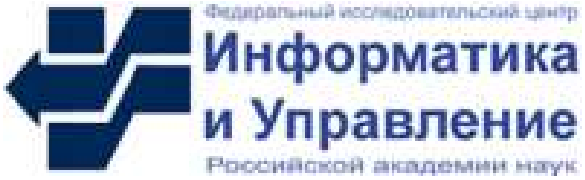
КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы международной конференции

Москва, 30 октября – 3 ноября 2017 г.



КОМПЬЮТЕРНАЯ АЛГЕБРА

The Ministry of Education and Science
of the Russian Federation
Plekhanov Russian University of Economics

Institution of Russian Academy of Sciences
Dorodnicyn Computing Centre of
Federal Research Center
"Computer Science and Control" of RAS

COMPUTER ALGEBRA

International Conference Materials

Moscow, October 30 – November 3, 2017

Moscow
PRUE
2017

Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Российский экономический университет имени Г. В. Плеханова»
(ФГБОУ ВО «РЭУ им. Г. В. Плеханова»)

Федеральное государственное учреждение
«Федеральный исследовательский центр «Информатика и управление»
Российской академии наук»
Вычислительный центр им. А. А. Дородницына

КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы Международной конференции

Москва, 30 октября — 3 ноября 2017 г.

Москва
ФГБОУ ВО «РЭУ им. Г. В. Плеханова»
2017

UDC 519.6(063)
BBC 22.19я431
K637

Responsible editors:
Doctor of Physical and Mathematical Sciences S. A. A b r a m o v
Doctor of Physical and Mathematical Sciences T. M. S a d y k o v

Reviewers: PhD Yu. O. T r u s o v a, PhD K. P. L o v e t s k i y

It is printed in author's edition

Computer algebra : International Conference Materials. Moscow, October 30 – November 3, 2017 / ed. S. A. Abramov, T. M. Sadykov. – Moscow : Plekhanov Russian University of Economics, 2017. – 173 c.
ISBN 978-5-7307-1266-9

The International conference is organized jointly by Dorodnicyn Computing Center of Federal Research Center "Computer Science and Control" of RAS and Plekhanov Russian University of Economics with a support of Russian Foundation for Basic Research, grant no. 17-01-20398\17. The talks presented at the conference discuss actual problems of computer algebra – the discipline whose algorithms are focused on the exact solution of mathematical problems using a computer.

For scientists, graduate and undergraduate students in mathematics, physics and computer science.

UDC 519.6(063)
BBC 22.19я431

ISBN 978-5-7307-1266-9

УДК 519.6(063)
ББК 22.19я431
К637

Ответственные редакторы:
д-р физ.-мат. наук С. А. А б р а м о в
д-р физ.-мат. наук Т. М. С а д ы к о в

Рецензенты: канд. техн. наук Ю. О. Т р у с о в а
канд. физ.-мат. наук К. П. Л о в е ц к и й

Печатается в авторской редакции

К637 **Компьютерная алгебра** : материалы Международной конференции. Москва, 30 октября – 3 ноября 2017 г. / отв. ред. С. А. Абрамов, Т. М. Садыков. – Москва : ФГБОУ ВО «РЭУ им. Г. В. Плеханова», 2017. – 173 с.
ISBN 978-5-7307-1266-9

Международная конференция проводится совместно Вычислительным центром им. А. А. Дородницына ФИЦ «Информатика и управление» РАН и Российским экономическим университетом имени Г. В. Плеханова при поддержке РФФИ, проект № 17-01-20398\17. В представленных на конференции докладах обсуждаются актуальные проблемы компьютерной алгебры – научной дисциплины, алгоритмы которой ориентированы на точное решение математических задач с помощью компьютера.

Для научных работников, аспирантов и студентов физико-математических и технических специальностей.

