Задача проверки тождеств в конечных решетках

Е. В. Богомолова Н. В. Китов
cyberkiller@mail.ru

УрФУ (Екатеринбург)

Аннотация

Исследуется сложность задачи проверки тождеств в конечных решетках. Показано, что тождества, обе части которых представлены в виде суммы одночленов, можно проверить за время, полиномиальное от размера тождества, в любой конечной решетке, а задача проверки тождеств, у которых в виде суммы одночленов представлена только одна часть, является co-NP-полной для любой неодноэлементной дистрибутивной решетки.

1 Постановка задачи

Мы предполагаем, что читатель знаком с исходными понятиями универсальной алгебры и сложности вычислений в объеме начальных глав учебников [4, 1, 9], и будем свободно ими пользоваться.

Пусть $\mathcal{A}$ — произвольная, но фиксированная конечная алгебра. Задача проверки тождеств в алгебре $\mathcal{A}$, обозначаемая CHECK-ID($\mathcal{A}$), — это комбинаторная задача распознавания, входными данными которой служат всевозможные пары (p, q) термов в сигнатуре алгебры $\mathcal{A}$, а ответами — «ДА» или «НЕТ» в зависимости от того, выполнено или не выполнено тождество $p = q$ в этой алгебре. Эта задача алгоритмически разрешима — если термы p и q в совокупности зависят от m переменных, то можно поочередно подставлять вместо переменных всевозможные m-ки элементов алгебры $\mathcal{A}$ и проверять, приводят ли такие подстановки к равным значениям термов p и q. Очевидно, что время работы такого прямолинейного алгоритма в худшем случае экспоненциально зависит от размера входных данных, так как число m-ок, подлежащих перебору, равно $|\mathcal{A}|^m$. С другой стороны, для любой конечной алгебры $\mathcal{A}$ задача CHECK-ID($\mathcal{A}$) принадлежит классу сложности co-NP: если для какой-то пары термов (p, q) тождество $p = q$ не выполняется в алгебре $\mathcal{A}$, то недетерминированный полиномиальный алгоритм может угадать m-ку элементов из $\mathcal{A}$, опровергающую данное тождество, и подтвердить свою догадку, вычислив значения термов p и q на этой m-ке, что требует лишь полиномиального от размера термов p и q числа шагов типа «Подсчитать результат операции над известными элементами алгебры $\mathcal{A}$». Поскольку алгебра $\mathcal{A}$ фиксирована и не является частью входа, каждый такой шаг выполняется за константное время, и общее время работы алгоритма ограничено многочленом от размера входа.

Исследовать вычислительную сложность задачи CHECK-ID($\mathcal{A}$) предложил М. В. Сапир в хорошо известном обзоре [7], см. там проблему 2.4. Как подмечено в [7, с. 402], если $\mathcal{A}$ – двухэлементная булева алгебра, то задача Check-Id($\mathcal{A}$) равносильна «отрицанию» классической задачи Выполнимость. Поскольку последняя NP-полна (см. [1, 9]), отсюда следует, что задача проверки тождеств в двухэлементной булевой алгебре будет co-NP-полной. Понятно, что тот факт, что проверка тождеств в булевой алгебре сложна, связан с тем, что операции булевой алгебры обладают максимальной выразительной силой — как хорошо известно, любую булеву функцию можно реализовать подходящим термом в сигнатуре булевой алгебры.

In: A.A. Makhnev, S.F. Pravdin (eds.): Proceedings of the 47th International Youth School-conference "Modern Problems in Mathematics and its Applications", Yekaterinburg, Russia, 02-Feb-2016, published at http://ceur-ws.org

Что можно сказать о сложности задачи Check-Id($\mathcal{A}$), если исходная конечная алгебра $\mathcal{A}$ обладает меньшими, чем булевы алгебры, «выразительными возможностями», например, если $\mathcal{A}$ — полугруппа, группа, кольцо, решетка? Этот вопрос также явно ставился в [7].

