Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования Московский физико-технический институт (государственный университет)

МФТИ

60

60-я НАУЧНАЯ КОНФЕРЕНЦИЯ МФТИ

Москва,
Долгопрудный,
Жуковский
2017

# ТРУДЫ 60-Й ВСЕРОССИЙСКОЙ НАУЧНОЙ КОНФЕРЕНЦИИ МФТИ

**20-26 ноября 2017 года**

## Прикладная математика и информатика

Министерство образования и науки Российской Федерации

Федеральное государственное автономное образовательное учреждение высшего образования «Московский физико-технический институт (государственный университет)»

# Труды
## 60-й Всероссийской научной конференции МФТИ

20 - 26 ноября 2017 года

## Прикладная математика и информатика

Москва Долгопрудный Жуковский
МФТИ
2017

УДК 51+004
ББК 22.1+32.81
Т78

Т78 **Труды 60-й Всероссийской научной конференции МФТИ.**
20–26 ноября 2017 г. Прикладная математика и информатика. -
М.: МФТИ, 2017. - 320 с.
ISBN 978-5-7417-0652-7

Включены результаты оригинальных исследований студентов, аспирантов, преподавателей и научных сотрудников МФТИ и дружественных учебных и научных организаций. Статьи представляют интерес для специалистов, работающих в области прикладной математики и информатики.

**УДК 51+004**
**ББК 22.1+32.81**

**ISBN 978-5-7417-0652-7**

2. *Zhang Zh., Shi Y.* On the parity complexity measures of Boolean functions // Theoretical Computer Science. 2010. V. 411(26-28). P. 2612-2618.
3. *Lee T., Zhang Sh.* Composition theorems in communication complexity // Proceedings of the 37th International Colloquium on Automata, Languages and Programming (ICALP). 2010. P. 475–489.
4. *Tsang H.Y., Wong Ch.H., Xie N., Zhang Sh.* Fourier sparsity, spectral norm, and the log-rank conjecture //
5. Proceedings of the 2013 IEEE 54th Annual Symposium on Foundations of Computer Science (FOCS '13). – Washington (DC):IEEE Computer Society, 2013. P. 658–667.
6. *Abbe E., Alon N., Bandeira A.S.* Linear Boolean classification coding and ``the critical problem" // Proceedings of IEEE International Symposium on Information Theory (ISIT). 2014. P. 1231–1235.
7. *Jukna S.* Boolean function complexity: advances and frontiers. - Heidelberg-Berlin-NewYork: Springer-Verlag, 2012. 617 p.
8. *Yao P.* Parity decision tree complexity and 4-party communication complexity of XOR-functions are polynomially equivalent // Chicago Journal of Theoretical Computer Science. 2016. Article 12. P. 1-8.
9. *Kushilevitz E., Nisan N.* Communication complexity. New York (NY): Cambridge University Press, 1996. 189 p.
10. *Lee T., Shraibman A.* Lower bounds in communication complexity // Foundations and Trends® in Theoretical Computer Science. 2009. V. 3, N. 1. P. 263–399.

УДК 510.52

## Эффективная унирациональность кубической гиперповерхности

***А.В. Селиверстов***

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

Фиксируем счётное поле $K$ характеристики нуль с нумерацией, при которой арифметические операции 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 [1]. В общем случае, если два поля, в каждом из которых операции вычислимы за полиномиальное время, изоморфны друг другу, то не существует изоморфизма, вычислимого за полиномиальное время [2]. Говоря о расширении поля $L/K$, мы подразумеваем, что операции в поле $L$ также вычислимы за полиномиальное время, более того, существует вычислимый за полиномиальное время изоморфизм между полем $K$ и подполем поля $L$.

