x(z_1, z_2, z_3) \equiv (\exists y_1, y_2) (D(x, y_1, z_1) \land D(x, y_2, z_2) \land D(x, y_1 y_2, z_3)); \\
DV_x(z_1, z_2) \equiv (\exists z_1', z_2') (z_1' \approx_x z_1 \land z_2' \approx_x z_2 \land C(z_1', z_2')).
$$

Let us prove their main properties.

Proposition 12. Let $g,a \in A$, the element $g$ be invertible, the element $a$ be of infinite order, and $x = g\{e,a\}$. Let $L^*(x)$ be true in the monoid $\exp A$. Then, for any $z_1, z_2, z_3 \in \exp A$ such that $z_i \in \bar{n}_i$ for $i = 1, 2, 3$ we have

(i) $A_x(z_1, z_2, z_3)$ is true if and only if $n_1 + n_2 = n_3$;
(ii) $DV_x(z_1, z_2)$ is true if and only if $n_1 | n_2$.

Proof. To prove Claim (i) let $A_x(z_1, z_2, z_3)$ be true. Thus, the formulas $D(x, x^{n_1}w_1, z_1)$, $D(x, x^{n_2}w_2, z_2)$ and $D(x, x^{n_3}w_3, z_3)$ are true for some invertible $w_1$ and $w_2$. But $z_3 \in \bar{n}_3$ means the truth of $D(x, x^{n_3}z_3, z_3)$. Hence, the formulas $D(x, x^{n_1+n_2}w_1w_2, z_3)$ and $D(x, x^{n_3}w_3, z_3)$ are true for invertible $(w_1w_2)$ and $w_3$. By Claim (ii) of Proposition 9, we get $n_1 + n_2 = n_3$.

On the other hand, let us suppose $n_1 + n_2 = n_3$. Then, the formulas $D(x, x^{n_1}w_1, z_1)$, $D(x, x^{n_2}w_2, z_2)$, and $D(x, x^{n_1+n_2}w_1w_2, z_3)$ are true for some invertible elements $w_1$, $w_2$ and $w_3$. By Claim (i) of Proposition 5, the value of $P(x, x^m w)$ doesn’t depend on invertible $w$. Thus, the truth of $D(x, x^{n_1+n_2}w_1w_2, z_3)$ follows the truth $D(x, x^{n_1+n_2}w_1w_2, z_3)$ and, consequently, of $A_x(z_1, z_2, z_3)$.

Now consider Claim (ii). Let $z_1$ and $z_2$ satisfy the formula $DV_x(z_1, z_2)$. It means $D(x, x^{n_1}w_1, z_1')$ and $D(x, x^{n_2}w_2, z_2')$ for some invertible elements $w_1$ and $w_2$. Since the truth of the equality $z_1 \approx_x z_1'$, we have $D(x, x^{n_1}w_1, z_1')$ and $C(x, z_1')$, so $L^*(x)$ follows $L(z_1')$. Let us apply Claim (ii) of Proposition 9 to $L(z_1')$ and $C(z_1', z_2')$, we have $D(z_1', z_1'mw, z_2')$ for some natural number $m$ and invertible $w$. Then,

$$
x^{n_2+4n_1m}w^2w_1^{4m}w_2 = x^{n_2}((x^{n_1}w_1)^2)^{2m}w_2^2w_2 = x^{n_2}(x^{n_1}w_1z_1')^{2m}w_2^2w_2 = \\
= x^{n_2}x^{2n_1m}z_1'^{2m}w_2^2w_2 = x^{n_2}x^{2n_1m}(z_1'^{2m}w_2)^2w_2^2w_2 = x^{n_2}x^{2n_1m}z_1'^{2m}w_2w_2 = \\
= (x^{n_1}w_1z_1')^m(x^{n_2}w_2z_2')w_1^{4m}w_2 = (x^{n_1}w_1)^2m(x^{n_2}w_2^2w_2)^2w_2 = x^{3n_1m+2n_2}w_1^{4m}w_2.
$$

The elements $w_1$, $w_2$, and $w$ are invertible, so the sets $w^2w_1^{4m}w_2$ and $w_1^{4m}w_2^2$ consist of one element. Then, for cardinalities we get $n_2 + 4n_1m + 1 = 3n_1m + 2n_2 + 1$ that is followed by Claim (iv) of Proposition 5. Therefore, we have $n_2 = n_1m$ and $n_1 | n_2$.