УДК 519.6(063)
ББК 22.19я431

ISBN 978-5-7307-1266-9

УДК 510.52

Поиск точек на гладкой кубической гиперповерхности

А. В. Селиверстов

Институт проблем передачи информации им. А.А. Харкевича Российской академии наук,
Большой Каретный переулок, д.19, стр. 1, Москва, Россия, 127051

Email: slvstv@iitp.ru

Хорошо известно, что гладкая проективная кубическая гиперповерхность размерности два или выше с отмеченной точкой над некоторым полем характеристики нуль унирациональна над этим полем. Следовательно, множество точек гиперповерхности над этим полем всюду плотное в топологии Зарисского. Рассмотрена вычислительная сложность поиска этих точек. Показано, что доминантное рациональное отображение из проективного пространства в гиперповерхность можно вычислить вероятностным алгоритмом, работающим без ошибок, который с высокой вероятностью завершает работу, делая лишь полиномиально ограниченное число арифметических операций над полем. В общем случае образ этого рационального отображения содержит не все точки над этим полем, но лишь большой набор таких точек. В частности, вычисление таких точек над конечным расширением поля рациональных чисел позволяет отказаться от аппроксимации вещественных или комплексных чисел, но использовать больше возможностей символьных вычислений. Эта задача тесно связана с подтверждением гладкости гиперповерхности и могут быть использованы для решения некоторых комбинаторных задач. Ранее И.В. Латкин и автор показали, что задача о разбиении множества сводится к задаче поиска особых точек на кубической гиперповерхности. Рациональная параметризация поверхностей используется в компьютерной графике.

Ключевые слова: кубическая гиперповерхность, рациональное отображение, вычислительная сложность.

1. Введение

Многообразие X унирационально над полем K, если его поле рациональных функций $K(X)$ вкладывается в чисто трансцендентное расширение поля K. Существование такого вложения полей эквивалентно существованию доминантного рационального отображения $\mathbb{P}^m \dashrightarrow X$, определённого над полем K, где $m = \dim X$. Рациональное отображение обозначено символом $\dashrightarrow$, поскольку оно определено лишь на открытом всюду плотном множестве.

Гладкая кубическая гиперповерхность размерности не меньше двух, определённая над некоторым полем K, унирациональна над K тогда и только тогда, когда ей принадлежит некоторая K-точка [1]. Для гладких поверхностей над полем рациональных чисел это доказал Сегре [2]. В случае бесконечного поля K, если существует K-точка, то множество K-точек всюду плотное в топологии Зарисского. В общем случае унирациональность над полем K позволяет найти не все K-точки, но лишь большой набор K-точек.

Многообразие рационально над полем K, если поле рациональных функций изоморфно чисто трансцендентному расширению поля K. Гладкая кубическая кривая на плоскости и гладкая трёхмерная гиперповерхность в $\mathbb{P}^4$ иррациональные [3]. Кубическая поверхность в $\mathbb{P}^3$ рациональна над полем комплексных чисел. Однако над полем вещественных чисел гладкая проективная поверхность, имеющая две вещественные компоненты связности, иррациональная. Рациональная параметризация поверхностей используется в компьютерной графике [4, 5]. Для поверхности вычисление параметризации сводится к вычислению базиса Грёбнера полиномиального идеала, например, с помощью программ для символьных вычислений, включая облачный сервис MathPartner [6]. Однако с увеличением размерности сложность такого вычисления может быстро расти [7]. Это объясняет интерес к изучению вычислительной сложности поиска точек на гиперповерхности большой размерности. В частности, он связан с распознаванием гладкости гиперповерхности [8] и может применяться для решения комбинаторных задач [9].

