УДК 519.17 DOI 10.17223/2226308X/11/35

К ВОПРОСУ О МАКСИМАЛЬНОМ ЧИСЛЕ ВЕРШИН В ПРИМИТИВНЫХ РЕГУЛЯРНЫХ ГРАФАХ С ЭКСПОНЕНТОМ 3

И. В. Лось, М. Б. Абросимов

Найдено число примитивных регулярных графов со степенью $p \leqslant 9$, числом вершин $n \leqslant 16$ и экспонентом 3 для всех пар (n, p). Получена оценка сверху на максимальное число вершин в примитивных регулярных графах с экспонентом 3 в зависимости от p: $n_p \leqslant 3(p-1) + 2(p-2)(p-1) + (p-2)^2(p+1)$. Найдено точное значение максимального числа вершин в примитивных регулярных графах со степенью 3 и экспонентом 3: $n_3 = 12$.

Ключевые слова: *примитивный граф, регулярный граф, максимальное число вершин.*

Неотрицательная квадратная матрица A называется *примитивной*, если существует натуральное k, такое, что A^k положительна. Минимальное такое значение k называется *экспонентом* матрицы A [1]. Понятие примитивности легко переносится на графы. Большой интерес в области криптографии представляют примитивные ориентированные графы, которые используются для анализа качества перемешивания входных данных при итеративных преобразованиях информации. Экспонент определяет минимальное количество итераций, после выполнения которых каждый бит выходного значения зависит от всех битов входных данных. Достаточно много работ посвящено и примитивности неориентированных графов [2, 3]. В данной работе рассматриваются простые регулярные неориентированные графы. Напомним некоторые определения.

Регулярным, или *однородным*, графом *порядка* p называется граф, все вершины которого имеют степень p. *Диаметром* $\mathrm{d}(G)$ связного графа G называется длина наибольшего пути между всеми парами вершин графа G. Связный граф G называется *примитивным*, если между любой парой вершин этого графа (в том числе из вершины в саму себя) существует маршрут длины k для некоторого $k \in \mathbb{N}$. Минимальное такое число k называется *экспонентом* графа и обозначается $\exp(G)$.

Ряд работ посвящён исследованию примитивных регулярных графов [4 – 7]. Один из вопросов — при каком числе вершин могут существовать примитивные регулярные графы с заданным экспонентом. В [7] рассмотрен такой вопрос для экспонента 2. В данной работе получены результаты для регулярных примитивных графов с экспонентом 3.

Был проведён вычислительный эксперимент с использованием кластера высокопроизводительных вычислений ПРЦ НИТ СГУ по подсчёту регулярных графов с экспонентом, равным 3, в рамках которого построена таблица числа примитивных регулярных графов со степенью $p \leqslant 9$, числом вершин $n \leqslant 16$ и экспонентом 3. Для этого написана программа на языке C++. Генерация всех связных регулярных графов степени p с фиксированным числом вершин n производилась с помощью генератора графов genreg [8]. Затем для каждого из сгенерированных графов проверялось, равен ли экспонент 3.

Для этого матрица смежности графа возводилась в степень 3 и полученная матрица проверялась на отсутствие нулей. Важно отметить, что при текущих ограничениях на $n \leqslant 16$ строки матрицы можно хранить в виде двоичных масок в любом 32-битном типе данных, например в типе int. В этом случае перемножение двух матриц сводится к последовательному применению побитовой операции & к парам чисел, хранящих

нужные строки матриц, если вторую матрицу хранить в транспонированном виде. Это позволяет выполнять умножение двух матриц за время порядка $\mathrm{O}(n^2)$. Для возведения матрицы в степень можно воспользоваться алгоритмом бинарного возведения в степень [9], который позволяет возводить число или матрицу в степень k за $\mathrm{O}(\log k)$ действий, что даёт итоговую временную сложность решения $\mathrm{O}(n^2 \log k)$. Так как в нашем случае $k = 3$, имеем временную сложность $\mathrm{O}(n^2)$.