Now let us suppose $n_1 | n_2$, it follows the equality $n_2 = n_1m$ for some natural number $m$. Assume $z_1' = g^{n_1}\{e,a^n\}$ and $z_2' = g^{mn_1}\{e,a^{mn_1}\}$. Then, we have $D(x, x^{n_1}z_1')$ and $D(x, x^{n_2}z_2')$, see Claim (i) of Proposition 9. Thus, the equalities $z_1' \approx_x z_1$ and $z_2' \approx_x z_2$ hold. Since $D(x, x^{n_1}z_1')$ is true, we obtain $C(x, z_1')$, hence, we have $L(z_1')$ due to $L^*(x)$. By Claim (i) of Proposition 9, we get the truth of $D(z_1'(z_1')^m, z_2')$ and $C(z_1', z_2')$. Therefore, the formula $DV_x(z_1, z_2)$ is true also.

□
Therefore, the interpretation of the entire formula $\Phi$ is $(\exists\text{the } A)$ higher degree of undecidability (see [14]). In this case the theory of $\exp \mathfrak{A}$ is algorithmically equivalent to elementary arithmetic.

Let $a \in \mathfrak{A}$ be an element of infinite order and $x = \{e, a\}$. Then, $L^* (x)$ is true in the monoid $\exp \mathfrak{A}$.

Proof. It follows by Proposition 8 that $L(x)$ is true for such $x$. By Corollary 7, we get that the formula $P(x, y)$ is true for $y = x^n w$ exactly, where $n$ is a natural number and $w$ is an invertible element. Let us select an arbitrary $z \in \exp \mathfrak{A}$ such that $C(x, z)$ is true. From $C(x, z)$ we obtain $D(x, y, z)$, so $y = x^n w$ for some $n$ and $w$, $zx^n w = x^{2n} w^2$, and $(zw^{-1}) x^n = x^{2n}$. As $e \in x^n$, so by Proposition 2, we have

$$zw^{-1} \subseteq x^{2n} = \{e = a^0, a = a^1, a^2, \ldots, a^{2n}\}.$$  

The powers $a^k$ are pairwise different because the element $a$ has infinite order. Hence, we can conclude that the set $zw^{-1}$ must contain $a^n$ and can’t contain powers greater than $a^n$. On the other hand, $a^k \neq e$ for all $k > 0$, hence, $zw^{-1}$ must contain $e$. Since $D(x, y, z)$, we get $R_2(z)$ and $z = \{e, a^n\}$. Evidently, the element $a^n$ must have infinite order, therefore, $L(z)$ is followed by Proposition 8.

Now we can prove the main result of the paper.

Let a commutative cancellative monoid $\mathfrak{A}$ contain an element of infinite order. Then, elementary arithmetic can be interpreted in the theory of the monoid $\exp \mathfrak{A}$.

Proof. Remember, that the following two relations are enough to interpret elementary arithmetic: addition and divisibility (see [8, 14]). Let us select an arbitrary element $t$ of the monoid $\exp \mathfrak{A}$ such that $L^* (t)$ is true. According to Proposition 13 such $t$ exists. Then, the domain of our interpretation is the set of equivalence classes for the relation $\approx_t$.

Consider any formula $\Phi$. For every subformula $\phi$ of the formula $\Phi$ we construct its interpretation $\phi'$ as following:

- if $\phi$ is $x + y = z$, then $\phi'$ is $A_t(x, y, z)$;
- if $\phi$ is $x | y$, then $\phi'$ is $DV_t(x, y)$;
- if $\phi$ is $x = y$, then $\phi'$ is $x \approx_t y$;
- if $\phi$ is $\psi \circ \theta$, then $\phi'$ is $\psi' \circ \theta'$, where $\circ \in \{\land, \lor, \rightarrow\}$;
- if $\phi$ is $\neg \psi$, then $\phi'$ is $\neg \psi'$;
- if $\phi$ is $(\forall x) \psi$, then $\phi'$ is $\neg (\exists x) \psi$, then $\phi'$ is $(\exists x)(C(t, x) \land \psi')$.