2. Обозначения и предварительные сведения

Фиксируем счётное поле K характеристики нуль с нумерацией, при которой арифметические операции $+$, $-$, $\times$ и $(\cdot)^{-1}$ вычислимы за полиномиальное время. Примером такого поля служит конечное расширение поля рациональных чисел, элементы которого представимы многочленами ограниченной степени с рациональными коэффициентами, а для записи числителя и знаменателя дроби используется двоичная запись. Элементы конечного расширения поля рациональных чисел представимы многочленами ограниченной степени с рациональными коэффициентами; арифметические операции над таким полем подразумевают вычисление остатков от деления многочленов. В сервисе MathPartner это выполнимо посредством команды reduceByGB. В общем случае, если два поля, в каждом из которых операции вычислимы за полиномиальное время, изоморфны друг другу, не существует изоморфизма, вычислимого за полиномиальное время [10]. Поэтому, говоря о расширении поля L/K, мы подразумеваем, что операции в поле L также вычислимы за полиномиальное время, более того, существует полиномиально вычислимый изоморфизм между полем K и подполем поля L. Выполнимость этого условия зависит от выбора нумерации полей.

Отождествим проективное пространство $\mathbb{P}^n$ с множеством одномерных линейных подпространств в K^{n+1}. Обозначаем через $(x_0 : \cdots : x_n)$ однородные координаты в $\mathbb{P}^n$. Фиксируем такую нумерацию векторов из K^{n+1}, при которой сложение и умножение на элементы поля K выполняются за полиномиальное время. Говоря о вычислениях с точками из $\mathbb{P}^n$, мы подразумеваем вычисления с некоторыми векторами из K^{n+1}, соответствующими этим точкам. Для краткости мы будем оценивать сложность вычислений количеством арифметических операций над полем K. Эта оценка отличается от числа шагов некоторой машины Тьюринга лишь множителем, ограниченным некоторым многочленом от длины входа.

Дискриминант многочлена степени d от одной переменной над полем комплексных чисел равен нулю, если некоторый корень кратный. Дискриминант сам является однородным многочленом с целыми коэффициентами от всех коэффициентов исходного многочлена. Дискриминант многочлена $at^3 + bt^2 + pt + q$ равен $b^2p^2 - 4ap^3 - 4b^3q - 27a^2q^2 + 18abpq$. Дискриминант формы $g(s,t)$ от двух переменных степени d равен дискриминанту любого из двух многочленов от одной переменной $g(1,t)$ и $g(s,1)$, вычисляемому по формуле для степени d. Если степень неоднородного многочлена меньше d, то он формально рассматривается как многочлен степени d, а старшие коэффициенты принимаются равными нулю. Поскольку форма $g(s,t)$ определяет d точек на проективной прямой $\mathbb{P}^1$, её дискриминант обращается в нуль, если среди этих точек есть совпадающие.

Обозначим через $\overline{K}$ алгебраическое замыкание поля K. Заданная уравнением $f = 0$ гиперповерхность гладкая, если частные производные $\frac{\partial f}{\partial x_i}$ не обращаются одновременно в нуль над полем $\overline{K}$, когда некоторая переменная отлична от нуля.

Лемма 1 *Дана гладкая гиперповерхность $X \subset \mathbb{P}^n$ степени не ниже второй, где $n \geqslant 4$. Размерность линейного подпространства $Y \subset X$ строго меньше $\frac{n}{2}$.*

Доказательство. Обозначим через f форму, определяющую X. Поскольку X неприводимая и отлична от гиперплоскости, каждая частная производная $\frac{\partial f}{\partial x_i}$ не равна тождественно константе. Без ограничения общности можно считать, что подпространство Y задано уравнениями $x_{k+1} = x_{k+2} = \cdots = x_n = 0$, где $k = \dim Y$. Тогда при всех значениях индекса $i \leqslant k$ частные производные $\frac{\partial f}{\partial x_i}$ обращаются в нуль на Y. Если число $n - k$ оставшихся частных производных не превышает размерности k подпространства Y, то они имеют нетривиальный общий нуль на Y, который соответствует особой $\overline{K}$-точке гиперповерхности X. Следовательно, $2k < n$. □

Обозначим через T_p проективную касательную гиперплоскость к гиперповерхности X в точке p. Обозначим через C_p сечение гиперповерхности X гиперплоскостью T_p.

