Приложение к лекциям об экспандерах (Санкт-Петербург, апрель 2017 г.)

24 Две алгебраические конструкции спектральных экспандеров

В этой главе мы опишем две конструкции спектральных экспандеров, удобных для практических применений (без доказательства оценки для второго собственного числа).

Экспандер Маргулиса. В качестве множества вершин графа мы возьмём $V = \mathbb{Z}_n \times \mathbb{Z}_n$ (таким образом, граф будет содержать n^2 вершин). Каждая вершина (x, y) из $\mathbb{Z}_n \times \mathbb{Z}_n$ соединяется рёбрами со следующими восьмью вершинами:

$$(x, y \pm 2x), (x, y \pm (2x+1)), (x \pm 2y, y), (x \pm (2y+1), y)$$

(все арифметические вычисления производятся по модулю n). Таким образом, степень каждой вершины графа равна 8. При достаточно больших n в этом графе не будет кратных рёбер.

Можно показать, что данный граф является спектральным экспандером с параметрами $(n^2, 8, <5\sqrt{2})$, см. O. Gabber and Z. Galil. *Explicit constructions of linear-sized superconcentrators.* J. Comput. System Sci., 22(3):407-420, 1981. Параметры данного экспанедра не оптимальны, однако его очень легко реализовывать на практике.

Графы Рамануджана. В любом регулярном графе степени d второе по абсолютной величине собственное число не может быть меньше $2\sqrt{d-1} - o(1)$. В то же время, для большинства графов второе собственное значение очень близко к этой границе. Таким образом, d-регулярные графы, которые у которых второе по абсолютной величине собственное число ниже границы $2\sqrt{d-1}$, заслуживают особого внимания — это экспандеры с максимальным возможным спектральным зазаором. Такие графы называют *графами Рамануджана*.

Любоцкий, Сарнак, Филлипс и Маргулис указали явную (и алгоритмически эффективную) конструкцию графов Рамануджана. Таким образом, была получена эффективная конструкция спектрального экспандера практически с наилучшими возможными параметрами. Ниже мы опишем эту конструкцию.

Пусть p и q простые числа, $p = 1 \ mod \ 4$ и $q = 1 \ mod \ 4$. Рассмотрим группу $\mathrm{PGL}(2, \mathbb{Z}/q\mathbb{Z})$. Эту группу можно описать так: мы рассматриваем все невырожденные матрицы 2×2 над полем вычетов по модулю q, профакторизованные по отношению пропорциональности (т.е., мы отождествляем

матрицы, получающиеся друг из друга умножением на элемент поля); будем применять к получившимся объектам операцию матричного умножения.

Далее мы выберем в этой группе некоторое множество S. Выберем такое целое i, что $i^2 = -1 \ mod \ q$. Можно доказать, что имеется ровно $(p+1)$ целочисленное решение уравнения

$$a_0^2 + a_1^2 + a_2^2 + a_3^2 = p$$

такое, что a_0 положительно и нечётно, а a_1, a_2, a_3 чётны. Каждой такой четвёрке сопоставим матрицу

$$A = \begin{pmatrix} a_0 + ia_1 & a_2 + ia_3 \\ -a_2 + ia_3 & a_0 - ia_1 \end{pmatrix}.$$

Эти матрицы и образуют множество S. Отметим, что S симметрично: если некоторый элемент группы h принадлежит S, от обратный к нему элемент h^{-1} также лежит в S.

Рассмотрим следующий граф: в качестве вершин возьмём все элементы группы; вершины x и y соединяем ребром, если $x = yh$ для некоторого $h \in S$.

Нетрудно понять, что полученный граф состоит из $\Theta(q^3)$ вершин (число элементов в группе $\mathrm{PGL}(2, \mathbb{Z}/q\mathbb{Z})$), и степень каждой вершины равна $(p+1)$ (по числу элементов в S). Свойства данного графа зависят от соотношения p и q. Рассмотрим случай, когда p является квадратичным вычетом по модулю q. Тогда полученный граф состоит из двух связных компонент (в одной компоненте лежат матрицы, определитель которых является квадратичным вычетом, в другой — матрицы с определителем, являющимся квадратичным невычетом по модулю q). Обозначим $X^{p,q}$ связную компоненту полученного графа. Можно доказать, что у $X^{p,q}$ второе по абсолютной величине собственное число не превосходит $2\sqrt{p}$, т.е., мы получили граф Рамануджана. Однако доказательство этого факта непросто и использует сложную алгебраическую технику, см. P. Sarnak. Some applications of modular forms. Cambridge University Press, 1990. *Русский перевод:* П. Сарнак. Модулярные формы и их приложения. Москва, Фазис, 1998.

Упражнение 24.1 *Реализуйте описанные конструкции графов на своём любимом языке программирования: напишите программу, которая по входу i находит список (номеров) всех вершин графа, соединённых ребром с вершиной номер i.*