Сибирский математический журнал
Май—июнь, 2010. Том 51, № 3

УДК 510.53:512.562

ОПРЕДЕЛИМОСТЬ В СТРУКТУРЕ СЛОВ С ОТНОШЕНИЕМ ВКЛЮЧЕНИЯ

О. В. Кудинов,
В. Л. Селиванов, Л. В. Ярцева

Аннотация. Разработана теория определимости (первого порядка) в структуре слов с отношением включения, аналогичная развитым ранее теориям для h-квазипорядка на конечных k-размеченных лесах и для структуры слов с инфиксным порядком. В частности, показано, что любой элемент определим (при условии, что слова длины 1 и 2 взяты как параметры) и что теория первого порядка этой структуры атомна и вычислимо изоморфна арифметике первого порядка. Охарактеризована группа автоморфизмов этой структуры и показано, что любой арифметический предикат, инвариантный относительно автоморфизмов, определим в этой структуре.

Ключевые слова: подслово, инфиксный порядок, определимость, автоморфизм, наименьшая неподвижная точка, теория первого порядка, биинтерпретируемость.

§ 1. Введение

Изучение определимости в естественных структурах является одним из центральных вопросов логики и теории вычислимости. Для теории вычислений представляет интерес изучение естественных структур на словах и деревьях. В частности, много глубоких фактов об определимости и (не)разрешимости получено для конечно определенных полугрупп и групп. Изучение естественных предпорядков на словах и деревьях также является традиционной темой (см., например, работы [1, 2] и библиографию в них), в рамках которой получены интересные результаты об определимости и (не)разрешимости.

В этой работе детально изучается теория определимости в структуре $(A^*; \preceq)$, где A^* — множество слов в конечном алфавите A, содержащем не менее двух символов, а $\preceq$ — частичный порядок на A^* (называемый *отношением включения*), определяемый следующим образом: $u \preceq v$, если u является «подсловом» v, т. е. u получается из v удалением некоторого числа символов. Без потери общности можем считать что $A = A_k = \{0, \dots, k-1\}$ для некоторого $k \geq 2$. Как хорошо известно, $u \preceq v$ равносильно тому, что существует вложение $f : u \to v$, т. е. возрастающая функция $f : A_{|u|} \to A_{|v|}$ такая, что $u(i) = v(f(i))$ для всех $i < |u|$, где $u(i)$ — i-й символ, а $|u|$ — длина слова u. Структура $(A^*; \preceq)$ представляет интерес для ряда областей, включая теорию «хороших» частичных порядков [3, 4], комбинаторику слов [1] и теорию автоматов [5, 6].

Работа первого и второго авторов выполнена при финансовой поддержке ННИО–РФФИ (436 RUS 113/1002/01, 09–01–91334), кроме того, работа первого автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 08–01–00336а, 09–01–12140_ОФИ_М).

Эта работа существенно опирается на статьи [7, 8], в которых аналогичная теория определимости развита для h-предпорядка на конечных размеченных лесах и для структуры $(A^*; \leq)$ слов с инфиксным частичным порядком: ($u \leq v$, если $v = xuy$ для некоторых $x, y \in A_k^*$). Мы используем некоторые понятия и результаты из этих работ.

Используем также некоторые стандартные обозначения, например, ε обозначает пустое слово, $xu = x \cdot u$ — конкатенацию слов x и u, $|u|_a$ — число вхождений символа $a \in A$ в слово u, $A^{[m,n]}$ — множество $\{u \in A^* \mid m \leq |u| \leq n\}$. Для $i \leq j \leq |u|$ положим $u[i, j) = u(i) \cdots u(j-1)$; слово $u[i, j]$ определяется аналогично. Мы отождествляем символы с соответствующими односимвольными словами.

Для данной структуры $\mathbf{A}$ сигнатуры σ предикат на A называется *определимым*, если он определяется формулой первого порядка сигнатуры σ (на самом деле это определение не вполне точно; для получения хорошо известного точного определения необходимо фиксировать также подходящий список переменных, как в определении оператора Γ в следующем параграфе). Функция на $\mathbf{A}$ *определима*, если определим ее график. Элемент определим, если соответствующее одноэлементное множество определимо. Структура определима в $\mathbf{A}$, если определимы ее универсум и все предикаты ее сигнатуры.

В § 2 напоминаются необходимые понятия и факты из [7]. В § 3 установим полезные частные результаты об определимости в структуре $(A^*; \preceq)$. В частности, покажем, что любой элемент определим в $A^{[1,2]}$-обогащении $(A^*; \preceq)$ (т. е. в обогащении, полученном добавлением к сигнатуре $\{\preceq\}$ констант, обозначающих все слова длины 1 и 2) и что инфиксный порядок определим в $A^{[1,2]}$-обогащении структуры $(A^*; \preceq)$. В § 4 охарактеризуем группу автоморфизмов структуры $(A^*; \preceq)$. В § 5 докажем основные результаты статьи, в частности, что любой арифметический предикат на A^*, который инвариантен относительно автоморфизмов структуры $(A^*; \preceq)$, определим в $(A^*; \preceq)$.

