Латкин И.В.[1], Селиверстов А.В.[2]

[1] Восточно-Казахстанский государственный технический университет им. Д. Серикбаева, г. Усть-Каменогорск, к.ф.-м.н., доцент кафедры «Высшая математика», lativan@yandex.kz
[2] Институт проблем передачи информации им. А.А. Харкевича РАН, г. Москва, к.ф.-м.н., ведущий научный сотрудник лаборатории 6, slvstv@iitp.ru

О сложности фрагментов теории поля комплексных чисел

КЛЮЧЕВЫЕ СЛОВА

Вычислительная сложность, теория первого порядка, комплексные числа, перемена кванторов, иерархия классов.

АННОТАЦИЯ

В статье обсуждается вычислительная сложность фрагментов теории первого порядка поля комплексных чисел с ограничением на число перемен кванторов в формулах, находящихся в предварённой форме.

Напомним, что каждая полная рекурсивно аксиоматизируемая теория первого порядка разрешима. Примерами таких теорий служат теория алгебраически замкнутого поля фиксированной характеристики, теория вещественно замкнутых полей, теория плотных линейных порядков без концевых элементов, арифметика Пресбургера и чистая теория равенства. Последняя из перечисленных теорий разрешима на полиномиально ограниченной памяти и полна в этом классе [1]. Но для большинства разрешимых теорий сложность разрешающего алгоритма очень велика. Например, известен алгоритм дважды экспоненциального времени для теории поля комплексных чисел. С другой стороны, любой разрешающий алгоритм теории алгебраически замкнутого поля фиксированной характеристики требует использовать (по меньшей мере) экспоненциальную память [2]. Нижние границы сложности арифметики Пресбургера и её фрагментов обсуждаются в работе [3]. Высокая сложность и у многих неполных теорий [4].

Мы рассмотрим разрешающие алгоритмы для фрагментов теории поля комплексных чисел, состоящих из формул, у которых в предварённой форме число перемен кванторов ограничено некоторой фиксированной величиной. Актуальность исследования таких алгоритмов объясняется их тесной связью со многими прикладными вопросами, в частности, с исследованием систем алгебраических уравнений.

Использование базисов Грёбнера является весьма общим методом решения многих задач, связанных с системами алгебраических уравнений над алгебраически замкнутым полем [5]. История их возникновения и, в

частности, вклад в развитие теории выдающегося российского математика А.И. Ширшова описан в [6]. Алгоритмы вычисления базисов Грёбнера входят во многие пакеты для символьных вычислений, включая Maple и Singular. Однако применение этих методов часто оказывается малоэффективным из-за появления в ходе вычислений многочленов очень высокой степени [7–9]. Время работы соответствующих алгоритмов дважды экспоненциальное или ещё выше.

Существуют другие методы, не связанные с нахождением базисов Грёбнера и позволяющие определить совместность системы алгебраических уравнений с рациональными коэффициентами за экспоненциальное время. Впервые эта возможность была показана в работе [10], в дальнейшем метод был немного усовершенствован [11]. Наряду с этим развивались вероятностные алгоритмы [12–14]. Однако все известные вероятностные методы решения систем уравнений также требуют экспоненциального времени в общем случае. Хотя недавно для решения этой задачи описан эффективный вероятностный алгоритм, имеющий низкую сложность при некоторых дополнительных ограничениях на число мономов в уравнениях [14].

В работе [15] найден разрешающий алгоритм для формул в предварённой форме с ограниченным числом перемен кванторов, время работы которого экспоненциально зависит от длины формулы, но дважды экспоненциально – от числа перемен кванторов.

Напомним вкратце строение так называемой полиномиальной иерархии языков PH [1]. Она и другие ей подобные иерархии были введены для более точной классификации проблем по сложности их решения, так как каждую разумно поставленную проблему, ответ на которую может быть только «да» или «нет», можно сформулировать в терминах принадлежности к соответствующему языку.

Нижним (нулевым) уровнем этой иерархии объявляется класс языков распознаваемых детерминированными машинами Тьюринга за полиномиальное время. Таким образом, языки этого класса считаются наиболее легко распознаваемыми. Насколько оправдана подобная точка зрения, мы обсудим позднее. Следующий, первый, уровень иерархии состоит из двух классов языков. Языки одного класса, обозначаемого как P-Сигма-1, распознаются недетерминированными машинами Тьюринга за полиномиальное время, а другой класс – P-Пи-1 содержит все дополнения до языков первого, т.е. это просто классы NP и coNP, соответственно. Если уже определены классы уровня k, то уровень k+1 состоит из двух подуровней. На «нижнем» располагается класс P-Дельта-(k+1), языки которого распознаются детерминированными машинами Тьюринга за полиномиальное время, с использованием языка L из класса P-Сигма-k в качестве оракула, т.е. «подсказчика», который может сказать мгновенно, принадлежит ли данное слово языку L. «Верхний» подуровень состоит из двух классов языков. В первом из них – P-Сигма-(k+1) собраны все языки,

распознаваемые недетерминированными машинами Тьюринга за полиномиальное время, тоже с использованием языка L из класса P-Сигма-k в качестве оракула. Во втором, P-Пи-(k+1) – все дополнения до языков первого класса. Верно ли подуровни названы «верхним» и «нижним», до сих пор неизвестно, вполне вероятно, что при достаточно больших k (два или более) все классы иерархии PH совпадают.