Лемма 2 *Дана гладкая кубическая гиперповерхность $X \subset \mathbb{P}^n$, где $n \geqslant 4$. Для любой точки $p \in X$ гиперплоское сечение C_p неприводимое.*

Доказательство. Гиперплоское сечение гиперповерхности определяется одной кубической формой. Если эта форма приводимая, то один из её делителей — линейная форма. В этом случае на гиперповерхности лежит линейное подпространство размерности $n-2$. При $n \geqslant 4$ это противоречит лемме 1. □

Плоское сечение гладкой кубической поверхности может быть приводимым, поскольку над алгебраически замкнутым полем на такой поверхности лежат 27 прямых. Поэтому мы ограничимся случаем $n \geqslant 4$, чтобы избежать проверки условий, истинных в высоких размерностях в силу леммы 2.

Лемма 3 *Дана гладкая кубическая гиперповерхность $X \subset \mathbb{P}^n$, где $n \geqslant 4$. Общая точка $p \in X$ служит двойной точкой гиперплоского сечения C_p.*

Доказательство. Точка p может быть двойной или тройной особой точкой сечения C_p. Если p тройная, то C_p — это конус с вершиной p. Это верно и для сечения общей плоскостью. Но сечение конуса плоскостью, проходящей через его вершину и не лежащей целиком на конусе, состоит из объединения прямых. По теореме Бертини, сечение гиперповерхности X общей плоскостью — это гладкая кубическая кривая. Следовательно, для общей точки p сечение C_p не является конусом. □

Свойство, истинное в общей точке, истинно с большой вероятностью в случайно выбранной точке. Для оценки этой вероятности мы будем использовать лемму Шварца–Зиппеля [11].

Лемма Шварца–Зиппеля *Даны многочлен $f \in K[x_0, \ldots, x_n]$ полной степени d и конечное множество $S \subset K$ мощности $|S|$. Если случайные величины $r_0, \ldots, r_n$ независимы и равномерно распределены на множестве S, то вероятность* $\Pr[f(r_0, \ldots, r_n) = 0] \leqslant \frac{d}{|S|}$.

Работая с полями характеристики нуль, удобно в качестве S использовать положительные целые рациональные числа из некоторого интервала. Если случайные числа собираются из независимых бернуллиевских случайных величин (случайных битов), то мощность множества S должна быть степенью двойки. Увеличение мощности не ухудшает оценку вероятности в лемме Шварца–Зиппеля и получаемых на её основе результатов. Поэтому множество $S = \{1, \ldots, N\}$ можно заменить на множество $\{1, \ldots, 2^{\lceil \log_2 N \rceil}\}$, увеличивая мощность менее чем в два раза. Далее такая возможность явно не оговаривается, но может использоваться для реализации алгоритмов. Широко применяются различные псевдослучайные последовательности, однако трудно строго обосновать достижимость ожидаемого результата. Обсуждение генераторов псевдослучайных чисел выходит за рамки этой работы. Допуская некоторую вольность, мы не будем последовательно различать случайную величину и реализацию этой случайной величины. По сути, вероятностный алгоритм получает на вход конкретную реализацию случайной величины.

Рассмотренные алгоритмы используют решение систем линейных уравнений. Здесь точная оценка сложности сама может служить темой для большой работы. Однако алгоритмы, асимптотически более эффективные, чем метод Гаусса, обычно не используются на практике. С другой стороны, в MathPartner решение системы линейных уравнений выполнимо одной командой solve.

3. Основная часть

Лемма 4 *Даны гладкая кубическая гиперповерхность $X \subset \mathbb{P}^n$, определённая формой $f(x_0, \ldots, x_n)$, причём $f(0, \ldots, 0, 1) = 0$, и положительное число ε. Если случайные величины $r_1, \ldots, r_{n-1}$ независимы и равномерно распределены на множестве целых рациональных чисел от 1 до $N = \left\lceil \frac{6n+9}{\varepsilon} \right\rceil$, то прямая ℓ, проходящая через точки $(0 : \cdots : 0 : 1)$ и $(1 : r_1 : \cdots : r_{n-1} : 0)$, пересекает гиперповерхность X ровно в двух разных $\overline{K}$-точках p и q, которые не принадлежат гиперповерхности $x_0 = 0$ и служат двойными точками сечений C_p и C_q, соответственно, с вероятностью не меньше $1 - \varepsilon$.*