В теории вычислимости активно обсуждаются варианты так называемой гипотезы биинтерпретируемости, утверждающей, что некоторые структуры степеней неразрешимости биинтерпретируемы (с параметрами) со структурой $(\omega; +, \cdot)$ (см., например, работу [9] и приведенную в ней библиографию). Эта гипотеза (которая, насколько нам известно, до сих пор открыта для наиболее интересных структур степеней неразрешимости) рассматривается как, в определенном смысле, лучший возможный результат об определимости для структур степеней.

Данная работа и статьи [7, 8] показывают, что некоторые естественные структуры на словах и лесах биинтерпретируемы (даже без параметров!) со структурой $(\omega; +, \cdot)$. Мы полагаем, что методы этих работ могут оказаться полезными для получения похожих результатов и для других структур, включая структуры, изучаемые в [2].

§ 2. Вспомогательные результаты

В этом параграфе приведем необходимые сведения из работы [7], в которой развит метод изучения определимости в структурах определенного вида. Наряду с определимостью первого порядка рассмотрим определимость формулами специального вида, связанными с теорией допустимых множеств и индуктивной определимости. Напомним несколько важных определений из [10–12].

Пусть σ — конечная сигнатура, содержащая бинарный предикатный символ $\leq$ и, возможно, некоторые другие предикатные и константные символы. RQ-*формулы* сигнатуры σ строятся из атомарных формул в соответствии с обычными правилами логики первого порядка для пропозициональных связок $\wedge, \vee, \neg, \to$ и (неограниченных) кванторов $\forall, \exists$, а также следующих правил для ограниченных кванторов: если φ — RQ-формула и x, y — переменные, то выражения $\forall x \leq y\varphi$ и $\exists x \leq y\varphi$ суть RQ-формулы. Как и в случае с обычными формулами первого порядка, любая RQ-формула эквивалентна *специальной* RQ-формуле, т. е. формуле без импликации, в которой отрицания относятся только к атомным подформулам.

Δ_0-*формулы* сигнатуры σ строятся индуктивно в соответствии со следующими правилами: любая атомарная формула сигнатуры σ есть Δ_0-формула; если φ и ψ — Δ_0-формулы, то $\neg\varphi$, $(\varphi \wedge \psi)$, $(\varphi \vee \psi)$ и $(\varphi \to \psi)$ суть Δ_0-формулы; если x, y — переменные и φ — Δ_0-формула, то $\forall x \leq y\varphi$ и $\exists x \leq y\varphi$ суть Δ_0-формулы.

Σ-*формулы* сигнатуры σ строятся индуктивно в соответствии со следующими правилами: любая Δ_0-формула является Σ-формулой; если φ и ψ — Σ-формулы, то $(\varphi \wedge \psi)$ и $(\varphi \vee \psi)$ суть Σ-формулы; если x, y — переменные и φ — Σ-формула, то $\forall x \leq y\varphi$, $\exists x \leq y\varphi$ и $\exists x\varphi$ суть Σ-формулы.

Предикат на σ-структуре $\mathbf{A}$ называется Δ_0-*определимым* (соответственно Σ-*определимым*), если он определим Δ_0-формулой (соответственно Σ-формулой). Предикат на A называется Δ-*определимым*, если и предикат, и его отрицание Σ-определимы.

Пусть P — n-арный предикатный символ, не принадлежащий σ, φ — RQ-формула сигнатуры $\sigma \cup \{P\}$ и $\bar{x} = x_1, \ldots, x_n$ — список переменных, содержащий все свободные переменные формулы φ. Говорят, что P *входит в* φ *позитивно*, если φ — специальная формула, не имеющая подформул вида $\neg P(y_1, \ldots, y_n)$.

Для любого n-арного предиката Q на σ-структуре $\mathbf{A}$ обозначим через $(\mathbf{A}, Q)$ обогащение структуры $\mathbf{A}$ до структуры сигнатуры $\sigma \cup \{P\}$, в которой P интерпретируется как Q. Тогда можно определить оператор $\Gamma = \Gamma_{\varphi,\bar{x}}$ на множестве n-арных предикатах на A, который сопоставляет произвольному предикату Q предикат

$$\Gamma_{\varphi,\bar{x}}(Q) = \{(a_1, \ldots, a_n) \mid (\mathbf{A}, Q) \models \varphi(a_1, \ldots, a_n)\}.$$

