S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 13, стр. 1035–1039 (2016) УДК 510.5, 512, 510.6
DOI 10.17377/semi.2016.13.082 MSC 03C57, 03D15, 06E99

БЕЗАТОМНЫЕ БУЛЕВЫ АЛГЕБРЫ, ВЫЧИСЛИМЫЕ ЗА ПОЛИНОМИАЛЬНОЕ ВРЕМЯ

П.Е. АЛАЕВ

Abstract. We construct an example of atomless Boolean algebra $\mathfrak{B}$, computable in polynomial time, that has no primitive recursive function $f : B \to B$ such that $0 < f(a) < a$ for $a \neq 0$. In addition, we show that if two primitive recursive atomless Boolean algebras $\mathfrak{B}_1$ and $\mathfrak{B}_2$ have such functions, then there is an isomorphism $g : \mathfrak{B}_1 \to \mathfrak{B}_2$ such that g and g^{-1} are primitive recursive functions.

Keywords: computable structure, Boolean algebra, primitive recursive structure, polynomial time computability, primitive recursive isomorphism

1. Введение

Статья посвящена одному интересному вопросу, связанному с булевыми алгебрами, вычислимыми за полиномиальное время. Если $\mathfrak{B}_1, \mathfrak{B}_2$ — две вычислимые ненулевые безатомные булевы алгебры, то хорошо известно, что между ними есть вычислимый изоморфизм $g : \mathfrak{B}_1 \to \mathfrak{B}_2$. Например, это следует из описания автоустойчивых булевых алгебр, которое было независимо найдено в [5] и [6]. Тем самым с точки зрения общей теории вычислимости $\mathfrak{B}_1$ и $\mathfrak{B}_2$ идентичны.

Насколько сильно они могут различаться, если мы рассматриваем вычислимость с ограниченными ресурсами? Если $\mathfrak{B}$ — вычислимая безатомная булева алгебра, то всегда существует вычислимая функция $f : \mathfrak{B} \to \mathfrak{B}$ т.ч. $0 < f(a) < a$ при $a \neq 0$. Она может быть построена с помощью перебора всех элементов $\mathfrak{B}$. Если $\mathfrak{B}$ при этом вычислима за полиномиальное время, то что можно сказать о сложности такой функции? Нетрудно найти естественное представление $\mathfrak{B}_0 \cong \mathfrak{B}$, в котором такая функция f может быть выбрана

Alaev, P.E., Atomless Boolean algebras computable in polynomial time.

Работа поддержана РФФИ (грант 14-01-00376).

Поступила 10 октября 2016 г., опубликована 22 ноября 2016 г.

вычислимой за полиномиальное время. В данной статье строится пример безатомной алгебры $\mathfrak{B}_1$, вычислимой за полиномиальное время, в которой нет даже примитивно рекурсивной функции f с таким свойством. Тем самым никакие разумные оценки на сложность f в общем случае невозможны.

В частности, отсюда следует, что между $\mathfrak{B}_0$ и $\mathfrak{B}_1$ не существует изоморфизма g т.ч. g и g^{-1} — п.р.ф. В [4], в частности, показано, что такого сорта эффект верен вообще для любой локально конечной структуры (в том числе и для булевой алгебры): если $\mathfrak{A}_0$ — бесконечная локально конечная структура, вычислимая за полиномиальное время, то существует структура $\mathfrak{A}_1 \cong \mathfrak{A}_0$, также вычислимая за полиномиальное время, т.ч. не существует изоморфизма $g : \mathfrak{A}_0 \to \mathfrak{A}_1$, для которого g и g^{-1} — п.р.ф. Однако разница между $\mathfrak{B}_0$ и $\mathfrak{B}_1$ состоит не только в отсутствии изоморфизма, но и в существенном различии важных внутренних свойств.

