О сложности фрагментов теории поля комплексных чисел

И.В. Латкин
Восточно-Казахстанский государственный технический университет им. Д. Серикбаева

А.В. Селиверстов
Институт проблем передачи информации им. А.А. Харкевича РАН

- **David Hilbert** (1893) Nullstellensatz
- **Alfred Tarski** (1930) Разрешимость теории поля комплексных чисел.
- **Wolfgang Gröbner** (1950 – кольца коммутативных полиномов), **Анатолий Илларионович Ширшов** (1962 – алгебры Ли), **Хэ́йсукэ Хиронака** (1964 – локальные кольца) Определение базиса Грёбнера.
- **Bruno Buchberger** (1965) Алгоритм вычисления базиса Грёбнера.
- **Ernst W. Mair, Albert R. Meyer** (1982) Дважды экспоненциальная нижняя оценка степеней многочленов базиса Грёбнера биномиального идеала.
- **J. Heintz** (1982) Элиминация кванторов в теории поля комплексных чисел выполнима за дважды экспоненциальное время и требует как минимум экспоненциальной памяти.
- **Александр Леонидович Чистов** (1984) Совместность системы уравнений проверяется за экспоненциальное время.
- **Дмитрий Юрьевич Григорьев** (1986) Доказательство формул с ограниченным числом перемен кванторов за экспоненциальное время.

L.A. Bokut, Y. Chen. Gröbner–Shirshov bases and their calculation // Bulletin of Mathematical Sciences. – 2014. doi: 10.1007/s13373-014-0054-6

Утверждение Существует алгоритм, строящий по всякой формуле теории первого порядка алгебраически замкнутых полей эквивалентную ей бесквантворную за время $\exp((\log_c L)n^{2k+1})$, где c – константа, L – размер формулы, n – число переменных, k – число перемен кванторов.

В частности, проверка принадлежности 1 идеалу выполнима за экспоненциальное время (число перемен кванторов в формуле $k = 1$), а при фиксированном числе переменных n – за полиномиальное время.

Д. Ю. Григорьев. Сложность разрешения теории первого порядка алгебраически замкнутых полей // Известия АН СССР. 1986. Сер. матем., Т.50, № 5. С.1106–1120

А.Л. Чистов. Алгоритм полиномиальной сложности для разложения многочленов и нахождение компонент многообразия в субэкспоненциальное время // Записки научных семинаров ЛОМИ. 1984. Т.137. С.124–188

A.L. Chistov. An improvement of the complexity bound for solving systems of polynomial equations // Записки научных семинаров ПОМИ. 2011. Т. 390. С.299–306

Нижним (нулевым) уровнем полиномиальной иерархии **PH** служит класс языков, распознаваемых детерминированными машинами Тьюринга за полиномиальное время.

Первый, уровень иерархии состоит из двух классов языков. Языки одного класса, обозначаемого как Σ_1^P, распознаются недетерминированными машинами Тьюринга за полиномиальное время, а другой класс – Π_1^P содержит все дополнения до языков первого, т.е. это классы NP и coNP. Если уже определены классы уровня k, то уровень k+1 состоит из двух подуровней. На нижнем располагается класс Δ_{k+1}^P, языки которого распознаются детерминированными машинами Тьюринга за полиномиальное время, с использованием языка L из класса Σ_k^P в качестве оракула, который может сказать мгновенно, принадлежит ли данное слово языку L. Верхний подуровень состоит из двух классов языков. В первом из них – Σ_{k+1}^P собраны все языки, распознаваемые недетерминированными машинами Тьюринга за полиномиальное время, тоже с использованием языка L из класса Σ_k^P в качестве оракула. Во втором, Π_{k+1}^P – все дополнения до языков первого класса.

Утверждение Существует алгоритм, строящий по всякой формуле чистой теории равенства эквивалентную ей бескванторную, используя полиномиально ограниченную память. Доказуемые формулы с k переменами кванторов образуют множество из k-го уровня полиномиальной иерархии.

В частности, доказуемые экзистенциальные формулы составляют NP-полное множество.

C. Wrathall. Complete sets and the polynomial-time hierarchy // Theoretical Computer Science. 1977. V.3. P.23–33

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 экспоненциальная иерархия EXP-H вырождена.

Далее рассматриваются проективные гиперповерхности, которые заданы формами с коэффициентами из конечного алгебраического расширения поля рациональных чисел.
Элементы конечного алгебраического расширения можно отождествить с многочленами ограниченной степени над полем рациональных чисел.
Арифметические операции над этим полем сводятся к операциям над целыми числами, размер которых ограничен полиномом от длин записей исходных алгебраических чисел.

Покажем, что задача о распознавании гиперплоскости, на которой не лежит никакая вершина многомерного куба, сводится к проверке гладкости комплексной проективной гиперповерхности нечётной степени, начиная с третьей. Это говорит о вычислительной трудности проверки гладкости таких гиперповерхностей, хотя для квадрики гладкость проверяется легко.

Назовем (-1, 1)-точкой всякую точку в проективном пространстве, чьи однородные координаты равны -1 или 1 с точностью до общего ненулевого множителя. Это вершины многомерного куба. Проверка принадлежности некоторой (-1, 1)-точки к данной гиперплоскости является NP-полной задачей.

Теорема Для любого нечётного числа d, начиная с трёх, существует детерминированный алгоритм, который получает на вход гиперплоскость H, заданную линейной формой от n переменных, где n не меньше трёх, и за полиномиальное время выдает такую гиперповерхность S степени d, что особые (-1, 1)-точки на S взаимно однозначно соответствуют (-1, 1)-точкам, лежащим на H.