σ-Структура $\mathbf{A}$ называется *ограниченной*, если $\leq$ — транзитивное направленное отношение (направленность означает, что для любых $x, y \in A$ существует $z \in A$ такое, что $x, y \leq z$) и для любой Δ_0-формулы φ из $\mathbf{A} \models \forall x \leq t\exists y\varphi$ следует $\mathbf{A} \models \exists v\forall x \leq t\exists y \leq v\varphi$. Легко видеть [10, 12], что если P — n-арный предикатный символ, входящий позитивно в Σ-формулу φ со свободными переменными из $\bar{x}$, то оператор Γ монотонен в любой σ-структуре. По теореме Тарского о неподвижной точке оператор Γ имеет наименьшую неподвижную точку. Обозначим ее через $LFP(\Gamma)$. В общем случае определенный таким способом предикат $LFP(\Gamma)$ может быть сложным (в частности, не определимым формулой первого порядка). Но для некоторых структур $\mathbf{A}$ наименьшая неподвижная точка любой Σ-формулы φ оказывается Σ-предикатом (в этом случае говорят, что $\mathbf{A}$ обладает *свойством Ганди*). Сформулируем соответствующее достаточное условие из [7].

Будем говорить, что σ-структура $\mathbf{A}$ *допускает* Δ-*кодирование конечных множеств*, если существует бинарный Δ-предикат $E(x, y)$ на $\mathbf{A}$ такой, что из $E(x, y)$ следует $x \leq y$ для всех $x, y \in A$, и для любых $n < \omega$ и $x_1, \ldots, x_n \in A$

найдется $y \in A$ такой, что

$$\mathbf{A} \models \forall x(E(x, y) \leftrightarrow x = x_1 \vee \cdots \vee x = x_n).$$

Назовем σ-структуру $\mathbf{A}$ *локально конечной*, если множество $\{x \mid x \leq y\}$ конечно для любого $y \in A$. Следующий результат полезен для понимания определимости в некоторых структурах.

Теорема 2.1 [7]. *Пусть $\mathbf{A}$ — ограниченная локально конечная σ-структура, допускающая Δ-кодирование конечных множеств и такая, что структура $(\omega; \leq)$ Δ-определима в $\mathbf{A}$. Тогда $\mathbf{A}$ имеет свойство Ганди.*

Напомним, что структура $\mathbf{A}$ с нумерацией α (т. е. α — сюръекция из ω на A) называется *арифметической*, если предикат равенства и все сигнатурные предикаты являются арифметическими по модулю α. Очевидно, любой определимый предикат на арифметической структуре $(\mathbf{A}; \alpha)$ является арифметическим (по модулю α) и инвариантным относительно автоморфизмов $\mathbf{A}$; будем говорить, что нумерованная структура $(\mathbf{A}; \alpha)$ имеет *свойство максимальной определимости*, если верно и обратное, т. е. любой арифметический предикат, инвариантный относительно автоморфизмов $\mathbf{A}$, определим в $\mathbf{A}$.

Пусть опять $\mathbf{A}$ — счетная σ-структура и α — нумерация множества A. Говорят, что *элементы* $(\mathbf{A}; \alpha)$ *равномерно* Σ-*определимы*, если существует арифметическая последовательность унарных Σ-формул $\{\psi_n(v_0)\}$ такая, что ψ_n определяет элемент $\alpha(n)$ в $\mathbf{A}$ для любого $n < \omega$.

Напомним (ср. [9, 13]), что структура $\mathbf{B}$ конечной сигнатуры τ *биинтерпретируема* со структурой $\mathbf{C}$ конечной сигнатуры ρ, если $\mathbf{B}$ определима в $\mathbf{C}$ (в частности, существует биекция $f : B \to B_1$ на определимое множество $B_1 \subseteq C^m$ для некоторого $m \geq 1$, индуцирующая изоморфизм $\mathbf{B}$ на τ-структуру с универсумом $\mathbf{B}_1$, определимую в $\mathbf{C}$), $\mathbf{C}$ определима в $\mathbf{B}$ (в частности, существует подобная биекция $g : C \to C_1$ на определимое множество $C_1 \subseteq B^n$ для некоторого $n \geq 1$), функция $g^m \circ f : B \to B^{nm}$ определима в $\mathbf{B}$ и функция $f^n \circ g : C \to C^{mn}$ определима в $\mathbf{C}$.

Теорема 2.2 [7]. *Пусть $(\mathbf{A}; \alpha)$ — арифметическая σ-структура с равномерно Σ-определимыми элементами такая, что $\mathbf{A}$ ограниченна, локально конечна, допускает Δ-кодирование конечных множеств, и структура $(\omega; \leq)$ Δ-определима в $\mathbf{A}$. Тогда $\mathbf{A}$ имеет свойство максимальной определимости и биинтерпретируема с $(\omega; +, \cdot)$.*

§ 3. Несколько результатов об определимости

В этом параграфе установим несколько фактов об определимости в $A^{[1,2]}$-обогащении структуры $(A^*; \preceq)$.