Гладкая проективная кубическая кривая на плоскости иррациональна. Однако отличная от конуса неприводимая проективная кубическая гиперповерхность размерности два или выше с отмеченной $K$-точкой унирациональна над $K$. Для гладкой кубической поверхности над полем рациональных чисел унирациональность доказал Беньямино Сегре [3], при некоторых ограничениях – Ю.И. Манин [4, с. 57], а в более общем случае – Янош Коллар [5]. Однако в этих работах доказана лишь чистая теорема существования. Мы рассмотрим вычислительную сложность поиска доминантного рационального отображения проективного пространства в гиперповерхность. В общем случае образ этого отображения содержит не все $K$-точки, но множество таких $K$-точек всюду плотное в топологии Зарисского.

Допуская некоторую вольность, мы не различаем случайную величину и реализацию этой случайной величины. По сути, вероятностный алгоритм получает на вход некоторую реализацию случайной величины.

**Теорема**. Существует вероятностный алгоритм, который получает на вход кубическую форму над полем K, определяющую отличную от конуса неприводимую кубическую гиперповерхность X в n-мерном проективном пространстве, где размерность n

не меньше трёх, координаты K-точки на X, положительное число E и n-1 независимую случайную величину, каждая из которых равномерно распределена на множестве целых рациональных чисел от 1 до N>(6n+9)/E. С вероятностью не меньше 1-E алгоритм выдаёт доминантное рациональное отображение из (2n-4)-мерного проективного пространства в X над полем K, то есть список рациональных функций. Иначе с вероятностью меньше E алгоритм выдаёт сообщение об отказе от вычисления. При этом число арифметических операций над полем K, которые выполняет алгоритм, ограничено сверху многочленом от размерности n.

Число $N$ в формулировке теоремы не ограничено сверху и может быть выбрано так, чтобы случайные числа были распределены на множестве, мощность которого равна степени двойки. В этом случае случайные числа можно отождествить с последовательностями случайных битов – независимых бернуллиевских случайных величин; алгоритм использует $O(n\log_2 n)$ битов.

Вначале алгоритм проверяет гладкость отмеченной точки. Если $K$-точка особая (двойная), то гиперповерхность $X$ рациональная над $K$, а искомое рациональное отображение вычисляется детерминированным алгоритмом за полиномиальное время. Иначе дальнейшие шаги алгоритма основаны на конструкции из работы [5]. Через выделенную $K$-точку на $X$ проводится прямая, определяемая $n$-1 случайным числом. Алгоритм проверяет условие, что эта прямая пересекает $X$ в двух других точках, которые служат двойными точками сечений касательными гиперплоскостями. Иначе алгоритм отказывается от вычислений и выдаёт предупреждение. Если это условие выполнено, то оба сечения либо содержат рациональные над $K$ неприводимые компоненты, либо содержат рациональные над квадратичным расширением $L/K$ и сопряжённые неприводимые компоненты. Обычно эти сечения неприводимые. Сопоставляя двум точкам этих рациональных многообразий третью точку пересечения проходящей через них прямой с $X$, мы получим доминантное рациональное отображение из произведения двух рациональных многообразий в $X$. При этом если две точки сопряжены, то третья точка определена над полем $K$. А если две точки определены над $K$, то такова же и третья точка. Композиция рациональных отображений даст искомое рациональное отображение. Отметим два существенных отличия от работы [5], связанных с вычислительной сложностью.

Во-первых, промежуточные вычисления проходят над некоторым полем $L$, которое получается присоединением к полю $K$ квадратного корня из его элемента. Если этот корень извлекается, то $L=K$. Однако символьные вычисления можно проводить по одним и тем же формулам, не проверяя, извлекается ли квадратный корень. В любом случае окончательный ответ будет получен над исходным полем $K$.

Во-вторых, вместо прямой общего положения, проходящей через выделенную $K$-точку гиперповерхности, используется прямая, случайно выбранная из конечного множества. В первом случае требуемое свойство следует из теоремы Бертини – чистой теоремы существования, а в эффективном варианте это свойство выполнено с большой вероятностью, которую можно оценить снизу посредством леммы Шварца–Зиппеля [6]. Эта оценка и составляет научную новизну работы.