Доказательство. Покажем, что с большой вероятностью прямая ℓ трансверсально пересекает X в двух $\overline{K}$-точках p и q, отличных от точки $(0 : \cdots : 0 : 1)$. Ограничение f на эту прямую — это кубическая форма $f(x_0, r_1 x_0, \ldots, r_{n-1} x_0, x_n)$. Если точки p и q совпадают между собой, или одна из них совпадает с $(0 : \cdots : 0 : 1)$, то дискриминант этой формы от двух переменных x_0 и x_n равен нулю. Этот дискриминант — форма $\Delta(r_1, \ldots, r_{n-1})$ шестой степени. Поскольку X гладкая, из теоремы Бертини следует, что $\Delta(r_1, \ldots, r_{n-1})$ не обращается тождественно в нуль. По лемме Шварца–Зиппеля, вероятность её обращения в нуль не превышает $\frac{6}{N}$.

Предположим, что это условие выполнено. Точки p и q — это особые точки сечений C_p и C_q, соответственно. Остаётся оценить вероятность того, что ни C_p, ни C_q не является конусом.

Касательная гиперплоскость T_p определена линейной формой $h_0 x_0 + \cdots + h_n x_n$, где $h_i = \frac{\partial f}{\partial x_i}\big|_p$. Поскольку ℓ пересекает X трансверсально, $h_n \neq 0$. Поэтому C_p определяется внутри T_p кубической формой

$$g(x_0, \ldots, x_{n-1}) = f(h_n x_0, \ldots, h_n x_{n-1}, -h_0 x_0 - \cdots - h_{n-1} x_{n-1}).$$

C_p — это конус тогда и только тогда, когда частные производные $\frac{\partial g}{\partial x_i}$ линейно зависимы [12]. Эти производные — формы, чьи коэффициенты равны формам шестой степени от однородных координат p_0, $r_1, \ldots, r_{n-1}$ и p_n точки p. Поэтому их линейная независимость эквивалентна полному рангу матрицы, содержащей n строк и составленной из коэффициентов этих форм. В свою очередь, это эквивалентно необращению в нуль некоторого минора порядка n. По лемме 3, некоторый из этих миноров не обращается тождественно в нуль на гиперповерхности. Обозначим его через $M(x_0, r_1, \ldots, r_{n-1}, p_n)$. При условии $\Delta \neq 0$, ни одно из двух сечений C_p и C_q не является конусом, если ложно условие

$$(\exists x_n) f(1, r_1, \ldots, r_{n-1}, x_n) = 0 \wedge M(1, r_1, \ldots, r_{n-1}, x_n) = 0.$$

Эта формула эквивалентна обращению в нуль результанта $\mathrm{Res}_{x_n}(f, M)$. Таким образом, нам нужно оценить вероятность необращения в нуль произведения двух многочленов Δ и $\mathrm{Res}_{x_n}(f, M)$, каждый из которых зависит от случайных чисел $r_1, \ldots, r_n$. По лемме Шварца–Зиппеля, эта вероятность не меньше $1 - \frac{6n+9}{N}$. □

Теорема 1 *При всех $n \geqslant 2$ особая неприводимая кубическая гиперповерхность $X \subset \mathbb{P}^n$ с двойной K-точкой p над полем K характеристики нуль рациональная над K. Существует бирациональное отображение $\varphi : \mathbb{P}^{n-1} \dashrightarrow X$, заданное формами с коэффициентами из поля K. Более того, существует алгоритм, который получает на вход форму f, определяющую гиперповерхность X, и координаты двойной точки p, а выдаёт формы, определяющие отображение φ, делая $O(n^3)$ операций над полем K.*