Для $x, y \in A^*$ пусть $S(x, y)$ означает, что y непосредственно следует за x по отношению $\preceq$. Поскольку $S(x, y)$ эквивалентно свойству $x \prec y \wedge \neg\exists z \preceq y(x \prec z \prec y)$, S является Δ_0-предикатом в $(A^*; \preceq)$.

Для любого $a \in A^*$ множества a^* и a^+ являются Δ_0-определимыми в $A^{[1]}$-обогащении $(A^*; \preceq)$ (используем обозначения в стиле регулярных выражений теории автоматов). Например, $x \in a^+$ тогда и только тогда, когда $a \preceq x$ и $\neg \bigvee\{b \preceq x \mid b \in A, b \neq a\}$.

Для различных символов $a, b \in A$ множества a^*b^*, a^*b^+, a^+b^* и a^+b^+ являются Δ_0-определимыми в $A^{[1,2]}$-обогащении $(A^*; \preceq)$. Например, $x \in a^*b^+$ тогда и только тогда, когда $b \preceq x$, $ba \not\preceq x$ и $\neg \bigvee\{c \preceq x \mid c \in A \setminus \{a, b\}\}$.

Для всех $a \in A$ и $u, v \in A^*$ пусть $P_a(u,v)$ означает, что $a \preceq v$ и u получается из v удалением в точности одного вхождения символа a в слово v. Пусть $p_a(u) = ua$ и $p^a(u) = au$, и пусть $Q_a(u,v) \leftrightarrow v \in ua^*$, $Q^a(u,v) \leftrightarrow v \in a^*u$.

Лемма 3.1. *Для любого $a \in A^*$ предикаты P_a, Q_a, Q^a и функции p_a, p^a являются Δ_0-определимыми в $A^{[1,2]}$-обогащении структуры $(A^*; \preceq)$.*

Доказательство. Поскольку $P_a(u,v)$ эквивалентно

$$S(u,v) \wedge \exists x \preceq u \exists y \preceq v (y \in a^+ \wedge y \not\preceq u \wedge S(x,y)),$$

предикат P_a Δ_0-определим. В случае функции p_a достаточно проверить, что

$$v = ua \leftrightarrow P_a(u,v) \wedge \bigwedge_{b \in A \setminus \{a\}} \forall x \preceq v (x \in a^* b^+ \to x \preceq u).$$

Слева направо это очевидно. Обратно, пусть верно правое условие. Если $u \in a^*$, то ясно, что $v = ua$. Если $u \notin a^*$, то $v = v_1 b^m a^n$ для однозначно определяемых $b \in A \setminus \{a\}, m \geq 1, n \geq 0$ и $v_1 \notin A^* b$. Пусть $x = a^k b^m$, где $k = |v_1|_a$. Тогда $x \preceq v$, поэтому $x \preceq u$. Поскольку $P_a(u,v)$, имеем $v = ua$.

Для случая предиката Q_a достаточно проверить, что

$$v \in ua^* \leftrightarrow u \preceq v \wedge \bigwedge_{b \in A \setminus \{a\}} \forall x \preceq v (p_b(x) \preceq v \to p_b(x) \preceq u).$$

Слева направо это очевидно. Обратно, пусть верно правое условие. В случае $v \in a^*$ ясно, что $v \in ua^*$. В противном случае $v = xba^n$ для однозначно определяемых $b \in A \setminus \{a\}, n \geq 0$ и $x \in A^*$. Поскольку $xb = p_b(x) \preceq v$, имеем $xb \preceq u$. Так как $u \preceq v$, то u получается из v удалением некоторых символов. Ввиду существования только одного вложения xb в v удаленные символы не могут быть из xb. Следовательно, u представляется в виде xba^m для некоторого $m \leq n$, поэтому $v \in ua^*$.

Для оставшихся случаев p^a и Q^a доказательства аналогичны случаям p_a и Q_a соответственно. $\square$

Следствие 3.2. *Элементы структуры A^* равномерно Σ-определимы в $A^{[1,2]}$-обогащении структуры $(A^*; \preceq)$.*

Доказательство. Индукцией по длине слова $w \in A^*$ построим Σ-формулу $\phi_w(x)$ со свободной переменной x, которая определяет w в $A^{[1,2]}$-обогащении $(A^*; \preceq)$. Для $w = \varepsilon$ в качестве ϕ_ε можем взять формулу $\neg \exists y \preceq x (y \prec x)$.

Для $|w| \geq 1$ представим w в виде va, $a \in A$, и возьмем в качестве ϕ_w Σ-формулу $\exists y (\phi_v(y) \wedge \psi(y,x))$, где ϕ_v — Σ-формула, определяющая v (которая существует по индукции), а ψ — Δ_0-формула, определяющая p_a (которая существует по лемме 3.1).