Алгоритм может быть преобразован следующим способом. Существует вероятностный алгоритм, который никогда не отказывается от вычислений и даёт правильный ответ, 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 параллельно осуществлять полный перебор вариантов, то правильный ответ будет получен за конечное время.

Условие отличия гиперповерхности от конуса существенно. Во-первых, конус над плоской гладкой кубической кривой не может быть унирациональным. Во-вторых, если отмеченная $K$-точка совпадает с вершиной конуса, то алгоритм не применим, даже если конус унирационален. Если гиперповерхность рациональная, алгоритм не обязательно

найдёт бирациональное отображение. Для рациональных поверхностей известны другие методы [7].

Построенное рациональное отображение позволяет быстро найти всюду плотное в топологии Зарисского множество $K$-точек на кубической гиперповерхности с отмеченной $K$-точкой. С другой стороны, найденные $K$-точки можно использовать для доказательства гладкости гиперповерхности методом, описанным в работе [8].

**Литература**


1. *Малашонок Г.И.* Система компьютерной алгебры MathPartner // Программирование. 2017. № 2. С. 63–71.
2. *Алаев П.Е.* Структуры, вычислимые за полиномиальное время. I // Алгебра и логика. 2016. Т. 55, № 6. С. 647–669.
3. *Segre B.* A note on arithmetical properties of cubic surfaces // Journal of the London Mathematical Society. 1943. V. 18. P. 24–31.
4. *Манин Ю.И.* Кубические формы: алгебра, геометрия, арифметика. –М.: Наука, 1972. 304 с.
5. *Kollár J.* Unirationality of cubic hypersurfaces // Journal of the Institute of Mathematics of Jussieu. 2002. V. 1. P. 467–476.
6. *Schwartz J.T.* Fast probabilistic algorithms for verification of polynomial identities // Journal of the ACM. 1980. V. 27, no. 4. P. 701–717.
7. *González-Sánchez J.*, *Polo-Blanco I.* Construction algorithms for rational cubic surfaces // Journal of Symbolic Computation. 2017. V. 79. P. 309–326.
8. *Селиверстов А.В.* О касательных прямых к аффинным гиперповерхностям // Вестник Удмуртского университета. Математика. Механика. Компьютерные науки. 2017. Т. 27, № 2. С. 248–256.


УДК 519.713

## Автоматы со структурой данных и сложность вычислений

***А.А. Рубцов***

Национальный исследовательский университет «Высшая школа экономики»
Московский физико-технический институт (государственный университет)

Односторонние недетерминированные конечные автоматы, снабжённые структурами данных, занимают важную нишу в теории формальных языков. С их помощью описывают такие широкие классы языков, как контекстно-свободные языки и индексные языки: в первом случае структурой данных выступает стек, а во втором — вложенные стеки. Приведём примеры более специальных классов, которые определяются через автоматы данного вида: автоматы со счётчиками, автоматы со словарём (Set Automata), открытые в 2014 году [1], автоматы, снабжённые $k$ счётчиками с ограниченным числом переключений между увеличениями и уменьшениями.

Некоторые общие вычислительные и структурные свойства таких моделей были исследованы в 60–70-х годах XX века [2–4]. Вариации таких автоматов получили названия Balloon Automata и Abstract Family of Automata. Для данных моделей были установлены структурные свойства, описываемые в терминах абстрактных семейств языков (Abstract Family of Languages), в частности замкнутость относительно пересечения с регулярными языками и, в зависимости от структуры данных, замкнутость относительно стирающего или нестирающего гомоморфизма. Важным результатом этих исследований, который относится к вопросам разрешимости, является факт того, что проблема принадлежности слова языку либо разрешима одновременно для односторонних и двусторонних автоматов со структурами данных, либо одновременно неразрешима.

Мы предлагаем новый формализм описания автоматов данного вида и устанавливаем с его помощью связь данной модели со сложностью вычислений. А именно, мы формализуем понятие структуры данных. Структура данных определяется через язык протоколов $\mathrm{PROT}$ этой структуры. Заметим, что языком протокола работы со стеком