Доказательство. Без ограничения общности можно считать, что точка p имеет однородные координаты $(1 : p_1 : \cdots : p_n)$. В противном случае достаточно сделать линейную замену переменных, вычислимую за полиномиальное время. Отождествим проективное пространство $\mathbb{P}^{n-1}$ с множеством прямых в $\mathbb{P}^n$, проходящих через точку p. В аффинном пространстве, где $x_0 = 1$, эти прямые заданы параметрически $(p_1 + a_1 t : \cdots : p_n + a_n t)$. Точка p соответствует значению $t = 0$. Отображение φ сопоставляет прямой, проходящей через точку p, другую точку пересечения этой прямой с X. Поскольку точка p двойная, это отображение определено почти везде. Ограничение формы f на прямую — это форма от двух переменных, коэффициентами которой служат формы от координат $p_1,\ldots, p_n$ точки p и коэффициентов $a_1,\ldots, a_n$. Поскольку точка p двойная, зная коэффициенты этого ограничения, легко найти образ отображения φ. Исключение составляет случай, когда прямая лежит на гиперповерхности X. □

Построение бирационального отображения из теоремы 1 существенно использует предположение, что точка p — это двойная, а не тройная точка. Если точка p тройная, то X — это конус, а точка p принадлежит вершине этого конуса.

Теорема 2 *Существует вероятностный алгоритм, который получает на вход кубическую форму $f(x_0,\ldots, x_n)$, определяющую гладкую кубическую гиперповерхность $X \subset \mathbb{P}^n$, где $n \geqslant 4$, координаты K-точки на X, положительное число ε и $n-1$ независимую случайную величину, каждая из которых равномерно распределена на множестве целых рациональных чисел от 1 до $N = \lceil \frac{6n+9}{\varepsilon} \rceil$. С вероятностью не ниже $1-\varepsilon$ алгоритм выдаёт доминантное рациональное отображение $\mathbb{P}^{2n-4} \dashrightarrow X$ над полем K, то есть список рациональных функций. Иначе с вероятностью меньше ε алгоритм выдаёт сообщение об отказе от вычисления. При этом алгоритм делает $O(n^4)$ арифметических операций над полем K.*

Доказательство. Без ограничения общности можно считать, что точка с однородными координатами $(0 : \cdots : 0 : 1)$ принадлежит X. Если на X существует некоторая K-точка, то этого можно добиться линейной заменой координат над полем K. Рассмотрим прямую ℓ, проходящую через точки $(0 : \cdots : 0 : 1)$ и $(1 : r_1 : \cdots : r_{n-1} : 0)$ для случайных чисел $r_i \in \{1,\ldots, N\}$. Согласно лемме 4, с вероятностью не меньше $1-\varepsilon$ прямая ℓ пересекает X ровно в трёх различных точках, хотя бы две из которых p и q служат двойными точками сечений C_p и C_q, соответственно.

Для поданного на вход набора случайных чисел алгоритм проверяет это условие. Если оно не выполнено, то выдаётся отказ от вычисления. Предположим, что это условие выполнено.

С точностью до мультипликативной константы ограничение формы f на прямую ℓ имеет вид $x_0(x_n^2 - 2bx_0x_n + cx_0^2)$, где функции $b(r_1,\ldots, r_{n-1})$ и $c(r_1,\ldots, r_{n-1})$ определены над полем K. Точки p и q соответствуют значениям координат $x_0 = 1$, $x_i = r_i$ и $x_n = b \pm \sqrt{b^2 - c}$, где $\sqrt{b^2 - c} \neq 0$. Для выбранных значений чисел r_i обозначим через L/K расширение поля K присоединением корня $\sqrt{b^2 - c}$. Поле L может совпадать с полем K. Рассмотрим сюръективное K-линейное отображение $\tau : K \times K \to L$, заданное формулой $\tau(y, z) = y + z\sqrt{b^2 - c}$. Для всех $y, z \in K$ произведение $\tau(y, z)\tau(y, -z) \in K$ и сумма $\tau(y, z) + \tau(y, -z) \in K$. Если $K \neq L$, то отображение τ служит изоморфизмом K-линейных пространств.