Пусть α — естественная нумерация множества $A^* = A^*_k$, полученная упорядочиванием слов в A^* сначала по длине, затем лексикографически (т. е. $\alpha(0) = \varepsilon$, $\alpha(1) = 0, \ldots, \alpha(k) = k-1$, $\alpha(k+1) = 00$, $\alpha(k+2) = 01, \ldots$). Записывая (рекурсивно) явные Σ-определения элементов в построенное выше доказательство, получим вычислимую (следовательно, арифметическую) последовательность $\{\theta_n(x)\}$ Σ-формул такую, что θ_n определяет $\alpha(n)$ для любого $n \geq 0$. $\square$

Для любых $u, v \in A^*$ пусть $u \leq_p v$ (соответственно $u \leq_s v$) означает, что u является префиксом (соответственно суффиксом) v, т. е. $v = ux$ (соответственно $v = xu$) для некоторого $x \in A^*$.

Лемма 3.3. *Отношения $\leq_p$, $\leq_s$, $\leq$ являются Δ_0-определимыми в $A^{[1,2]}$-обогащении структуры $(A^*;\preceq)$.*

Доказательство. Для отношения $\leq_p$ по лемме 3.1 достаточно проверить, что

$$u \leq_p v \leftrightarrow u \preceq v \wedge \bigwedge_{a\in A} \exists y \preceq v(Q_a(u,y) \wedge \neg\exists z \preceq vP_a(y,z)).$$

Пусть $u \leq_p v$, тогда $v = ux$ для некоторого $x \in A^*$, в частности, $u \preceq v$. Для данного $a \in A$ пусть $y = ua^n$, где $n = |x|_a$. Тогда $y \in ua^*$ и $\neg\exists z \preceq vP_a(y,z)$.

Обратно, пусть правое условие верно, в частности, $u \preceq v$ и $|u| \leq |v|$. Рассуждая от противного, предположим, что $u \not\leq_p v$, и возьмем минимальное $i < |u|$ с условием $u(i) \neq v(i)$. Пусть $a = v(i)$, и пусть $y \preceq v$ таково, что $y \in ua^*$ и $\neg\exists z \preceq vP_a(y,z)$. Пусть f — вложение u в v, и пусть $z = v[0,i), y[i,|y|] = u[0,i)au[i,|y|)a^n$, где n удовлетворяет условию $y = ua^n$. Тогда $P_a(y,z)$ и $z \preceq v$, поскольку можно определить вложение $g : A_{|z|} \to A_{|v|}$ следующим образом: $g(j) = j$ для $j \leq i$ и $g(j) = f(j-1)$ для $i < j < |y|$; противоречие.

Для отношения $\leq_s$ доказательство аналогично доказательству для $\leq_p$.

Поскольку

$$u \leq v \leftrightarrow \exists w \preceq v(u \leq_p w \wedge w \leq_s v),$$

предикат $\leq$ Δ_0-определим. $\square$

Следствие 3.4. *$A^{[1,2]}$-обогащение структуры $(A^*;\preceq)$ допускает Δ-кодирование конечных множеств.*

Доказательство. По теореме 5 из [8] $A^{[1,2]}$-обогащение структуры $(A^*;\leq)$ допускает Δ-кодирование $E(x,y)$ конечных множеств, т. е. существуют Σ-формулы $\phi(x,y)$ и $\psi(x,y)$, которые определяют соответственно $E(x,y)$ и $\neg E(x,y)$ в $A^{[1,2]}$-обогащении $(A^*;\leq)$. По лемме 3.3 существует Σ-формула $\theta(u,v)$, определяющая отношение $u \leq v$ в $A^{[1,2]}$-обогащении $(A^*;\preceq)$. Заменяя любое вхождение $u \leq v$ в ϕ и ψ на $\theta(u,v)$ (и используя стандартную процедуру переименования связанных переменных в случае необходимости), получаем Σ-формулы $\phi'(x,y)$ и $\psi'(x,y)$, которые определяют $E(x,y)$ и $\neg E(x,y)$ в $A^{[1,2]}$-обогащении $(A^*;\preceq)$. $\square$

§ 4. Характеризация автоморфизмов

В этом параграфе охарактеризуем группу автоморфизмов $\mathrm{Aut}(A^*;\preceq)$ структуры $(A^*;\preceq)$. Начнем с очевидного следствия из утверждения 3.2.

Следствие 4.1. *Любой автоморфизм структуры $(A^*;\preceq)$, тождественный на $A^{[1,2]}$, является тождественным автоморфизмом.*

Обозначим через $\mathbf{S}_k$ симметрическую группу перестановок k элементов $\{0,\dots,k-1\}$, а через $\mathbf{A} \simeq \mathbf{B}$ — отношение изоморфизма между структурами $\mathbf{A}$ и $\mathbf{B}$. Поскольку для $k = 1$ имеем $(A_k^*;\preceq) \simeq (\omega;\leq)$, то $\mathrm{Aut}(A_k^*;\preceq)$ есть тривиальная одноэлементная группа. Для $k \geq 2$ наряду с тождественным автоморфизмом e группа $\mathrm{Aut}(A_k^*;\preceq)$ имеет также некоторые другие элементы, в частности, «обращающий» автоморфизм r, задаваемый соотношением $r(i_1\cdots i_n) = i_n\cdots i_1$ для всех $n \geq 0$ и $i_1,\dots,i_n < k$ (заметим, что $r \circ r = e$).