Объединение всех классов языков, входящих в какие-то уровни, описанные выше, называют PH иерархией.

По аналогии с полиномиальной иерархией PH [16] определяется экспоненциальная иерархия EH классов сложности, нулевой уровень которой состоит из языков, разрешимых за экспоненциальное время poly(exp(n)), где число n означает длину входа. Хотя это не доказано, широко распространено мнение о том, что иерархия EH невырожденная. Также рассматривается иерархия EXP-H, нулевой уровень которой состоит из языков, разрешимых за время exp(poly(n)). Аналогично определяется иерархия DoubleEXP-H для дважды экспоненциального времени.

Отметим, что вырождение полиномиальной иерархии PH влечёт вырождение других аналогичных иерархий. Доказательство основано на методе, называемом набивкой или накачкой. Однако обратная импликация не доказана.

Покажем, что равенство классов P-space=EXP влечёт равенство классов EXP-space=DoubleExp. Здесь множество из EXP-space допускается с использованием памяти exp(poly(n)), где число n означает длину входа. Множество из DoubleExp допускается за время exp(exp(poly(n))). Очевидно, любое множество класса EXP-space распознаваемо за дважды экспоненциальное время. Пусть P-space=EXP. Рассмотрим множество X слов в алфавите 0 и 1, распознаваемое за дважды экспоненциальное время $t(x)$ алгоритмом A. Обозначим Y множество слов с префиксом из log $t(x)$ нулей, единицы и слова x. В слове из Y суффикс x однозначно восстанавливается по слову из Y: это символы правее самой левой единицы. Очевидная модификация алгоритма A допускает множество Y за экспоненциальное от длины входа время. По предположению множество Y принадлежит P-space. Следовательно, Y допускается алгоритмом, требующим памяти, экспоненциально ограниченной длиной суффикса x. Поскольку слова из Y однозначно определяются своими суффиксами x, составляющими множество X, то таким образом, X принадлежит классу EXP-space.

Известно частичное вырождение иерархии AM, отражающей интерактивные взаимодействия с конечным числом раундов между вероятностной машиной (Артуром), работающей полиномиальное время, и машиной с неограниченными ресурсами (Мерлином) [17]. Неформально, Артур должен узнать истину, ведя диалог с Мерлином, обладающим гораздо большими возможностями, но при этом, проверяя, не обманывает ли его Мерлин. Конечное число раундов можно свести к частному случаю, когда Мерлин даёт все ответы сразу. При этом посредством диалога с

полиномиальным числом перемежений вопросов и ответов можно моделировать работу произвольного алгоритма с полиномиально ограниченной памятью. Важное отличие AM от PH состоит в использовании Артуром вероятностного алгоритма. По аналогии с этим результатом можно было бы ожидать, что иерархия PH тоже вырождена и класс NP совпадает с двойственным классом coNP. Однако многочисленные попытки доказать или опровергнуть это утверждение не привели к успеху.

Для всякого сложностного класса языков, т.е. класса, выделяемого на основании «одинаковости» временной или ёмкостной сложности алгоритмов, которые распознают языки этого класса, важной характеристикой служат полные в этом классе языки. Такой язык L должен, во-первых, сам принадлежать этому классу, во-вторых, для каждого языка M из этого класса вопрос о принадлежности слов языку M должен полиномиально сводиться к аналогичному вопросу для языка L. Таким образом, полный для сложностного класса язык полностью его характеризует относительно сложности вычислений, можно, поэтому сказать, что полный в данном классе язык – это его паспорт.

Ярким примером этому может служить класс NP, для него известно очень много полных языков [1]. В их число входят языки, соответствующие таким признано сложным задачам, как задача о существовании гамильтонова цикла, задачи о выполнимости формул исчисления высказываний и о возможности правильно раскрасить вершины графа в k цветов и многие другие широко известные задачи.

