ЭКСТРЕМАЛЬНЫЕ ЗАДАЧИ НА МНОГООБРАЗИЯХ И МЕТОДЫ АРИФМЕТИЧЕСКОЙ ГЕОМЕТРИИ

Н.М. ГЛАЗУНОВ,
Институт кибернетики им. В.М. Глушкова
НАН Украины, Киев, Украина
glanm@yahoo.com

Аннотация. *Исследуются задачи дискретной (целочисленной) оптимизации и применения для их исследования избранных методов арифметической (диофантовой) геометрии. Представлены результаты применения методов декомпозиции и локализации к задачам недифференцируемой оптимизации на многообразиях. В некоторых случаях задачу оптимизации на нелинейном многообразии удается свести к оптимизационной задаче на линейном многообразии, а также к проверке существования решений алгебраического многообразия в конечном поле. Кратко представляются результаты о положительно определенных экстремальных квадратичных формах и развитие этих результатов .*

Ключевые слова: *многообразие, алгебраическое многообразие, нулевая группа (ко)гомологий, идеал алгебраического многообразия, декомпозиция, локальное кольцо, оптимизация.*

Введение

В монографиях [1-3] авторами представлены задачи недифференцируемой оптимизации и предложены соответствующие методы их решения. Одним из классов задач (недифференцируемой) оптимизации являются задачи дискретой (целочисленной) оптимизации, в которых требуется указать точные значения точек экстремума и точные значения, или оценки, экстремальных значений функций в этих точках. Далее, для краткости, мы будем называть такие задачи экстремальными. При применении приближенных методов значения дискретные (целочисленные) точек экстремума найти удается не всегда. В сообщении предлагается использовать для этих целей методы арифметической (диофантовой) геометрии. Задачи

и методы арифметической (диофантовой) геометрии имеют историю, сопоставимую с историей всей математики, что видно из одного из названий этого направления: диофантова геометрия. Далее мы используем более распространенный в настоящее время термин – арифметическая геометрия. На методах арифметической геометрии основывается доказательство Большой теоремы Ферма, а разделы арифметической геометрии, изучающие эллиптические кривые над полями характеристики $p > 0$ являются одной из математических основ эллиптической криптографии и соответствующих схем цифровой подписи. Приложения методов арифметической геометрии к некоторым оптимизационным задачам представлено в [4], а также в [12-14]. Работа посвящена развитию этих результатов.

В последней главе монографии Н.З. Шора [1] рассмотрены (недифференцируемые) полиномиальные оптимизационные задачи и их связи с системами квадратичных форм и квадратичных уравнений.

В сообщении мы представляем две (классические) задачи, связанные с кругом вышеназванных идей монографии [1]. Первая задача является обобщением задачи о Пифагоровых треугольниках, и называется задачей о конгруэнтных числах [5]. Вторая задача связана с системой квадратичных форм по Сегре [6-7]. Для второй задачи удается получить метод нахождения её экстремальных решений. Полное решение первой задачи автору (октябрь 2021 г.) неизвестно. Мы приведем формулировки этих задач, методы их исследования и результаты в, соответственно, разделах 1 и 2, и в планируемом сообщении.

1. Вычисление конгруэнтных чисел

Конгруэнтным числом называют натуральное число, равное площали прямоугольного треугольника с рациональными сторонами.

Задача. *Перечислить натуральные числа, которые являются значениями площадей прямоугольных треугольников со сторонами, длины которых являются рациональными числами.*

Пусть S есть натуральное число, являющееся площадью прямоугольного треугольника с рациональными катетами a, b и

гипотенузой c. Тогда по теореме Пифагора должны выполняться равенства (в форме Д. Загира)

$$a^2 + b^2 = c^2$$
$$ab = 2St^2. \tag{1}$$

В [5] рациональные решения этой системы квадратичных форм (квадратичной системы) сводятся к исследованию рациональных точек на эллиптической кривой

$$y^2 = x^3 - S^2 x.$$

К сожалению, автору неизвестен на время написания этого сообщения алгоритм нахождения рациональных точек на эллиптических кривых такого типа. Но для эллиптических кривых, для которых выполняется гипотеза Берча–Суиннертона-Дайера [8,11], такой алгоритм предложен Ю.И. Маниным [8]. В связи с этим мы приведем здесь схему I сведения квадратичной системы типа (1) к уравнению эллиптической кривой, а также обратную схему II построения квадратичной системы по эллиптической кривой. Схемы могут быть выведены из результатов, представленных в [8,9], и в [10], и доведены до алгоритмов.

I. Исходные данные. Пусть квадратичные формы, определяющие квадратичную систему типа (1) в 4-мерном проективном пространстве P^3, задаются симметрическими матрицами A, B размера 4×4 и имеют вид:

$$x^{Tr} Ax = 0,\ x^{Tr} Bx = 0. \tag{2}$$

Кривая. Тогда, если многочлен $\det(\alpha A + \beta B)$, принадлежащий кольцу $k[\alpha, \beta]$, не имеет кратных корней, (2) определяет кривую рода один.

II. Исходные данные. Эллиптическая кривая E с точкой x на ней, заданная как погружение в P^2 (с помощью обратимого пучка $O(3x)$ [9]), например, в форме Вейерштрасса.

Квадратичная система. По E, с помощью обратимого пучка $O(4x)$, строится квадратичная система в P^3.

