АЛГЕБРА И МАТЕМАТИЧЕСКАЯ ЛОГИКА

ТЕОРИЯ И ПРИЛОЖЕНИЯ

г. Казань, 24–28 июня 2019 г.

Материалы международной конференции
“Алгебра и математическая логика: теория и приложения”,
посвященной 125-летию со дня рождения основателя кафедры алгебры
Казанского университета члена-корреспондента АН СССР
Николая Григорьевича Чеботарева и 75-летию со дня рождения заведующего кафедрой
академика АН РТ Марата Мирзаевича Арсланова

АЛГЕБРА

И

МАТЕМАТИЧЕСКАЯ ЛОГИКА:

ТЕОРИЯ И ПРИЛОЖЕНИЯ

(г. Казань, 24-28 июня 2019 г.)

Казанский (Приволжский) федеральный университет

2019

Казанский (Приволжский)
федеральный университет
Россия, Татарстан
420008, Казань
ул. Кремлевская 18

Kazan (Volga Region)
Federal University
Russia, Tatarstan
420008, Kazan
Kremlevskaya st. 18

Казанский (Приволжский) федеральный университет,
Российский фонд фундаментальных исследований
Мероприятие проводится при финансовой поддержке
Российского фонда фундаментальных исследований, проект №19-01-20103

УДК 510:512
ББК 22.1

Материалы печатаются в авторской редакции.

Материалы конференции "Алгебра и математическая логика: теория и приложения" (г. Казань, 24-28 июня 2019 г.). – Казань: КФУ, 2019. – 185 с.

Сборник содержит тезисы докладов, представленных на международную коференцию "Алгебра и математическая логика: теория и приложения" (г. Казань, 24-28 июня 2019 г.), посвященной 125-летию со дня рождения основателя кафедры алгебры Казанского университета члена-корреспондента АН СССР Николая Григорьевича Чеботарева и 75-летию со дня рождения заведующего кафедрой академика АН РТ Марата Мирзаевича Арсланова.

УДК 510:512
ББК 22.1

Теорема 2. *Если алгебраическая система конечна и имеет отношение линейного порядка, то для любой формулы* PFP*-логики с кванторами первого и второго порядков можно построить эквивалентную формулу вида*

$$(M\bar{y}_1)\,\mathrm{PFP}_{Q(\bar{y}_2)}(\psi),$$

где M — кванторы первого порядка, а ψ — формула логики первого порядка.

Для доказательства данной теоремы мы заменяем каждую подформулу видов $(\exists Q)\varphi$ и $(\forall Q)\varphi$ на оператор частичной фиксированной точки. Таким образом мы получим формулу с кванторами только первого порядка, но несколькими PFP-операторами. После этого можем воспользоваться теоремой 1, чтобы преобразовать формулу к указанному виду.

Литература

1. Дудаков С.М. О безопасности рекурсивных запросов // Вестник ТвГУ. Серия: Прикладная математика. 2012. № 4. С. 71–80.

2. Libkin L. Elements of Finite Model Theory. Springer, 2004.

ЗАМЕТКИ О ГЕНЕРИЧЕСКОЙ СЛОЖНОСТИ ЗАДАЧ РАСПОЗНАВАНИЯ

А. В. Селиверстов

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук, Москва

slvstv@iitp.ru

Большое внимание уделяется изучению *генерических* алгоритмов (Рыбалов, 2017 и 2018). Они служат важным частным случаем эвристических алгоритмов, когда на почти любом входе результатом работы алгоритма служит правильный ответ, но на пренебрежимо малой доле входов (то есть доле, стремящейся к нулю при увеличении длины входа) алгоритм может отказаться от вычислений, выдавая явно сообщение об отказе. Напротив, отсутствие быстрого генерического алгоритма служит для обоснования надёжности криптографических методов (Рыбалов, 2016).

В этой работе языком называется непустое множество слов конечной длины над алфавитом $\{0,1\}$. Язык распознаётся генерическим алгоритмом, если алгоритм правильно распознаёт те входы, на которых не происходит отказа от вычисления. Очевидная трудность связана с тем, что последовательное выполнение всюду определённого и генерического алгоритмов полиномиального времени может дать тривиальный генерический алгоритм, который либо отвергает вход, либо отказывается от вычислений. Например, посредством набивки (padding), каждая задача распознавания сводится за полиномиальное время (по Карпу) к задаче, которая разрешима (тривиальным) генерическим алгоритмом полиномиального времени.

Определение 1. Генерический алгоритм распознавания назовём нетривиальным, если существуют бесконечное множество входов, которые он принимает, и бесконечное множество входов, которые он отвергает, не отказываясь от вычисления на этих входах.

По аналогии с определением неуниформных классов языков $P/poly$ и $NP/poly$ определяются неуниформные генерические алгоритмы.

Определение 2. Язык распознаётся неуниформным генерическим алгоритмом полиномиального времени, если для каждой длины входа n существует такая пара булевых схем полиномиального от n размера, что если первая схема даёт ответ 1, то вход принимается, когда вторая схема даёт ответ 1, и отвергается, когда вторая схема даёт ответ 0. При этом доля входов длины n, на которых первая схема даёт ответ 0, стремится к нулю с ростом n. Ответ 0 первой схемы означает, что алгоритм отказывается от вычислений. Если обе булевы схемы вычислимы за полиномиальное время, это определение эквивалентно определению генерического алгоритма полиномиального времени.

Теорема 1. *Если язык принадлежит пересечению классов $coNP \cap NP/poly$, то он сводится за полиномиальное время к языку, распознаваемому нетривиальным неуниформным генерическим алгоритмом полиномиального времени.*

Доказательство теоремы 1 использует набивку (padding); она не даёт практически полезного алгоритма. Однако теорема 1 устанавливает связь вычислительной сложности (в худшем случае) с генерической сложностью (в типичном случае).

