УДК 514.142

Об эвристическом вероятностном алгоритме для задачи о разбиении множества

А.В. Селиверстов

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

Задача о разбиении множества NP-полная. Её формулировка: дан набор положительных целых чисел $a_0,..., a_{n+1}$; существует ли разбиение на два подмножества с равными суммами элементов? Эта задача эквивалентна поиску точки с координатами 1 или –1 на гиперплоскости.

В работах [1, 2] предложен алгоритм, который получает на вход набор положительных целых чисел $a_0,..., a_{n+1}$ и за полиномиальное время выдаёт такой многочлен $f(x_1,..., x_n)$ третьей степени с целыми коэффициентами, что особые точки аффинной гиперповерхности $f=0$ соответствуют решениям задачи о разбиении множества. Более того, координаты особых точек могут быть равны только 1 или –1. Гладкость означает отсутствие решения.

Дискриминант многочлена от одной переменной равен нулю, если некоторый корень кратный. Дискриминант сам является однородным многочленом с целыми коэффициентами от всех коэффициентов исходного многочлена. Многочлен называется *свободным от квадратов*, если он не делится на квадрат другого многочлена положительной степени. Обозначим через f свободный от квадратов многочлен степени d с целыми коэффициентами.

Построим семейство конусов, каждому из которых принадлежат все особые точки на гиперповерхности $f=0$, если они существуют. Прямая, проходящая через точку U с координатами $(u_1,..., u_n)$, состоит из точек с координатами $((x_1–u_1)t+u_1,..., (x_n–u_n)t+u_n)$, где t играет роль координаты на прямой. Обозначим через $r(t)$ ограничение на эту прямую многочлена f, а через $D[f,U](x_1,..., x_n)$ дискриминант многочлена $r(t)$, вычисляемый по формуле для дискриминанта многочленов степени d. Если точка U не является особой точкой гиперповерхности $f=0$, то уравнение $D[f,U](x_1,..., x_n)=0$ определяет конус, у которого почти любая образующая касается гиперповерхности $f=0$ или проходит через её особую точку. Если точка U принадлежит гиперповерхности и не является особой, то конус приводимый и содержит касательную гиперплоскость. Если точка U особая, то многочлен $D[f,U]$ тождественно равен нулю. Обозначим через p проекцию гиперповерхности $f=0$ на координатную гиперплоскость $x_n=0$. Если f нетривиально зависит от переменной x_n, то прообраз общей точки на координатной гиперплоскости содержит d точек.

Лемма. *Даны неприводимый многочлен $f(x_1,..., x_n)$ степени d не меньше двух, который нетривиально зависит от переменной x_n, положительное число $s>0$ и конечное множество точек W. Пусть случайные координаты $z_1,..., z_{n-1}$ независимы и равномерно распределены на множестве целых чисел от 1 до $n(|W|+d)/s$. Если касательные гиперплоскости к гиперповерхности $f=0$ в совокупности не пересекаются в одной точке, то вероятность того, что касательная гиперплоскость к гиперповерхности в некоторой точке из прообраза $p^{-1}(z_1,..., z_{n-1}, 0)$ пересекает множество W, не превосходит числа s. Если же все касательные гиперплоскости пересекаются в одной точке, то эта точка – особая точка гиперповерхности $f=0$.*

Обозначим через h линейную функцию, определяющую касательную гиперплоскость к гиперповерхности $f=0$ в принадлежащей ей точке U. Если касательные гиперплоскости к гиперповерхности $f=0$ не пересекаются в одной точке, то по лемме для почти всех точек U многочлен $D[f,U]/h$ равен нулю в каждой особой точке гиперповерхности $f=0$. Деление многочленов сводится к решению системы линейных уравнений.

Если многочлен F равен линейной комбинации кубов переменных и свободного члена, то каждый моном многочлена $D[F,U]$ зависит самое большее от четырёх переменных; каждый моном многочлена $D[F,U]/h$ зависит самое большее от трёх переменных.