Лемма 4.2. *Пусть $k \geq 2$, и пусть f — автоморфизм структуры $(A_k^*;\preceq)$ такой, что $f(i) = i$ и $f(ij) = ji$ для всех $i,j < k$. Тогда $f = r$.*

Доказательство. Функция $f\circ r$ является автоморфизмом $(A_k^*;\preceq)$, тождественным на $A_k^{[1,2]}$. По следствию 4.1 $f\circ r = e$, следовательно, $f = f\circ r\circ r = r$. $\square$

Следующий результат и соответствующая теорема из [8] показывают, что группы автоморфизмов структур $(A_k^*;\preceq)$ и $(A_k^*;\leq)$ изоморфны (хотя сами структуры далеко не изоморфны). Схема приводимого ниже доказательства та же, что схема соответствующего доказательства в [8], но некоторые детали отличаются.

Теорема 4.3. *Для любого* $k \geq 2$ *будет* $\mathrm{Aut}(A_k^*;\preceq) \simeq \mathbf{S}_k \times \mathbf{S}_2$.

Доказательство. Ограничивающее отображение $f \mapsto f|_{A_k}$, как легко видеть, является групповым гомоморфизмом из $\mathrm{Aut}(A_k^*;\preceq)$ на $\mathbf{S}_k$. Проверим, что ядро K этого гомоморфизма совпадет с $\{e,r\}$. Очевидно, $e,r \in K$. Обратно, пусть $f \in K$, тогда $f(i)=i$ для всех $i<k$. Поскольку $\{01,10\}$ — множество минимальных элементов в $(\{u \in A_k^* \mid 0,1 \prec u\};\preceq)$, то $f(01) \in \{01,10\}$. Мы различаем два случая.

Случай 1. $f(01)=01$. Тогда $f(10)=10$. Докажем, что на самом деле $f(ij)=ij$ для всех $i,j<k$. При $i=j$ это очевидно, так что пусть $i \neq j$. Сначала предположим, что $0 \in \{i,j\}$, пусть $0=i$ (случай $0=j$ аналогичен). Как и выше, $f(0j) \in \{0j, j0\}$. Рассуждая от противного, предположим, что $f(0j)=j0$. Для слова $w=10j$ имеем $10, 0j \preceq w$, так что $10=f(10) \preceq f(w)$ и $j0=f(0j) \preceq f(w)$. Но $|f(w)|=3$ (потому что любой автоморфизм $(A_k^*;\preceq)$, очевидно, сохраняет длину слов), следовательно, $f(w) \in \{1j0, j10\}$. В случае $f(w)=1j0$ имеем $f(1j)=1j$ и $10, 0j, j1 \preceq f(j10)$; противоречие. Аналогичное противоречие получается в оставшемся случае $f(w)=j10$ (надо рассмотреть $f(1j0)$).

Случай $1 \in \{i,j\}$ аналогичен случаю $0 \in \{i,j\}$, так что остается рассмотреть случай $0,1 \notin \{i,j\}$. Поскольку $f(0i)=0i$ и $i \in \{i,j\}$, то $f(ij)=ij$ (заменой 1 на i в предыдущем абзаце). Мы показали, что f тождествен на $A_k^{[1,2]}$. По следствию 4.1 $f=e$.

Случай 2. $f(01)=10$. По аналогии со случаем 1 можно показать, что на самом деле $f(ij)=ji$ для всех $i,j<k$. По лемме 4.2 $f=r$. Это завершает доказательство равенства $K=\{e,r\}$.

Пусть $g \mapsto \tilde{g}$ — вложение $\mathbf{S}_k$ в $\mathrm{Aut}(A_k^*;\preceq)$, определяемое соотношением $\tilde{g}(i_1 \cdots i_n) = g(i_1) \cdots g(i_n)$ для всех $n \geq 0$ и $i_1, \ldots, i_n < k$ (заметим, что $\tilde{g}|_{A_k} = g$ для любого $g \in \mathbf{S}_k$). Тогда $\widetilde{\mathbf{S}}_k = \{\tilde{g} \mid g \in \mathbf{S}_k\}$ и K являются подгруппами группы $\mathrm{Aut}(A_k^*;\preceq)$, $\widetilde{\mathbf{S}}_k \cap K = \{e\}$ и r коммутирует с любым элементом $\widetilde{\mathbf{S}}_k$. Тогда каждый элемент группы $\mathrm{Aut}(A_k^*;\preceq)$ однозначно представим в виде $\tilde{g} \circ h$, где $g \in \mathbf{S}_k$ и $h \in K$. Поэтому $\mathrm{Aut}(A_k^*;\preceq) \simeq \widetilde{\mathbf{S}}_k \times K$. Это завершает доказательство, поскольку $\widetilde{\mathbf{S}}_k \simeq \mathbf{S}_k$ и $K \simeq \mathbf{S}_2$. $\square$

§ 5. Основные результаты

Теперь мы готовы установить центральный результат этой статьи.