Стоит отметить, что одними такими важными для практики задачами список известных полных проблем для класса NP не исчерпывается. В последнее время он активно пополняется за счёт классических задач алгебры. Например, таковой является задача о вычислении геодезической длины элементов в свободной разрешимой группе ступени 2 и фиксированного ранга [18]. В то же время для некоторых, казалось бы, очень тесно связанных с этой задачей проблем равенства, сопряженности и степени имеются алгоритмы полиномиальной сложности [18]. Более того, эти алгоритмы являются полиномиальными не только от длины исследуемых слов, но также и от ранга и ступени разрешимости свободной разрешимой группы, что сильно контрастирует с давно известными алгоритмами для решения этих задач, основанными на вложении Магнуса. Недавно эти детерминированные полиномиальные алгоритмы удалось заметно упростить [19], интересно, что вероятностные аналоги этих алгоритмов, которые описаны там же, имеют в качестве верхней границы сложности многочлены, степени которых лишь на единицу меньше, чем у детерминированных алгоритмов.

Наличие полных языков для некоторых сложностных классов является открытой проблемой. Например, существование полного языка во всей иерархии PH равносильно тому, что она имеет только конечное число уровней, т.е. она является почти вырожденной.

В отличие от этого, уровни полиномиальной иерархии PH допускают простую характеристику на основе полных языков в каждом классе. Примеры полных языков из второго P-Дельта-класса можно найти в [20]. Для классов P-Сигма-k и P-Пи-k таковыми служат классы предварённых формул с соответствующим числом перемен кванторов в теории чистого равенства. Вся же теория чистого равенства является полной для класса P-space [1], и неизвестно принадлежит ли она иерархии PH. В последнем случае она была бы полной и там.

Отметим, что если иерархия PH (или аналогичная ей) не вырождена, то помимо «стандартных» уровней иерархии, существуют и промежуточные классы. Аналогичная ситуация наблюдается в теории тьюринговых степеней неразрешимости, которой посвящено значительное количество публикаций, включая [21]. Можно ожидать, что существует много языков, которые принадлежат некоторому уровню иерархии, но не полны в нём и не принадлежат вложенным уровням. Тем не менее, известно лишь немного кандидатов из класса NP, для которых не доказана ни полиномиальная разрешимость, ни NP-полнота. Один из таких языков состоит из пар изоморфных графов.

Известный результат [15] показывает, что формулы с ограниченным числом перемен кванторов в теории поля комплексных чисел разрешимы алгоритмами экспоненциального времени, хотя это время зависит от числа перемен кванторов. Это может служить косвенным указанием на то, что либо экспоненциальная иерархия EXP-H вырождена, либо сложность фрагментов с ограниченным числом перемен кванторов у теории поля комплексных чисел существенно ниже, чем у известных в настоящее время алгоритмов разрешения. Последнее обстоятельство может иметь важное теоретическое и практическое значение.

С другой стороны, даже совместность систем алгебраических уравнений с целыми коэффициентами, которая выражается в теории полей экзистенциальной формулой, является NP-трудной задачей. А именно, NP-полную задачу о разбиении множества целых чисел на две части с одинаковыми суммами за полиномиальное время можно свести к задаче распознавания особой точки на гиперповерхности в пространстве достаточно большой размерности. Отметим, что при фиксированной размерности эта задача эффективно разрешима за время, полиномиально зависящее от степени гиперповерхности [22].

Вернёмся к вопросу о том, почему принято считать, что полиномиальные алгоритмы являются быстрыми. Для обоснования этого часто ограничиваются простым указанием на тот факт, что экспонента с любым основанием b большим единицы и показателем, линейно зависящим от аргумента n, станет больше значения любого многочлена $f(n)$ при всех n, начиная с некоторого значения m, зависящего от b и f. Поэтому при всех входах, чья длина n больше m, алгоритм с верхней оценкой времени $f(n)$ будет работать быстрее алгоритма с экспоненциальной

оценкой. То же верно, например, для субэкспоненциальной функции $n^{\log(n)}$. Это теоретическое обоснование не всегда согласуется с практикой, поскольку иногда экспоненциальные алгоритмы работают быстрее полиномиальных даже на достаточно длинных входах.

Одна из причин этого в следующем. При подсчёте времени работы берутся во внимание только «внешние» действия программы, а именно, сколько и каких операций произвела машина с исходными данными и теми, что хранятся в оперативной памяти (к примеру, сложений, вычитаний, умножений, сравнений, пересылок из одних ячеек памяти в другие и т.п.). Аналогом этому для машин Тьюринга служит подсчёт числа стираний-записываний и сдвигов головки. Но в действительности время работы тратится не только на эти операции, но и на поиск нужной команды. Почти то же самое происходит и в реальной вычислительной машине. Кроме того, часто полиномиальность алгоритма достигается разбором конечного и фиксированного числа случаев, и написанием для каждого из этих частных случаев своей подпрограммы. Например, для многих классов графов известны полиномиальные алгоритмы, определяющие, изоморфны ли данные графы рассматриваемого класса: для деревьев, для графов, у которых вершины имеют степени не выше второй и т.д.