То, что сложность функции f важна для изучения безатомных булевых алгебр, демонстрирует предложение, доказанное в конце статьи: если $\mathfrak{A}_0$ и $\mathfrak{A}_1$ — две примитивно рекурсивные ненулевые булевы алгебры, обладающие примитивно рекурсивной функцией f с указанным свойством, то существует изоморфизм $g : \mathfrak{A}_0 \to \mathfrak{A}_1$ т.ч. g и g^{-1} — п.р.ф. Это показывает, что оценки на сложность вычисления f могут дать некоторые оценки на сложность изоморфизма g.

2. Структуры, вычислимые за полиномиальное время

Кратко напомним несколько основных определений. Если Σ — конечный алфавит, то через Σ^* обозначим множество всех слов в этом алфавите. Если слово $a = a_1 \dots a_k \in \Sigma^*$, то его *размером* $\|a\|$ называем число $k + 1$. Функция $f : A \to \Sigma^*$, где $A \subseteq (\Sigma^*)^n$, является *вычислимой за полиномиальное время* (коротко, *p-вычислимой*), если существует машина Тьюринга T и константы $c, m \in \omega$ т.ч. $f(x)$ вычисляется машиной T не более чем за $c\|x\|^m$ шагов для любого $x \in A$, где $x = (x_1, \dots, x_n)$ и $\|x\| = \max\{\|x_1\|, \dots, \|x_n\|\}$. Подмножество $A \subseteq (\Sigma^*)^n$ *p-вычислимо*, если p-вычислима его характеристическая функция $\chi_A : (\Sigma^*)^n \to \{0, 1\}$.

Поскольку гёделевская нумерация для Σ^* позволяет легко перейти от слов к натуральным числам, определение вычислимых функций на Σ^* и вычислимых подмножеств $(\Sigma^*)^n$ является стандартным. То же самое касается примитивно рекурсивных функций и множеств. Поскольку согласно обычному определению примитивно рекурсивные функции должны быть всюду определены, функцию $f : A \to \Sigma^*$, где $A \subseteq (\Sigma^*)^n$, будем называть *примитивно рекурсивной* (*п.р.ф.*), если она является сужением на A некоторой примитивно рекурсивной функции $f_0 : (\Sigma^*)^n \to \Sigma^*$.

Скажем, что структура $\mathfrak{A}$ конечного языка является *вычислимой за полиномиальное время* (*p-вычислимой*), если существует конечный алфавит Σ т.ч. её носитель A является p-вычислимым подмножеством Σ^* и все функции и предикаты $\mathfrak{A}$ тоже p-вычислимы.

Определение примитивно рекурсивной структуры звучит дословно так же, если заменить в этом определении p-вычислимость на примитивную рекурсивность. Ясно, что p-вычислимая структура является примитивно рекурсивной.

3. Булева алгебра без эффективного алгоритма деления элементов

Пусть $\mathfrak{L} = (L, \leqslant)$ — линейный порядок с наименьшим элементом e. Если $a, b \in L$, то через $[a, b)$ обозначим полуинтервал $\{x \in L \mid a \leqslant x < b\}$, а через $[a, \infty)$ — полуинтервал $\{x \in L \mid a \leqslant x\}$. Через $\mathfrak{B}(\mathfrak{L})$ обозначим подалгебру, порождённую в булевой алгебре $P(L)$ всех подмножеств L семейством всех полуинтервалов $[a, b)$, где $a, b \in L$. Строение этой алгебры хорошо известно (см. [2]) — каждый её элемент единственным образом может быть представлен в одной из форм:
i) $[a_1, b_1) \cup \ldots \cup [a_n, b_n)$,
ii) $[a_1, b_1) \cup \ldots \cup [a_n, b_n) \cup [a_{n+1}, \infty)$,
где $n \geqslant 0$, $a_i < b_i$ и $b_i < a_{i+1}$ при всех i. При этом единицей $\mathfrak{B}(\mathfrak{L})$ является элемент $[e, \infty)$, а нулём — пустое множество $\emptyset$, которое соответствует форме i) при $n = 0$.