Therefore, the interpretation of the entire formula $\Phi$ is $(\exists t)(L^* (t) \land \Phi')$.

The soundness of this interpretation is implied by Corollary 11, Propositions 12 and 13, and the $L^*$ definition.

Corollary 15. Let a commutative cancellative monoid $\mathfrak{A}$ contains an element of infinite order. Then, the elementary theory of the monoid $\exp \mathfrak{A}$ is algorithmically undecidable at least as elementary arithmetic.

Note that the last result distinguishes the claim of Corollary 1 in [11]. In [11] the free cyclic monoid $\mathfrak{A}$ is considered, and it was proved that the theory of $\exp \mathfrak{A}$ is algorithmically equivalent to elementary arithmetic.

In the current article we investigate more general monoids those theories themselves can have higher degree of undecidability (see [14]). In this case the theory of $\exp \mathfrak{A}$ has also higher degree
of undecidability. The last sentence holds because the theory of $\mathfrak{A}$ is interpretable in the monoid $\exp \mathfrak{A}$ using the predicate $R_1$.

At last, remember that every Abelian group is a commutative cancellative monoid. If an Abelian group is not a torsion group, then it has an element of infinite order. So the previously proved claims are applicable to these groups.

**Corollary 16.** Let $\mathfrak{A}$ be an Abelian group but not a torsion group. Then, elementary arithmetic can be interpreted in the theory of the monoid $\exp \mathfrak{A}$. Hence, this theory is undecidable.

In particular, the theory of $\exp \mathfrak{A}$ is undecidable when $\mathfrak{A}$ is the additive or multiplicative group of (integer, rational, real, complex) numbers.

5. Conclusion

We have proved that an algebra of finite subsets is undecidable for the wide class of monoids. The question appears whether it is possible to generalize this result to other monoids. Are used restrictions important or they can be eliminated?

- Are the theory of the algebra $\exp \mathfrak{A}$ is undecidable when all elements of $\mathfrak{A}$ have finite orders?
  
  In particular, is such claim holds for infinite Abelian torsion groups? An example of such group is the multiplicative group of complex roots of unity.

- Is such claim true for monoids without cancellation?

- Is such claim true for non-commutative monoids?

Acknowledgments

This work is financially supported by Russian Foundation of Basic Research (RFFI), project 20-01-00435.

References

[1] Hopcroft J E, Motwani R and Ullman J D 2013 *Introduction to Automata Theory, Languages, and Computation: Pearson New International Edition* (Pearson Education Limited) ISBN 9781292056166

[2] Gillibert P 2014 *International Journal of Algebra and Computation* 24(1) 1–9

[3] Gray R D 2019 *Inventiones mathematicae* 219(3) 987–1008

[4] D’Angeli D, Rodaro E and Wächter J P 2020 *Semigroup Forum* 101(1) 51–76

[5] Codd E F 1970 *Communications of ACM* 13(6) 377–387

[6] Kanellakis P C, Kuper G M and Revesz P Z 1995 *J. Comput. Syst. Sci.* 51(1) 26–52

[7] Brough T and Cain A J 2015 *Semigroup Forum* 90(3) 763–774

[8] Boolos G S, Burgess J P and Jeffrey R C 2007 *Computability and Logic* (Cambridge University Press) ISBN 9780521877527

[9] Dudakov S M 2019 *Vestnik TvGU. Seriya Prikladnaya matematika [Herald of Tver State University. Series: Applied mathematics] 4* 108–116 (in Russian)

[10] Dudakov S M and Karlov B N 2020 *Theory of Computing Systems* URL https://doi.org/10.1007/s00224-020-09995-4

[11] Dudakov S M 2020 *Lobachevskii Journal of Mathematics* 40(2) 168–175

[12] Place T and Zeitoun M 2016 *Logical Methods in Computer Science* 12(1) URL https://doi.org/10.2168/LMCS-12(1:5)2016

[13] Grillet P A 2001 *Commutative Semigroups* Advances in Mathematics - Kluwer Academic Publishers (Springer US) ISBN 9780792370673

[14] Rogers H 1987 *Theory of Recursive Functions and Effective Computability* (Cambridge, MA, USA: MIT Press) ISBN 0262680521