Представление натуральных чисел тетрарными положительно определенными целыми квадратичными формами будет представлено. Отметим здесь только, что число представлений натурального числа такой формой конечно.

Метод Таннелла (Tannell) **проверки натурального числа на конгруэнтность** [5]. Метод сводит такую проверку к экстремальной задаче о числе целочисленных решений квадратичной системы. Он состоит из доказанной достаточной части и условной необходимой части. Вариант метода и его обсуждение будет представлен в планируемом докладе.

2. Нахождение экстремумов системы Сегре

Системой Сегре называют систему квадратичных форм вида

$$\begin{cases} x_1^2 - x_2^2 + y_1^2 - y_2^2 = 0,\ x_1^2 - x_3^2 + y_1^2 - y_3^2 = 0,\ x_2^2 - x_3^2 + y_2^2 - y_3^2 = 0, \\ x_1^3 - x_2^3 + y_1^3 - y_2^3 = 0,\ x_1^3 - x_3^3 + y_1^3 - y_3^3 = 0,\ x_2^3 - x_3^3 + y_2^3 - y_3^3 = 0, \end{cases} \qquad (3)$$

Она была введена в работе Сегре [6] и исследовалась Сегре, Касседсом [7], и другими авторами. Кубический формы второй строки с помощью известных подстановок [1] могут быть сведены к системе квадратичных форм. Но для системы (3) мы интересуемся её арифметической геометрией (декомпозицией, рациональными точками) с целью сведения задачи оптимизации (здесь, для примера, рациональной минимизации) к наиболее простому варианту. Сегре и другими показано, что это многообразие есть объединение 11 неприводимых множеств, а именно, четырех прямых (линейные многообразия), шести эллиптических кривых (кривые рода один), и одной кривой рода пять. Все эти множества задаются квадратичными или линейными системами уравнений. Приведем примеры линейных многообразий:

$$x_1 = x_2,\ x_1 = y_3, x_2 = y_3,\ y_1 = y_2, y_1 = x_3, y_2 = x_3,$$

и кривых рода один:

$$\begin{cases} x_1^2 + y_1^2 = x_2^2 + y_2^2,\ x_1^2 + y_1^2 = 2x_1y_1 + 2x_2y_2 + (x_1 + y_1)(x_2 + y_2), \\ x_3 = x_1, y_3 = y_1 \end{cases}$$

Рациональные решения, соответствующие прямым, называют тривиальными решениями. Исследовано [6,7], что только тривиальные решения являются рациональными точками многообразия Сегре. Поэтому задача рациональной минимизации на многообразии Сегре сводится к задаче рациональной минимизации на линейном многообразии.

Замечание. Задача рациональной минимизации на линейном многообразии значительно проще задачи рациональной минимизации на нелинейном многообразии. К тому же, полученное линейное многообразие имеет меньшую размерность.

Далее в сообщении планируется представить результаты о положительно определенных экстремальных квадратичных формах и развитие этих результатов .

Литература.

1. Shor N.Z. Nondifferentiable optimization and polynomial problems. – Boston: Kluwer Acad. Publ., 1998. – 394 p.
2. Соломон Д.И. Дробное программирование и недифференцируемая оптимизация. – Saarbrucken: LAMBERT Acad. Publ., 2015. – 556 с.
3. Стецюк П.И. Двойственные оценки в квадратичних экстремальных задачах. – Кишинэу: Эврика., 2018. – 503 с.
4. Глазунов Н.М. Разработка методов обоснования гипотез формальных теорий. – Saarbrucken: LAMBERT Acad. Publ., 2014. – 280 с.
5. Tunnell J.B. A classical Diophantine problem and modular forms of weight 3/2// Invent.Math. – 1983. – Vol. 72. – P. 323–334.
6. Segre B. Alcune questioni Diofantee // Publ. Un. Math. Ital. – 1950. – (3). 5. – P. 33-43.
7. Cassels J.W. Diophantine equations with special reference to elliptic curves // J. London Math. Soc. – 1966. – Vol. 41. – P. 193–291.
8. Манин Ю.И. Круговые поля и модулярные кривые // УМН. – 1971. – Том 26, вып. 6. – С. 7–71.
9. Hartshorne R. Algebraic geometry. Graduate Texts in Mathematics. – NY: Springer, 1977. – 496 p.

10. Мамфорд Д. Лекции о тета-функциях. – М.: Мир, 1988. – 446.
11. Husemoller D. Elliptic curves. Second Edition. – NY: Springer, 2004. – 483 p.
12. Глазунов Н.М. Задачи на арифметические минимумы и методы их исследования / Н.М. Глазунов // Материалы 3-й международной конференции «Математическое моделирование, оптимизация и информационные технологии», 2012. – Кишинэу: Эврика. - С. 286–290.
13. Glazunov N.M. Quadratic forms, algebraic groups and number theory // Чебышевский сборник. Посвящается 75-летию академика В.П. Платонова. – 2015. – Том XVI, вып. 4 (56). – С. 77 – 89.
14. Glazunov N.M. Extremal forms and rigidity in arithmetic geometry and in dynamics // Чебышевский сборник. Посвящается столетию со дня рождения профессора А. Б. Шидловского. – 2015. – Том XVI, вып. 3 (55). – С. 124 – 146.