Имеется большой массив работ, посвященных задаче проверки тождеств в кольцах, группах и полугруппах. (Заметим, что в некоторых из этих работ задача проверки тождеств фигурирует под названием «задача эквивалентности термов».) Мы не будем здесь давать обзор таких работ, а отметим только несколько результатов, важных с точки зрения вопросов, рассматриваемых в данной заметке. Во-первых, в классе полугрупп известны примеры [8, 10], которые демонстрируют, что свойство конечной алгебры иметь полиномиально разрешимую задачу проверки тождеств, вообще говоря, не переносится на ее подалгебры и гомоморфные образы. Соответственно, из того, что у некоторой алгебры $\mathcal{A}$ имеется подалгебра или гомоморфный образ с co-NP-полной задачей проверки тождеств, вообще говоря, не следует, что и сама алгебра $\mathcal{A}$ такова. Во-вторых, при изучении сложности задачи проверки тождеств в ассоциативных кольцах, выяснилось, что ситуация может существенным образом зависеть от формы записи тождеств. Ясно, что каждое кольцевое тождество можно записать в виде $f(x_1, \dots, x_n) = 0$, где $f(x_1, \dots, x_n)$ — многочлен с целыми коэффициентами от некоммутирующих переменных $x_1, \dots, x_n$. Если не накладывать никаких априорных ограничений на вид многочлена $f(x_1, \dots, x_n)$, то задача Check-Id($\mathcal{R}$) для конечного ассоциативного кольца $\mathcal{R}$ разрешима за полиномиальное время, если кольцо $\mathcal{R}$ нильпотентно, и co-NP-полна, если $\mathcal{R}$ ненильпотентно [6, 3]. Понятно, что любой многочлен можно записать в стандартной форме — как сумму одночленов. Оказывается, задача проверки тождеств, левые части которых записаны в виде суммы одночленов, разрешима за полиномиальное время, например, для любого конечного ассоциативно-коммутативного кольца (это следует из работы [5], где получен даже несколько более общий результат). Причина такого контраста на самом деле довольно проста: в теории сложности вычислений время работы алгоритма для решения задачи измеряется функцией от длины входа этой задачи. В случае задачи проверки тождеств в кольце длиной входа является длина записи многочлена, и при переходе к стандартной записи эта длина может экспоненциально вырасти. Например, в записи многочлена $(x_1 + y_1) \dots (x_n + y_n)$ используется $5n$ символов (если считать, что умножение, как обычно, обозначается отсутствием точки), а если раскрыть все скобки и записать этот же многочлен в виде суммы одночленов, то таких одночленов будет 2^n и общая длина записи составит $(n + 1)2^n - 1$. Поэтому алгоритм, работающий полиномиальное время от длины стандартной записи, может оказаться экспоненциальным, если измерять время его работы как функцию длины исходной записи.

В данной заметке рассматривается задача проверки тождеств в конечных решетках. Единственной работой на эту тему, которую нам удалось обнаружить, является статья [2]. Из ее результатов вытекает, что задача CHECK-ID($\mathcal{L}$) является co-NP-полной для любой неодноэлементной дистрибутивной решетки $\mathcal{L}$. По-видимому, под влиянием этого факта у исследователей сложилось впечатление, что для случая решеток проблематика, связанная со сложностью проверки тождеств, исчерпана. Однако полугрупповые примеры, упомянутые в предыдущем абзаце, указывают на некоторую преждевременность такого заключения: хотя каждая неодноэлементная решетка содержит неодноэлементную дистрибутивную решетку в качестве подрешетки, это не исключает существование конечных решеток с полиномиальной задачей проверки тождеств. Мы не знаем, существуют ли такие примеры.

Другое направление, которое подсказано обсуждавшимися выше результатами о задаче проверки тождеств в кольцах, состоит в рассмотрении тождеств определенного вида. Будем по аналогии с кольцевым случаем называть решеточные операции сложением и умножением и обозначать их соответственно знаком $+$ и отсутствием точки. Наш основной результат показывает, что существует полиномиальный алгоритм, который проверяет в любой фиксированной неодноэлементной конечной решетке справедливость тождества $p = q$, в котором оба терма p и q представлены в виде суммы одночленов. С другой стороны, мы выводим из конструкции, использованной в [2], что для неодноэлементной дистрибутивной решетки задача проверки тождеств, у которых только одна из частей приведена к сумме одночленов, остается co-NP-полной.