Теорема 5.1. $A^{[1,2]}$*-обогащение структуры* $(A^*;\preceq)$ *обладает свойством Ганди и свойством максимальной определимости и биинтерпретируемо со структурой* $(\omega;+,\cdot)$.

Доказательство. Ясно, что структура $(A^*;\preceq)$ ограниченна и локально конечна. По следствию 3.2 элементы A^* равномерно Σ-определимы. Структура $(a^*;\preceq)$, $a \in A$, — Δ-определимая копия структуры $(\omega;\leq)$. По следствию 3.4 обогащение допускает Δ-кодирование конечных множеств. Таким образом, все условия теорем 2.1 и 2.2 выполнены. Заключения этих теорем дают желаемые свойства. □

Сформулируем немедленное следствие предыдущей теоремы.

Следствие 5.2. *Структура $(\omega;+,\cdot)$ определима в $A^{[1,2]}$-обогащении структуры $(A^*;\preceq)$. Поэтому теория первого порядка этого обогащения вычислимо изоморфна арифметике первого порядка $FO(\omega;+,\cdot)$.*

Завершим статью полной характеризацией определимых предикатов на структуре $(A^*;\preceq)$.

Теорема 5.3. *Для любого $k\geq 2$ структура $(A^*_k;\preceq)$ имеет свойство максимальной определимости.*

Доказательство. Пусть $S(x,y)$ — предикат из § 3. Пусть $\{v_a\}_{a\in A_k^{[1,2]}}$ — различные переменные, $\bar v$ — набор переменных

$$(v_0,\dots,v_{k-1},v_{00},\dots,v_{0(k-1)},\dots,v_{(k-1)0},\dots,v_{(k-1)(k-1)}),$$

и пусть $\rho=\rho(\bar v)$ — формула сигнатуры $\{\preceq\}$, равносильная конъюнкции следующих формул:

- $S(\varepsilon,v_i)$ для всех $i<k$,
- $\neg v_i=v_j$ для всех различных $i,j<k$,
- $S(v_i,v_{ij})\wedge S(v_j,v_{ij})$ для всех $i,j<k$,
- $\neg v_{ij}=v_{ji}$ для всех различных $i,j<k$,
- $\exists x(S(v_{ij},x)\wedge S(v_{jl},x)\wedge S(v_{il},x))$ для всех попарно различных $i,j,l<k$.

Проверим, что ρ определяет в структуре $(A^*_k;\preceq)$ орбиту $\mathrm{Orb}(\bar b)$ набора

$$\bar b=(0,\dots,k-1,00,\dots,0(k-1),\dots,(k-1)0,\dots,(k-1)(k-1))$$

(напомним, что $\mathrm{Orb}(\bar b)=\{f(\bar b)\mid f\in\mathrm{Aut}(A^*;\preceq)\}$, где $\bar b=(b_0,\dots,b_n)$ и $f(\bar b)=(f(b_0),\dots,f(b_n))$. В самом деле, поскольку $(A^*_k;\preceq)\models\rho(\bar b)$, то $(A^*_k;\preceq)\models\rho(f(\bar b))$ для любого $f\in\mathrm{Aut}(A^*;\preceq)$ и, следовательно, $(A^*_k;\preceq)\models\rho(\bar a)$ для любого $\bar a\in\mathrm{Orb}(\bar b)$.

Обратно, пусть $(A^*_k;\preceq)\models\rho(\bar v)$ для некоторых значений переменных $\bar v$ в множестве A^*_k; надо показать, что $\bar v\in\mathrm{Orb}(\bar b)$. Так как $S(\varepsilon,v_i)$ и $v_i\neq v_j$ для всех различных $i,j<k$, то $(v_0,\dots,v_{k-1})=(g(0),\dots,g(k-1))$ для некоторого $g\in\mathbf{S}_k$. Продолжим g до автоморфизма структуры $(A^*_k;\preceq)$ (также обозначаемого через g) соотношением $g(i_1\cdots i_n)=g(i_1)\cdots g(i_n)$, где $n\geq 0$ и $i_1,\dots,i_n<k$. Поскольку $S(v_i,v_{ij})\wedge S(v_j,v_{ij})$ для всех $i,j<k$ и $v_{ij}\neq v_{ji}$ для всех различных $i,j<k$, то $\{g(ij),g(ji)\}=\{v_{ij},v_{ji}\}$ для всех $i,j<k$, в частности, $v_{01}\in\{g(01),g(10)\}$. Повторяя доказательство теоремы 4.3 (случаи 1, 2) и используя условие $\exists x(S(v_{ij},x)\wedge S(v_{jl},x)\wedge S(v_{il},x))$ для всех попарно различных $i,j,l<k$, получим, что $\bar v=g(\bar b)$ в случае $v_{01}=g(01)$ и $\bar v=r(g(\bar b))$ в случае $v_{01}=g(10)$, где r — «обращающий» автоморфизм. В любом случае $\bar v\in\mathrm{Orb}(\bar b)$.