Предположим, что $\mathfrak{L}$ — p-вычислимый линейный порядок. Тогда $L \subseteq \Sigma^*$, где Σ — некоторый конечный алфавит. Ясно, что элементы $\mathfrak{B}(\mathfrak{L})$ в этом случае можно задать словами в алфавите $\Sigma \cup \{*, \infty\}$, где $*, \infty \notin \Sigma$. Элемент вида i) запишем как слово $a_1 * b_1 * a_2 * b_2 * \ldots * a_n * b_n$, а элемент вида ii) — как $a_1 * b_1 * \ldots * a_{n+1} * \infty$. В [1] показано, что булева алгебра, заданная таким образом, является p-вычислимой структурой. Тем самым получена

Теорема 1([1]). *Если $\mathfrak{L}$ — p-вычислимый линейный порядок с наименьшим элементом, то $\mathfrak{B}(\mathfrak{L})$ имеет p-вычислимое представление.*

Предположим теперь, что $\mathfrak{L}' = (L', \leqslant)$ — p-вычислимый плотный линейный порядок без концов, где $L' \subseteq \Sigma^*$. Назовём *функциями плотности* для $\mathfrak{L}'$ три функции $f_1, f_2 : L' \to L'$ и $f_3 : L' \times L' \to L'$ со свойствами:
1) $f_1(x) < x < f_2(x)$ при всех $x \in L'$;
2) $x < f_3(x, y) < y$ при всех $x, y \in L'$ т.ч. $x < y$.

Добавим к этому порядку наименьший элемент: пусть $\mathfrak{L} = (L, \leqslant)$, где $L = \{e\} \cup L'$ и $e < x$ для всех $x \in L'$. Тогда $\mathfrak{L}$ тоже можно считать p-вычислимым порядком над алфавитом $\Sigma \cup \{e\}$, где $e \notin \Sigma$. Обозначим через $\mathfrak{B}$ p-вычислимую булеву алгебру $\mathfrak{B}(\mathfrak{L})$, построенную по указанной выше схеме. Тогда $\mathfrak{B}$ — p-вычислимая безатомная булева алгебра. Далее для её элементов будем использовать стандартные обозначения i) и ii).

Лемма 1. *Следующие условия эквивалентны:*
a) *существует примитивно рекурсивная функция $f : \mathfrak{B} \to \mathfrak{B}$ со свойством: если $a \in \mathfrak{B}$ и $a \neq 0$, то $0 < f(a) < a$;*
b) *у $\mathfrak{L}'$ есть три примитивно рекурсивные функции плотности.*

Доказательство. (a $\Rightarrow$ b): построим $f_1 : L' \to L'$. Пусть $x \in L'$. Тогда $a = [e, x) \in \mathfrak{B}$ и $a \neq 0$. По условию $f(a) = [a_1, b_1) \cup \ldots \cup [a_n, b_n)$, где $a_i, b_i \in L$. Предположим, что $a_1 = e$. Тогда $e < b_1 < x$, и можно положить $f_1(x) = b_1$. Если же $a_1 \neq e$, то $a_1 \in L'$ и можно положить $f_1(x) = a_1$.

Аналогично строятся остальные функции: для построения $f_2(x)$ нужно рассмотреть $f(a)$, где $a = [x, \infty)$, а для построения $f_3(x, y)$ — рассмотреть $f(a)$, где $a = [x, y)$.

(b $\Rightarrow$ a): если $a \in \mathfrak{B}$ и $a \neq 0$, то a содержит полуинтервал $[a_1, b_1)$, где $a_1 < b_1$, или $[a_1, \infty)$. Если $a_1 \neq e$, то в первом случае положим $f(a) = [a_1, f_3(a_1, b_1))$, во втором $f(a) = [a_1, f_2(a_1))$. Если же $a_1 = e$, то в первом случае $f(a) = [e, f_1(b_1))$, а во втором $f(a) = [e, a_0)$ для некоторого фиксированного $a_0 \in L'$. $\square$

Отсюда нетрудно получить интересующий нас пример.