2 Основные результаты

Теорема. Пусть $(\mathcal{L} = L, +, \cdot)$ — неодноэлементная конечная решетка. Существует полиномиальный алгоритм, который проверяет, выполнено ли в $\mathcal{L}$ тождество $p = q$ при условии, что оба терма p и q представлены в виде суммы одночленов.

Доказательство. Упомянутый полиномиальный алгоритм основан на следующем наблюдении.

Лемма. Тождество

$$u_1 + u_2 + \cdots + u_k = v_1 + v_2 + \cdots + v_\ell, \tag{1}$$

где все u_i и v_j — одночлены (т.е. произведения переменных), выполнено в неодноэлементной решетке $(\mathcal{L} = L, +, \cdot)$ тогда и только тогда, когда выполнены два условия

(i) для любого $i \in \{1, \ldots, k\}$ найдется такое $j \in \{1, \ldots, \ell\}$, что каждая переменная из v_j появляется в u_i;

(ii) для любого $s \in \{1, \ldots, \ell\}$ найдется такое $t \in \{1, \ldots, k\}$, что каждая переменная из u_t появляется в v_s.

Доказательство леммы. Пусть $u = u_1 + u_2 + \cdots + u_k$, $v = v_1 + v_2 + \cdots + v_\ell$.

Необходимость каждого из условий (i) и (ii) доказывается методом контрапозиции. Предположим, например, что условие (i) нарушено. Тогда существует такое $i \in \{1, \ldots, k\}$, что в каждом одночлене v_j, $j \in \{1, \ldots, \ell\}$, есть хотя бы одна переменная, которая не появляется в одночлене u_i. Зафиксируем одну такую переменную для каждого $j \in \{1, \ldots, \ell\}$ и обозначим ее через $x[v_j]$. (Переменные $x[v_j]$, отвечающие разным j, могут совпадать — важно только то, что каждая выбранная переменная входит в соответствующий одночлен v_j и что ни одна из них не входит в одночлен u_i.) Поскольку решетка $\mathcal{L}$ неодноэлементна, в ней найдутся такие различные элементы a, b, что $ab = a$, $a + b = b$. Рассмотрим интерпретацию переменных тождества (1) в решетке $\mathcal{L}$, при которой все переменные $x[v_j]$ принимают значение a, а все остальные переменные принимают значение b. Тогда одночлен u_i принимает значение b, а следовательно, такое же значение принимает многочлен u. С другой стороны, значение каждого из одночленов v_j будет равно a, откуда и значение многочлена v равно a. Мы видим, что тождество (1) не выполняется в решетке $\mathcal{L}$. Аналогично рассуждаем в случае, когда нарушено условие (ii).

Для доказательства достаточности рассмотрим произвольный одночлен u_i из u. Если условие (i) выполнено, то в v найдется одночлен v_j такой, что каждая переменная из v_j появляется в u_i. В силу коммутативности, ассоциативности и идемпотентности умножения отсюда следует, что либо $u_i = v_j$, либо $u_i = v_j w$ для некоторого одночлена w. Поэтому $u_i + v_j = v_j$ (в первом случае срабатывает идемпотентность сложения, а во втором — закон поглощения). Используя ассоциативность и коммутативность сложения, получаем, что $u_i + v = v$, откуда $u + v = v$. Аналогично, из условия (ii) выводится, что $u + v = u$. Итак, $u = v$, т.е. тождество (1) выполнено в решетке $\mathcal{L}$. Лемма доказана.

Заключение теоремы сразу же следует из леммы, так как условия (i) и (ii) проверяются за линейное время от размера тождества. Теорема доказана.

Замечание 1. Конечно, в отличие от обсуждавшегося во введении случая колец, не всякое тождество произвольной решетки может быть переписано в виде равенства сумм одночленов. Это, однако, возможно для тождеств дистрибутивной решетки. Как уже отмечалось, в [2] показано, что задача проверки в конечной неодноэлементной дистрибутивной решетке co-NP-полна. Хотя на первый взгляд этот результат противоречит теореме, в действительности противоречия нет: как и в случае колец, разница в сложности объясняется тем, что при приведении многочлена к сумме одночленов с помощью дистрибутивного закона длина записи многочлена может экспоненциально возрастать.