Пусть теперь $P(\bar x)$, $\bar x=(x_1,\dots,x_n)$, — n-арный арифметический предикат на A^*_k, инвариантный относительно автоморфизмов $(A^*_k;\preceq)$. Нужно показать, что P определим в $(A^*_k;\preceq)$. Без потери общности предполагаем, что переменные $x_1,\dots,x_n$ отличаются от переменных v_a, зафиксированных выше. По теореме 5.1 существует формула $\phi(\bar x)$ сигнатуры $\{\preceq,a\}_{a\in A_k^{[1,2]}}$, которая определяет P. Пусть ϕ_1 — формула сигнатуры $\{\preceq\}$, полученная из ϕ подстановкой переменной v_a вместо константного символа a для всех $a\in A_k^{[1,2]}$. Наконец, пусть θ —

формула, полученная из формулы $\rho \wedge \phi_1$ навешиванием кванторов существования по переменным v_a для всех $a \in A_k^{[1,2]}$. Тогда θ определяет P в $(A_k^*; \preceq)$. $\square$

Из последней теоремы и конечности любой орбиты $\mathrm{Orb}(\bar{b})$ немедленно получаем следующие теоретико-модельные свойства структуры $(A^*; \preceq)$.

Следствие 5.4. *Структура $(A^*; \preceq)$ атомна и минимальнаа, а ее элементарная теория $FO(A^*; \preceq)$ вычислимо изоморфна арифметике первого порядка $FO(\omega; +, \cdot)$.*

Поскольку значительное влияние на авторов оказала монография [12], мы выражаем глубокую признательность ее автору, Ю. Л. Ершову.

ЛИТЕРАТУРА

1. *Lothaire M.* Combinatorics on words. Cambridge mathematical library. Cambridge: Cambridge Univ. Press, 1997.
2. *Kuske D.* Theories of orders on the set of words // RAIRO Theor. Inform. Appl. 2006. V. 40. P. 53–74.
3. *Higman G.* Ordering by divisibility in abstract algebras // Proc. London Math. Soc. 1952. V. 3. P. 326–336.
4. *Kruskal J. B.* The theory of well-quasi-ordering: a frequently discovered concept // J. Comb. Theory, Ser. A. 1972. V. 13. P. 297–305.
5. *Glasser C., Schmitz H.* The Boolean structure of dot-depth one // J. Autom., Lang. Comb. 2001. N 6. P. 437–452.
6. *Selivanov V. L.* A logical approach to decidability of hierarchies of regular star-free languages // Proc. of STACS-2001. Berlin, Springer-Verl., 2001. P. 539–550. (Lect. Notes Comput. Sci.; V. 2010).
7. *Kudinov O. V., Selivanov V. L.* A Gandy theorem for abstract structures and applications to first-order definability // Proc. of CiE-2009. Berlin: Springer-Verl., 2009. P. 290–299. (Lect. Notes Comput. Sci.; V. 5635).
8. *Kudinov O. V., Selivanov V. L.* Definability in the infix order on words // Proc. of DLT-2009, Berlin: Springer-Verl., 2009. P. 454–465. (Lect. Notes Comput. Sci.; V. 5583).
9. *Nies A.* Definability in the c.e. degrees: questions and results // Computability theory and its applications. Univ. of Colorado, 2000. P. 207–213. (Contemp. Math.; V. 257).
10. *Moschovakis Y.* Elementary induction on abstract structures. Amsterdam: North-Holland, 1974.
11. *Barwise J.* Admissible sets and structures. Berlin: Springer-Verl., 1975.
12. *Ершов Ю. Л.* Определимость и вычислимость. Новосибирск: Научная книга, 1996.
13. *Hodges W.* Model theory. Cambridge: Cambridge Univ. Press, 1993.

Статья поступила 1 марта 2010 г.

Кудинов Олег Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
kud@math.nsc.ru

Селиванов Виктор Львович, Ярцева Людмила Викторовна
Институт систем информатики им. А. П. Ершова СО РАН,
пр. Академика Лаврентьева, 6, Новосибирск 630090
vseliv@iis.nsk.su