Теорема 2. *Существует p-вычислимая безатомная булева алгебра $\mathfrak{B}_1$, в которой нет примитивно рекурсивной функции $f : \mathfrak{B}_1 \to \mathfrak{B}_1$ со свойством: если $a \neq 0$, то $0 < f(a) < a$.*

Доказательство. В [3] был построен пример p-вычислимого плотного порядка $\mathfrak{L}'$ без концов т.ч. у $\mathfrak{L}'$ нет примитивно рекурсивных функций плотности (см. также [7, Th. 5.6]). Применим к этому порядку указанную выше конструкцию: положим $L = \{e\} \cup L'$ и $\mathfrak{B} = \mathfrak{B}(\mathfrak{L})$. Из леммы 1 следует, что указанной функции f не существует. $\square$

Напомним, как можно построить стандартное представление $\mathfrak{B}_0 \cong \mathfrak{B}_1$, в котором указанная функция f может быть выбрана p-вычислимой. Если $n \in \omega$, то через $\mathrm{bin}(n)$ обозначим стандартную бинарную запись n как слова в алфавите $\{0, 1\}$. Пусть $L' = \{\frac{n}{2^k} \mid 0 < n < 2^k$ и $k \geqslant 1\}$. Элементы $\mathfrak{L}'$ можно представить как слова вида $\mathrm{bin}(n) * \mathrm{bin}(2^k)$ в алфавите $\{0, 1, *\}$. Ясно, что такое представление с естественным порядком $\leqslant$ даст нам p-вычислимый плотный линейный порядок $\mathfrak{L}'$ без концов. Более того, в нём нетрудно построить и p-вычислимые функции плотности. Отметим, что эта простая конструкция также была указана в [3]. Переходя от $\mathfrak{L}'$ к $\mathfrak{B}(\mathfrak{L})$ по указанной выше схеме, мы получим искомую алгебру $\mathfrak{B}_0$.

В заключение покажем, что сложность функции f тесно связана со сложностью изоморфизма между двумя безатомными булевыми алгебрами.

Предложение 1. *Пусть $\mathfrak{A}_0$ и $\mathfrak{A}_1$ — две примитивно рекурсивные безатомные ненулевые булевы алгебры, для каждой из которых существует п.р.ф. $f_i : A_i \to A_i$ т.ч. $0 < f_i(x) < x$ при $x \neq 0$. Тогда существует изоморфизм $g : \mathfrak{A}_0 \to \mathfrak{A}_1$ т.ч. g и g^{-1} — п.р.ф.*

Доказательство. Будем рассматривать булевы алгебры в языке $(+, \cdot, -, 0, 1)$, где операции соответствуют объединению, пересечению и дополнению элементов. Запись $x - y$ означает разность $x \cdot (-y)$. Поскольку в этом предложении идёт речь только про п.р.ф., можно считать, что $A_0, A_1 \subseteq \omega$. Опишем некоторую конструкцию. На шаге $t \in \omega$ построим два набора $\bar{a}_t$ и $\bar{b}_t$, где $\bar{a}_t = a_{t,0}, \ldots, a_{t,n_t} \mid 1_{A_0}$ и $\bar{b}_t = b_{t,0}, \ldots, b_{t,n_t} \mid 1_{A_1}$, а запись $x_1, \ldots, x_n \mid 1$ означает, что $x_1 + \ldots + x_n = 1$ и $x_i \cdot x_j = 0$ при $i \neq j$, $i, j \leqslant n$. При этом функции, которые по $t \in \omega$ находят номера наборов $\bar{a}_t$ и $\bar{b}_t$, будут примитивно рекурсивными, и будет выполнено условие: $a_{t,j} = 0 \Leftrightarrow b_{t,j} = 0$ при всех t, j.

Положим $n_0 = 0$, $\bar{a}_0 = 1_{A_0}$ и $\bar{b}_0 = 1_{A_1}$. Далее при построении наборов будем выполнять условие: если $k \in A_0$, то k, как элемент $\mathfrak{A}_0$, равен сумме некоторых элементов из $\bar{a}_{2k+1}$, а если $k \in A_1$, то k — сумма некоторых элементов из $\bar{b}_{2k+2}$.