Замечание 2. Назовем линейным многочлен, представляющий собой сумму переменных. Из двойственности между операциями сложения и умножения в решетках следует, что справедлив и двойственный вариант теоремы: существует полиномиальный алгоритм, который проверяет, выполнено ли в данной решетке $\mathcal{L}$ тождество $p = q$ при условии, что оба терма p и q представлены в виде произведений линейных многочленов.

В заключение покажем, как из редукции, использованной в [2], вытекает, что для неодноэлементной дистрибутивной решетки задача проверки тождеств, у которых одна из частей приведена к сумме одночленов, остается co-NP-полной. Напомним, что входом задачи Выполнимость служит произвольная булева формула $F(x_1, \ldots, x_n)$ в конъюнктивной нормальной форме, т.е. конъюнкция дизъюнкций переменных и их отрицаний. Применяя законы де Моргана, запишем отрицание $\neg F(x_1, \ldots, x_n)$ этой формулы в дизъюнктивной нормальной форме, т.е. в виде дизъюнкции конъюнкций переменных и их отрицаний. Теперь преобразуем $\neg F(x_1, \ldots, x_n)$ в решеточный многочлен по следующему правилу: знак дизъюнкции заменяем на знак $+$, знак конъюнкции — на отсутствие точки, а отрицание переменной x_i — на новую переменную y_i. В результате получим многочлен $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$, записанный в виде суммы одночленов. Например, для случая, когда исходная формула $F(x_1, \ldots, x_n)$ есть

$$(x_1 \vee x_2 \vee x_3) \wedge (\neg x_1 \vee x_2) \wedge (\neg x_2 \vee x_3) \wedge (\neg x_2 \vee \neg x_3),$$

дизъюнктивная нормальная форма ее отрицания есть

$$(\neg x_1 \wedge \neg x_2 \wedge \neg x_3) \vee (x_1 \wedge \neg x_2) \vee (x_2 \wedge \neg x_3) \vee (x_2 \wedge x_3),$$

и описанное преобразование дает многочлен

$$y_1y_2y_3 + x_1y_2 + x_2y_3 + x_2x_3.$$

Рассмотрим тождество

$$f(x_1, \ldots, x_n, y_1, \ldots, y_n) = f(x_1, \ldots, x_n, y_1, \ldots, y_n) + (x_1 + y_1) \cdots (x_n + y_n). \tag{2}$$

Левая часть этого тождества по построению есть сумма одночленов. В [2] показано, что тождество (2) не выполняется в неодноэлементной дистрибутивной решетке тогда и только тогда, когда исходная формула $F(x_1, \ldots, x_n)$ выполнима. Для удобства читателя воспроизведем аргумент из [2] в немного упрощенном виде (в [2] рассматриваются не решетки, а алгебры гораздо более общего вида, что делает доказательство более громоздким).

Допустим, что формула $F(x_1, \ldots, x_n)$ выполнима, и пусть $\varphi\colon \{x_1, \ldots, x_n\} \to \{0, 1\}$ — выполняющий набор значений истинности переменных, т.е. $F(\varphi(x_1), \ldots, \varphi(x_n)) = 1$. Рассмотрим множество $\{0, 1\}$ как двухэлементную решетку, в которой $0 + 1 = 1$ и $0 \cdot 1 = 0$. Проинтерпретируем в этой решетке переменные $x_1, \ldots, x_n$ в соответствии со значением функции φ, а каждой переменной y_i, $i = 1, \ldots, n$, придадим значение $1 - \varphi(x_i)$. Тогда произведение $(x_1 + y_1) \ldots (x_n + y_n)$, а вместе с ним и вся правая часть тождества (2) примет значение 1. Значение же многочлена $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$ совпадет со значением формулы $\neg F(x_1, \ldots, x_n)$, т.е. будет равно 0. Мы видим, что тождество (2) не выполняется в решетке $\{0, 1\}$.