Перейдём к нетривиальным генерическим алгоритмам полиномиального времени для решения прикладных задач. Точка на вещественной поверхности называется эллиптической, если в её окрестности поверхность аппроксимируется эллиптическим параболоидом. Распознавание эллиптических точек на поверхности играет важную роль в системах автоматизированного проектирования. В частности, эллиптических точек нет на широко используемых линейчатых поверхностях (Vršek, 2018). Примерами линейчатых поверхностей служат цилиндры и зонтик Уитни.

Понятие эллиптической точки обобщается для вещественных гиперповерхностей произвольной размерности. На графике многочлена эллиптическая точка соответствует точке из области определения, в которой матрица вторых частных производных этого многочлена знакоопределена.

Многочлены отождествляются с последовательностью рациональных дробей, числитель и знаменатель которых записаны в двоичной системе.

Теорема 2. *Дано нечётное целое число $d \geqslant 3$. Множество многочленов степени d от двух переменных над полем рациональных чисел, графики которых содержат эллиптические точки, распознаётся нетривиальным генерическим алгоритмом полиномиального времени.*

Ограничение на степень существенно. Графиком линейной функции от двух переменных служит плоскость, не имеющая эллиптических точек. Если же степень равна двум, то существование эллиптической точки распознаётся детерминированным алгоритмом за полиномиальное время.

Теорема 3. *Дано нечётное целое число $d \geqslant 3$. Множество многочленов степени d от трёх переменных над полем рациональных чисел, графики которых содержат эллиптические точки, распознаётся нетривиальным генерическим алгоритмом полиномиального времени.*

Общая идея доказательства теорем 2 и 3 состоит в том, что для почти всех рассматриваемых многочленов график содержит эллиптическую точку. (Фраза “для почти всех” означает: “для всех, кроме некоторой части множества нулей некоторого многочлена, не равного тождественно нулю”.) Более того, для почти всех таких многочленов эллиптическая точка на графике может быть найдена за полиномиальное время; это наиболее трудная часть доказательства. С другой стороны, существуют легко распознаваемые многочлены, графики которых не содержат эллиптических точек. Например, таков любой многочлен, который линейной заменой переменных приводится к многочлену от одной переменной. Его графиком служит цилиндр. Также эллиптических точек нет на обезьяньем

седле. Оценка доли входов, на которых алгоритм отказывается от вычисления, использует лемму Шварца–Зиппеля (Schwartz, 1980).

Генерический алгоритм сначала пытается найти эллиптическую точку. Если это удаётся, то вход принимается. Иначе проверяется принадлежность многочлена к известным семействам многочленов, чьи графики не содержат эллиптических точек. Если это удаётся, то вход отвергается. Иначе выдаётся уведомление об отказе от вычисления.

Литература

1. Рыбалов А.Н. О генерической амплификации рекурсивно перечислимых множеств // Алгебра и логика. 2018. Т. 57. № 4. С. 448–455. https://doi.org/10.17377/alglog.2018.57.403.

2. Рыбалов А.Н. О генерической сложности проблемы дискретного логарифма // Прикладная дискретная математика. 2016. № 3(33). С. 93–97. https://doi.org/10.17223/20710410/33/8.

3. Рыбалов А.Н. О генерической сложности проблемы разрешимости систем диофантовых уравнений в форме Сколема // Прикладная дискретная математика. 2017. № 37. С. 100–106. https://doi.org/10.17223/20710410/37/8.

4. Schwartz J.T. Fast probabilistic algorithms for verification of polynomial identities // Journal of the ACM. 1980. V. 27. no. 4. P. 701–717. https://doi.org/10.1145/322217.322225.

5. Vršek J. Contour curves and isophotes on rational ruled surfaces // Computer Aided Geometric Design. 2018. V. 65. P. 1–12. https://doi.org/10.1016/j.cagd.2018.06.006.

ИЗОМОРФИЗМЫ РЕШЕТОК ПОДАЛГЕБР ПОЛУКОЛЕЦ НЕПРЕРЫВНЫХ ДЕЙСТВИТЕЛЬНОЗНАЧНЫХ ФУНКЦИЙ С MAX-СЛОЖЕНИЕМ

В. В. Сидоров

Вятский государственный университет, г. Киров

sedoy_vadim@mail.ru

Полукольцом называется алгебраическая система $\langle S, +, \cdot, 0, 1\rangle$, где $\langle S, +, 0\rangle$ — коммутативный моноид с нейтральным элементом нуль 0, $\langle S, \cdot, 1\rangle$ — моноид с нейтральным элементом единица 1, умножение дистрибутивно относительно сложения с обеих сторон и $0 \cdot a = a \cdot 0 = 0$ для всех $a \in S$. Множество $\mathbb{R}_+$ неотрицательных действительных чисел с операциями сложения и умножения является полукольцом.

Заменим в $\mathbb{R}_+$ обычное сложение на max-сложение $\vee$: $a \vee b = \max\{a, b\}$. Получим полукольцо ${\mathbb{R}_+}^{\vee}$. Множество $C^{\vee}(X)$ непрерывных ${\mathbb{R}_+}^{\vee}$-значных функций, заданных на произвольном топологическом пространстве X, с поточечными операциями max-сложения и умножения функций является полукольцом.

Классическая теорема Гельфанда–Колмогорова [1] утверждает, что для любого тихоновского пространства X спектр кольца $C(X)$ непрерывных действительнозначных функций гомеоморфен стоун-чеховской компактификации βX. В частности, топология произвольного компакта X определяется кольцом $C(X)$.