Определим рациональное отображение $\gamma : X \times X \dashrightarrow X$, которое сопоставляет двум точкам $v, w \in X$ третью точку пересечения прямой, проходящей через точки v и w, с X. Это отображение не определено, если прямая лежит в X. Иначе вычисление точки $\gamma(v, w)$ сводится к решению системы линейных уравнений и выполнимо посредством полиномиального числа арифметических операций над полем K. Для двух K-точек v и w образ $\gamma(v, w)$ снова будет K-точкой.

Касательные гиперплоскости T_p и T_q различны. Действительно, если $T_p = T_q$, то прямая, проходящая через точки p и q, целиком лежит на X. По лемме 2, оба сечения C_p и C_q неприводимые. По теореме 1, оба сечения C_p и C_q рациональны

над полем L. Соответствующие бирациональные отображения $\varphi_p : L^{n-2} \dashrightarrow C_p$ и $\varphi_q : L^{n-2} \dashrightarrow C_q$ вычислимы посредством полиномиального числа операций над полем K. Определим доминантное рациональное отображение $\psi : L^{2n-4} \dashrightarrow X$, которое равно композиции

$$L^{2n-4} = L^{n-2} \times L^{n-2} \overset{\varphi_p \times \varphi_q}{\dashrightarrow} C_p \times C_q \overset{\gamma}{\dashrightarrow} X.$$

Композиция $\psi(\tau(y_1, z_1), \ldots, \tau(y_{n-2}, z_{n-2}), \tau(y_1, -z_1), \ldots, \tau(y_{n-2}, -z_{n-2}))$ даёт искомое доминантное рациональное отображение $K^{2n-4} \dashrightarrow X$, определённое над полем K. □

Хотя доказательство унирациональности использует разбор случаев, в зависимости от принадлежности квадратного корня полю K, алгоритм не проверяет это условие, а работает одинаково во всех случаях. Это иллюстрирует различие между собственно алгоритмом и методом его обоснования, опирающемся на разбор случаев и чистые теоремы существования.

Алгоритм из теоремы 2 может быть преобразован следующим способом. Существует вероятностный алгоритм, который никогда не отказывается от вычислений и даёт правильный ответ за конечное время, причём с высокой вероятностью время его работы будет маленьким, но алгоритм может работать длительное время при некоторой реализации используемых случайных чисел. Для этого достаточно повторять вычисление на новых реализациях случайных чисел до тех пор, пока требуемое отображение не будет построено.

Если поле рациональных функций $K(X)$ полиномиально вычислимое и известно доминантное рациональное отображение $\mathbb{P}^m \dashrightarrow X$, то легко построить вычислимое за полиномиальное время чисто трансцендентное расширение поля K и вычислимое за полиномиальное время вложение поля рациональных функций $K(X)$ в это расширение.

4. Заключение

Предлагаемый метод позволяет быстро найти всюду плотное в топологии Зарисского множество K-точек на кубической гиперповерхности с известной K-точкой. В свою очередь, это даёт возможность проводить вычисления на гиперповерхности, работая над исходным полем, эффективно используя возможности символьных вычислений, вместо применения приближённых вычислений, которые могут быть связаны с большими погрешностями в высоких размерностях. Аналогичный метод применим и для поиска точек на кубической поверхности, но в этом случае требуется дополнительная проверка неприводимости сечения поверхности касательными плоскостями. Соответственно, в этом случае изменится оценка вероятности успеха.

Благодарности

Автор благодарит анонимного рецензента за полезные замечания.

Литература

1. *Kollár J.* Unirationality of cubic hypersurfaces // Journal of the Institute of Mathematics of Jussieu. — 2002. — Vol. 1. — P. 467–476.
2. *Segre B.* A note on arithmetical properties of cubic surfaces // Journal of the London Mathematical Society. 1943. — Vol. 18. — P. 24–31.
3. *Clemens C. H., Griffiths P. A.* The intermediate Jacobian of the cubic threefold // Annals of Mathematics. Second Series. — 1972. — Vol. 95, no. 2. — P. 281–356.
4. *Polo-Blanco I., Top J.* A remark on parameterizing nonsingular cubic surfaces // Computer Aided Geometric Design. — 2009. — Vol. 26, no. 8. — P. 842–849.
5. *González-Sánchez J., Polo-Blanco I.* Construction algorithms for rational cubic surfaces // Journal of Symbolic Computation. — 2017. — Vol. 79. — P. 309–326.