Обратно, допустим, что тождество (2) не выполняется в какой-то неодноэлементной дистрибутивной решетке. Поскольку все неодноэлементные дистрибутивные решетки удовлетворяют одним и тем же тождествам, (2) не выполнено и в решетке $\{0, 1\}$. Последнее возможно только, если при некоторой интерпретации ψ переменных $x_1, \ldots, x_n, y_1, \ldots, y_n$ в решетке $\{0, 1\}$ значение многочлена $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$ есть 0, а значение многочлена $(x_1 + y_1) \cdots (x_n + y_n)$ равно 1. Из последнего факта следует, что для каждого $i = 1, \ldots, n$ хотя бы одна из переменных x_i и y_i принимает значение 1. Зафиксируем для каждого $i = 1, \ldots, n$ одну такую переменную и затем заменим рассматриваемую интерпретацию ψ на интерпретацию φ, которая на выбранной переменной также дает 1, а на второй переменной с тем же индексом принимает значение 0. По построению $\varphi(x_i) \leqslant \psi(x_i)$ и $\varphi(y_i) \leqslant \psi(y_i)$ для каждого $i = 1, \ldots, n$, а поскольку решеточные многочлены монотонны, заключаем, что

$$f(\varphi(x_1), \ldots, \varphi(x_n), \varphi(y_1), \ldots, \varphi(y_n)) \leqslant f(\psi(x_1), \ldots, \psi(x_n), \psi(y_1), \ldots, \psi(y_n)).$$

Правая часть этого неравенства по выбору интерпретации ψ равна 0, значит, и левая часть равна 0. Итак, интерпретация φ обращает в 0 многочлен $f(x_1, \ldots, x_n, y_1, \ldots, y_n)$ и при этом по построению такова, что $\varphi(y_i) = 1 - \varphi(x_i)$ для каждого $i = 1, \ldots, n$. В силу последнего свойства ее можно рассматривать как интерпретацию булевых переменных $x_1, \ldots, x_n$, а в силу первого — формула $\neg F(x_1, \ldots, x_n)$ ложна при этой интерпретации. Поэтому $\varphi\colon \{x_1, \ldots, x_n\} \to \{0, 1\}$ будет выполняющим набором значений истинности переменных для формулы $F(x_1, \ldots, x_n)$.

Список литературы

[1] M. Garey, D. Johnson. Computers and intractability: a guide to the theory of NP-completeness. *N.Y.: W.H. Freeman & co*, 1979.

[2] P. A. Bloniarz, H. B. Hunt III, D. J. Rosenkrantz. Algebraic structures with hard equivalence and minimization problems. *J. ACM* 31(4):879–904, 1984.

[3] S. Burris, J. Lawrence. The equivalence problem for finite rings. *J. Symbolic Computation*, 15(1), 67–71, 1993.

[4] S. Burris, H. P. Sankappanavar. A Course in Universal Algebra. Berlin: Springer-Verlag, 1981.

[5] G. Horváth. The complexity of the equivalence problem over finite rings. *Glasgow Math. J.*, 54(1), 193–199, 2012.

[6] H. B. Hunt III, R. E. Stearns. The complexity of equivalence for commutative rings. *J. Symbolic Computation*, 10(5), 411–436, 1990.

[7] O. G. Kharlampovich, M. V. Sapir. Algorithmic problems in varieties. *Int. J. Algebra and Computation*, 5(4-5), 379–602, 1995.

[8] O. Klíma. Complexity issues of checking identities in finite monoids. *Semigroup Forum*, 79(3), 435–444, 2009.

[9] C. H. Papadimitriou. Computational Complexity. Reading–Menlo Park–N.Y.: Addison-Wesley Publishing Company, 1994.

[10] S. Seif. The Perkins semigroup has co-NP-complete term-equivalence problem. *Int. J. Algebra and Computation*, 15(2), 317–326, 2005.

Checking identities in finite lattices

Ekaterina V. Bogomolova, Nikita V. Kitov
Ural Federal University (Yekaterinburg, Russia)

Keywords: lattice, lattice identity, co-NP-complete problem.

Abstract. We study the complexity of identity checking in finite lattices. We show that every identity whose sides are both represented as sums of monomials can be checked in polynomial time in every finite lattice while checking identities with only one side being a sum of monomials is co=NP-complete for every non-singleton distributive lattice.