Сечение кубической гиперповерхности $x^3+y^3-z^3-t^3-w^3=0$ Гиперплоскостью $x+y-z-t-w=0$. Гиперплоскость не проходит через (-1,1)-точки. Сечение гладкое.

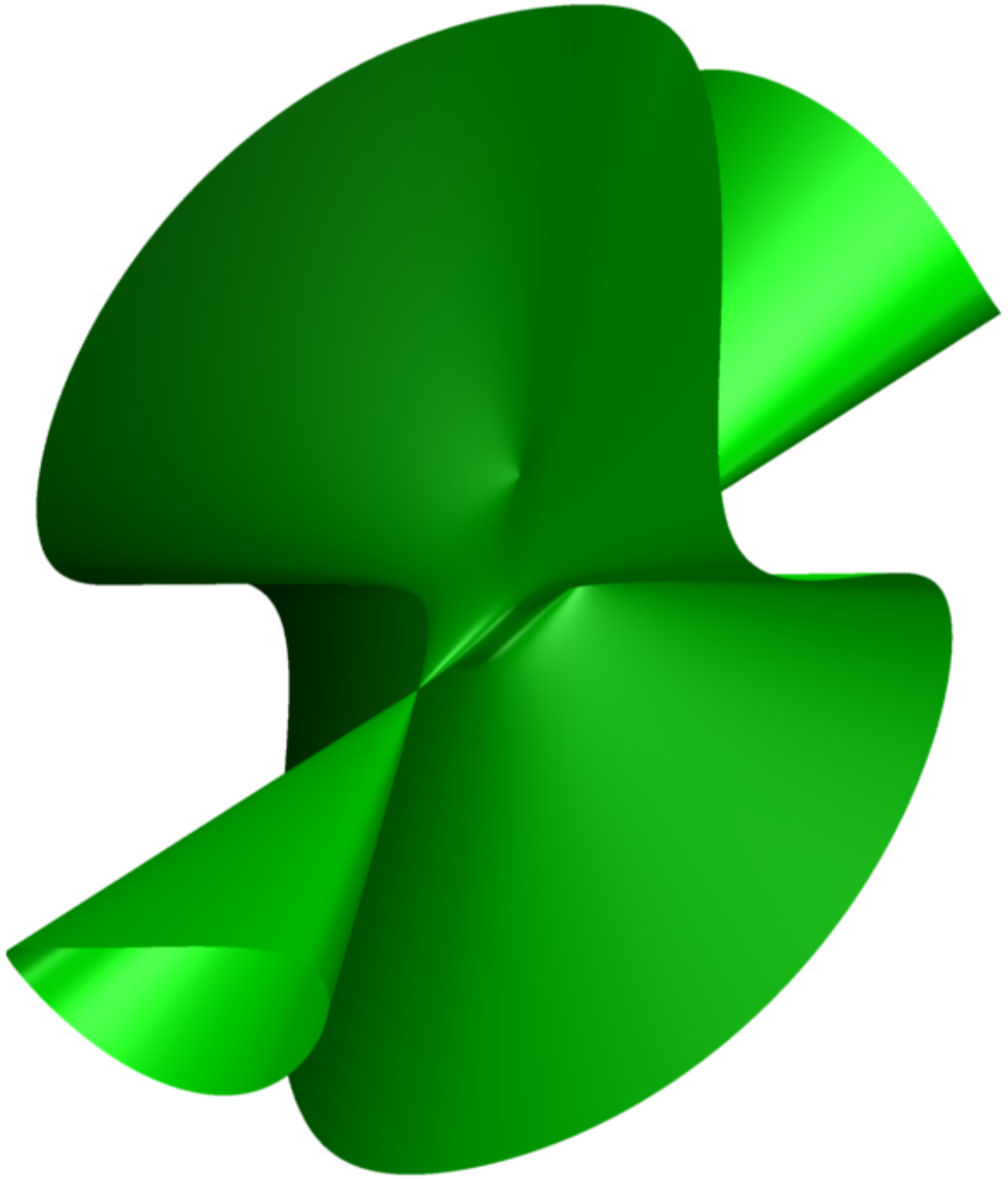
Нарисовано в Surfer

http://imaginary.org/program/surfer

Сечение кубической гиперповерхности $2x^3+y^3-z^3-t^3-w^3=0$ Гиперплоскостью $2x+y-z-t-w=0$. Гиперплоскость проходит через (-1,1)-точки. Сечение особое.

Нарисовано в Surfer

http://imaginary.org/program/surfer



Сечение кубической гиперповерхности $3x^3+y^3-z^3-t^3-w^3=0$ Гиперплоскостью $3x+y-z-t-w=0$. Гиперплоскость не проходит через (-1,1)-точки. Сечение гладкое.

Нарисовано в Surfer

http://imaginary.org/program/surfer

Следствие. Для любого нечётного числа d, начиная с трёх, множество гиперповерхностей степени d в конечномерных пространствах над конечным алгебраическим расширением поля рациональных чисел, содержащих особую (-1, 1)-точку, NP-полное.

Доказательство. Рассматриваемое множество гиперповерхностей принадлежит классу NP, поскольку недетерминированно угадав (-1, 1)-точку, за полиномиальное время можно проверить, является ли эта точка особой. Полнота в классе NP следует из предыдущей теоремы.

Спасибо за внимание

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