Пусть $\bar{a}_t$ и $\bar{b}_t$ уже построены. Предположим, что $t+1 = 2k+1$. Если $k \notin A_0$, то полагаем $\bar{a}_{t+1} = \bar{a}_t$ и $\bar{b}_{t+1} = \bar{b}_t$. Если же $k \in A_0$ и $\bar{a}_t = a_{t,0}, \ldots, a_{t,n_t}$, то положим

$$\bar{a}_{t+1} = a_{t,0} \cdot k,\ a_{t,0} - k,\ \ldots,\ a_{t,n_t} \cdot k,\ a_{t,n_t} - k.$$

Тем самым $n_{t+1} = 2n_t + 1$, $a_{t+1,2j} = a_{t,j} \cdot k$ и $a_{t+1,2j+1} = a_{t,j} - k$ при $j \leqslant n_t$.

Далее, если хотя бы один из элементов $a_{t+1,2j}, a_{t+1,2j+1}$ равен 0, например, $a_{t+1,2j} = 0$, то положим $b_{t+1,2j} = 0$ и $b_{t+1,2j+1} = b_{t,j}$. Если же они оба не равны 0, то применим к $b_{t,j}$ функцию f_1: найдём b т.ч. $0 < b < b_{t,j}$ и положим $b_{t+1,2j} = b$, $b_{t+1,2j+1} = b_{t,j} - b$.

Случай $t + 1 = 2k + 2$ рассматривается аналогично: мы делим элементы $\bar{b}_t$, получая набор $\bar{b}_{t+1}$, и с помощью f_0 находим ему нужных напарников для $\bar{a}_{t+1}$.

Искомый изоморфизм $g : A_0 \to A_1$ теперь строится так: если $k \in A_0$, то находим представление $k = \sum_{j \in I} a_{t,j}$, где $I \subseteq \{0, \dots, n_t\}$, и полагаем $g(k) = \sum_{j \in I} b_{t,j}$. Поскольку из конструкции ясно, что каждый элемент $\bar{a}_s$ — сумма определённых элементов из $\bar{a}_{s+1}$, указанное представление для k существует при всех $t \geqslant 2k+1$, а определение g не зависит от выбора t. Нетрудно проверить, что g — изоморфизм $\mathfrak{A}_0$ и $\mathfrak{A}_1$, являющийся п.р.ф.

При этом построение g^{-1} выглядит аналогично: если $k \in A_1$ и $k = \sum_{j \in I} b_{t,j}$ для некоторого $t \geqslant 2k + 2$, то $g^{-1}(k) = \sum_{j \in I} a_{t,j}$. $\square$

References

[1] Cenzer D., Remmel J., *Polynomial time versus recursive models*, Annals of Pure and Applied Logic, **54** (1991), 17–58. Zbl 0756.03021

[2] Goncharov S.S., *Countable Boolean algebras and decidability*, Siberian School of Algebra and Logic, New York, NY: Plenum. xii, 1997. Zbl 0912.03019

[3] Remmel J.B., *Polynomial time categoricity and linear orderings*, Progr. Comput. Sci. Appl. Logic, **12** (1993), 713–746. Zbl 0832.03020

[4] Alaev P.E., *Existence and uniqueness of structures computable in polynomial time*, Algebra and logic, **55**:1 (2016), 72–76. Zbl 06638201

[5] Remmel J.B., *Recursive isomorphism types of recursive Boolean algebras*, The Journal of Symbolic Logic, **46**:3 (1981), 572–594. Zbl 0543.03031

[6] Goncharov S.S., Dzgoev V.D., *Autostability of models*, Algebra and Logic, **19**:1 (1980), 28–37. Zbl 0468.03023

[7] Cenzer D., Remmel J.B., *Complexity Theoretic Model Theory and Algebra*, Handbook of Recursive Mathematics, **1**, 1998. Zbl 0941.03035

Pavel Evgenievich Alaev
Sobolev Institute of Mathematics,
pr. Koptyuga, 4,
630090, Novosibirsk, Russia
E-mail address: alaev@math.nsc.ru