6. *Малашонок Г. И.* Система компьютерной алгебры MathPartner // Программирование. — 2017. — No. 2. — P. 63–71. Перевод: *Malaschonok G. I.* MathPartner computer algebra // Programming and Computer Software. — 2017. — Vol. 43, no. 2. — P. 112–118.
7. *Mayr E.W., Ritscher S.* Dimension-dependent bounds for Gröbner bases of polynomial ideals // Journal of Symbolic Computation. — 2013. — Vol. 49. — P. 78–94.
8. *Селиверстов А. В.* О касательных прямых к аффинным гиперповерхностям // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. — 2017. — Т. 27, № 2. — С. 248–256.
9. *Seliverstov A. V.* On probabilistic algorithm for solving almost all instances of the set partition problem // *Weil P.* (ed.) Computer Science – Theory and Applications. CSR 2017. LNCS. — Vol. 10304. Springer, Cham, 2017. — P. 285–293.
10. *Алаев П. Е.* Структуры, вычислимые за полиномиальное время. I // Алгебра и логика. — 2016. — Т. 55, № 6. — С. 647–669. Перевод: *Alaev P. E.* Structures computable in polynomial time. I // Algebra and Logic. — 2017. — Vol. 55, no. 6. — P. 421–435.
11. *Schwartz J. T.* Fast probabilistic algorithms for verification of polynomial identities // Journal of the ACM. — 1980. — Vol. 27, no. 4. — P. 701–717.
12. *Gondim R., Russo F.* On cubic hypersurfaces with vanishing hessian // Journal of Pure and Applied Algebra. — 2015. — Vol. 219, no. 4. — P. 779–806.

UDC 510.52

Looking for points on a smooth cubic hypersurface

A. V. Seliverstov

Institute for Information Transmission Problems of the Russian Academy of Sciences (Kharkevich Institute)
Bolshoy Karetny per. 19, build.1, Moscow, 127051, Russia

Email: slvstv@iitp.ru

It is well known that a smooth projective cubic hypersurface of dimension two or higher with a marked point over a field of characteristic zero is unirational over the field. Consequently, the set of points of the hypersurface over the field is dense in the Zariski topology. There is considered the computational complexity of the search for such points. It is shown that a dominant rational map from a projective space to the hypersurface can be calculated by a probabilistic algorithm that works without errors and completes the work with a high probability, making a polynomially bounded number of arithmetic operations over the field. In the general case, the image of the rational map does not contain all points over the field, but only a large set of such points. In particular, the calculation of such points over a finite extension of the field of rational numbers allows us to abandon the approximation of real or complex numbers, but use more possibilities of symbolic computations. The problem is closely related to the proof of the smoothness of the hypersurface and can be used to solve some combinatorial problems. Earlier, I.V. Latkin and the author have shown the set partition problem can be reduced to the problem of finding singular points of a cubic hypersurface. Rational parametrization of surfaces is used in computer graphics.

Key words and phrases: cubic hypersurface, rational map, computational complexity.

Научное издание

КОМПЬЮТЕРНАЯ АЛГЕБРА

Материалы Международной конференции

Москва, 30 октября – 3 ноября 2017 г.

Макет и компьютерная верстка *Д. С. Кулябов*

Подписано в печать 05.10.2017. Формат 60x84 1/16.
Уч.-изд. л. 16,34. Усл. печ. л. 10,75. Тираж 150 экз. Заказ

ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.

Напечатано в ФГБОУ ВО «РЭУ им. Г. В. Плеханова».
117997, Москва, Стремянный пер., 36.

ISBN 978-5-7307-1266-9