Обозначим через q естественный эпиморфизм кольца многочленов на фактор-кольцо по идеалу, порождённому многочленами $x_k^2–1$. Элементы этого фактор-кольца отождествим с мультилинейными многочленами. При сведении задачи о разбиении множества, многочлен f

равен ограничению многочлена $F=a_0+a_1x_1^3+...+a_{n+1}x_{n+1}^3$ на гиперплоскость $a_0+a_1x_1+...+a_{n+1}x_{n+1}=0$. Если точка U лежит на этой гиперплоскости, то многочлены $D[f,U]/h$ и $D[F,U]/h$ равны при ограничении на гиперплоскость. Их образы при эпиморфизме q принимают одинаковые значения в точках с координатами 1 или –1, принадлежащих этой гиперплоскости. Обозначим через L линейное подпространство в пространстве мультилинейных многочленов, порождаемое образами при эпиморфизме q таких ограничений мультилинейных многочленов $q(D[F,U]/h)$, соответствующих случайно выбранным точкам U на гиперплоском сечении, как в лемме. Если это сечение содержит особую точку с координатами 1 или –1, то для общей точки U каждый многочлен из L обращается в нуль в особой точке. Если же L совпадает с пространством мультилинейных многочленов степени не выше третьей, то гиперповерхность гладкая во всех точках с координатами 1 или –1.

Теорема. *Для любого $s>0$ для проверки существования решения у задачи о разбиении множества существует вероятностный алгоритм, который*

- *получает на вход положительные целые $a_0,...,a_{n+1}$ из интервала от 1 до 2^n;*
- *выполняет $O(n^9)$ арифметических операций над вещественными алгебраическими числами и операций извлечения корня второй или третьей степени;*
- *принимает вход с вероятностью $>1–s$, если существует решение;*
- *иначе отвергает вход с вероятностью $>1–s$ за исключением для каждого значения n доли входов, стремящейся к нулю при увеличении n.*

Алгоритм строит кубическую гиперповерхность $F=0$, для которой особые точки гиперплоского сечения соответствуют решениям задачи о разбиении множества [1, 2]. Если сечение приводимое ($n=2$), то вход принимается. Иначе в сечении выбираются $O(n^3)$ случайных точек. Если среди этих точек оказалась точка с координатами 1 или –1, то вход принимается. Если касательные гиперплоскости пересекаются в одной точке, то вход принимается (согласно лемме, точка пересечения особая; она служит решением). Иначе по выбранным точкам вычисляется семейство мультилинейных многочленов; если оно *не* порождает пространство всех мультилинейных многочленов степени не выше третьей от n переменных, то вход принимается (решение даёт линейную зависимость многочленов). Иначе вход отвергается.

Число случайных битов, используемое алгоритмом, ограничено многочленом от n и $1/s$; оно не зависит от значений чисел $a_0,..., a_{n+1}$. Число арифметических операций и операций извлечения корня второй или третьей степени также ограничено многочленом от n. Но при этом возникают алгебраические числа, длина и степень которых могут быть большими [3]. Верхние оценки вероятности ошибки и доли исключений вычисляются по лемме Шварца–Зиппеля [4].

Детерминированная проверка правильности выбора конкретной точки U столь же трудна, как и решение исходной задачи о разбиении множества. Гораздо труднее проверить гладкость общей кубической гиперповерхности, поскольку степень её дискриминанта быстро растёт при увеличении размерности [5].

Литература

1. *Латкин И.В.*, *Селиверстов А.В.* Вычислительная сложность фрагментов теории поля комплексных чисел // Вестник Карагандинского университета. Сер. Математика. 2015. № 1 (77). С. 47–55. http://vestnik.ksu.kz/mathematics.html#ser5

2. *Селиверстов А.В.* О вычислительной сложности поиска особых точек // Дискретная математика, алгебра и их приложения / ред. И.Д. Супруненко, В.В. Лепин, О.И. Дугинов. Минск: Институт математики НАН Беларуси, 2015. С. 135–137. http://im.bas-net.by/~dima/

3. *Дубицкас А.*, *Смит К.* О длине суммы и произведения алгебраических чисел // Математические заметки. 2005. Т. 77, № 6. С. 854–860. DOI: 10.4213/mzm2540

4. *Schwartz J.T.* Fast probabilistic algorithms for verification of polynomial identities // J. ACM. 1980. V. 27, № 4. P. 701–717. DOI: 10.1145/322217.322225

5. *Гельфанд И.М.*, *Зелевинский А.В.*, *Капранов М.М.* Дискриминанты многочленов от многих переменных и триангуляции многогранников Ньютона // Алгебра и анализ. 1990. Т. 2, № 3. С. 1–62. http://mi.mathnet.ru/aa186