Для более адекватного описания сложности программ нужно ввести понятие комбинированной (или агрегированной) меры сложности алгоритма, которая учитывала бы и «внешнюю» и «внутреннюю» его сложность. Или точнее: нужно учитывать не только число шагов на ленте, но также и время поиска в программе очередной применимой команды, которое определяется сложностью описания (строения) всей программы, тогда многое станет на своё место. Однако если брать при этом в расчёт только длину программы, то этого будет явно не достаточно.

Работа выполнена при частичной поддержке Комитета науки МОН РК (грант 0726/ГФ) и Российского фонда фундаментальных исследований (проект 13-04-40196-Н).

Литература

1. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. – М.: Мир, 1982. – 416с.
2. Heintz J. Definability and fast quantifier elimination in algebraically closed fields // Theoretical Computer Science. – 1983. – V.24. – P.239–277.
3. Fürer M. The complexity of Presburger arithmetic with bounded quantifier alternation depth // Theoretical Computer Science. – 1982. – V.18. – P.105–111.
4. Верещагин Н.К. Новое доказательство разрешимости элементарной теории линейно упорядоченных множеств // Математические заметки. – 1990. – V.47, N 5. – P.31–38.
5. Кокс Д., Литтл Дж., О'Ши Д. Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. – М.: Мир, 2000. – 687 с.
6. Bokut L.A., Chen Y. Gröbner–Shirshov bases and their calculation // Bulletin of Mathematical Sciences. – 2014. doi: 10.1007/s13373-014-0054-6.
7. Mayr E.W., Meyer A.R. The complexity of the word problems for commutative semigroups and polynomial ideals // Advances in Mathematics. – 1982. – V.46, N 3. – P.305–329.
8. Чистов А.Л. Дважды экспоненциальная нижняя оценка на степень системы образующих

полиномиального простого идеала // Алгебра и анализ. – 2008. – Т.20, № 6. – С.186–213.
9. Mayr E.W., Ritscher S. Dimension-dependent bounds for Gröbner bases of polynomial ideals // Journal of Symbolic Computation. – 2013. – V. 49. – P.78–94.
10. Чистов А.Л. Алгоритм полиномиальной сложности для разложения многочленов и нахождение компонент многообразия в субэкспоненциальное время // Записки научных семинаров ЛОМИ. – 1984. – Т.137. – С.124–188.
11. Chistov A.L. An improvement of the complexity bound for solving systems of polynomial equations // Записки научных семинаров ПОМИ. – 2011. – Т. 390. – С.299–306.
12. Schwartz J.T. Fast probabilistic algorithms for verification of polynomial identities // Journal of the ACM – 1980. – V.27. – P.701–717.
13. Giusti M., Lecerf G., Salvy B. A Gröbner free alternative for polynomial system solving // Journal of Complexity – 2001. – V17. – P.154–211.
14. Herrero M.I., Jeronimo G., Sabia J. Affine solution sets of sparse polynomial systems // Journal of Symbolic Computation – 2013. – V.51. – P.34–54.
15. Григорьев Д.Ю. Сложность разрешения теории первого порядка алгебраически замкнутых полей // Известия АН СССР. Сер. матем. – 1986. – Т.50, № 5. – С.1106–1120.
16. Wrathall C. Complete sets and the polynomial-time hierarchy // Theoretical Computer Science. – 1977. – V.3. – P.23–33.
17. Babai L. Trading group theory for randomness // Proceedings of the 17th ACM Symposium on Theory of Computing (STOC). – 1985. – P. 421–429.
18. Miasnikov A.G., Romankov V., Ushakov A., Vershik A. The word and geodesic problems in free solvable groups // Transactions of the American Mathematical Society. – 2010. – V.362, №9. – P.4655–4682.
19. Ushakov A. Algorithmic theory of free solvable groups: Randomized computations // Journal of Algebra. – 2014. – V. 407. – P. 178–200.
20. Deineko V.G., Klinz B., Weginger G.J. Uniqueness in quadratic and hyperbolic 0–1 programming problems // Operations Research Letters. – 2013. – V.41. – P. 633–635.
21. Арсланов М.М. Определимые отношения в структурах тьюринговых степеней // Известия высших учебных заведений. Математика. - 2014. - № 2. - С.77–81.
22. Селиверстов А.В. О перечислении особых точек на аффинной гиперповерхности // Математика в современном мире. Материалы Международной конференции, посвященной 150-летию Д.А. Граве. – Вологда: ВГПУ. – 2013. – С.35.