На рис. 1 приводится результат работы программы — число графов с экспонентом 3 для различных n и p. Символ «$-$» означает, что графов с такими n и p не существует. Это может быть в двух случаях: $p \geqslant n$ или произведение pn нечётно. Серый фон клетки означает, что все связные регулярные графы со степенью p и числом вершин n имеют экспонент 2. В работе [7] показано, что это верно при $p > n/2$. Для клеток $(n = 16, p = 7)$ и $(n = 16, p = 8)$ значения ещё не посчитаны, так как их вычисление требует очень больших вычислительных ресурсов ввиду количества таких графов (порядка 730 миллиардов).

n	p						
	3	4	5	6	7	8	9
4	0	–	–	–	–	–	–
5	–	0	–	–	–	–	–
6	1	0	0	–	–	–	–
7	–	0	–	0	–	–	–
8	1	3	0	0	0	–	–
9	–	11	–	0	–	0	–
10	1	41	35	0	0	0	0
11	–	143	–	0	–	0	–
12	1	568	7 506	2 391	0	0	0
13	–	2 403	–	232 080	–	0	–
14	0	10 377	3 093 569	18 801 129	2 757 433	0	0
15	–	42 197	–	1 429 344 906	–	0	–
16	0	151 684	1 797 671 946	112 705 503 963	In progress	In progress	0

Рис. 1. Число графов с экспонентом 3 для различных n и p

Очевидно, что у примитивного графа с экспонентом 3 диаметр может быть 2 или 3. Для упрощения дальнейших рассуждений доказано вспомогательное утверждение — необходимое условие примитивности графа с экспонентом 3.

Утверждение 1. В примитивном графе с экспонентом 3 каждая вершина должна лежать хотя бы на одном цикле длины 3.

Условие не является достаточным. Получены некоторые достаточные условия примитивности графа с экспонентом 3, которые не являются необходимыми.

Утверждение 2. Если в графе G с диаметром $\mathrm{d}(G) \leqslant 3$ каждое ребро входит в состав некоторого цикла длины 3, то граф G является примитивным с экспонентом $\exp(G) \leqslant 3$, причём если $\mathrm{d}(G) = 3$, то и $\exp(G) = 3$.

Условие можно усилить.

Утверждение 3. Если в графе G с диаметром $\mathrm{d}(G) \leqslant 3$ из каждой пары смежных рёбер хотя бы одно входит в состав некоторого цикла длины 3, то граф G является примитивным с экспонентом $\exp(G) \leqslant 3$, причём если $\mathrm{d}(G) = 3$, то и $\exp(G) = 3$.

Обозначим через n_p максимально возможное число вершин в регулярном примитивном графе с порядком p и экспонентом 3.

Во-первых, доказана теорема, устанавливающая верхнюю оценку на n_p в зависимости от порядка графа p.

Теорема 1. Для максимально возможного числа вершин в регулярном примитивном графе с экспонентом 3 и порядком p имеет место неравенство

$$n_p \leqslant 3(p-1) + 2(p-2)(p-1) + (p-2)^2(p+1).$$

В частности, имеем $n_3 \leqslant 14$, $n_4 \leqslant 41$ и $n_5 \leqslant 90$.

Во-вторых, удалось получить точное значение n_3.

Теорема 2. Не существует кубических примитивных графов с экспонентом 3 и с числом вершин больше 12.

На рис. 2 изображён 12-вершинный кубический граф с экспонентом 3.

Следствие 1. $n_3 = 12$.

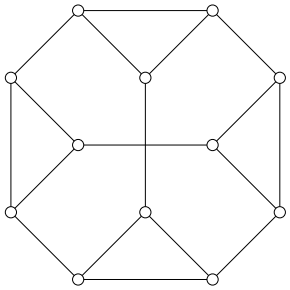

Рис. 2. 12-вершинный кубический граф с $\exp(G) = 3$

ЛИТЕРАТУРА

1. *Wielandt H.* Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. B. 52. S. 642–648.
2. *Князев А. В.* Оценки экстремальных значений основных метрических характеристик псевдосимметрических графов: дис. ... докт. физ.-мат. наук. М., 2002. 203 с.
3. *Когос К. Н., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
4. *Jin M., Lee S. G., and Seol H. G.* Exponents of r-regular primitive matrices // Inform. Center Math. Sci. 2003. V. 6. No. 2. P. 51–57.
5. *Bueno M. I. and Furtado S.* On the exponent of r-regular primitive matrices // Electronic J. Linear Algebra. 2008. V. 17. P. 28–47.
6. *Kim B., Song B., and Hwang W.* Nonnegative primitive matrices with exponent 2 // Linear Algebra and its Appl. 2005. No. 407. P. 162–168.
7. *Абросимов М. Б., Костин С. В.* К вопросу о примитивных однородных графах с экспонентом, равным 2 // Прикладная дискретная математика. Приложение. 2017. № 10. С. 131–134.
8. *Meringer M.* Fast Generation of Regular Graphs and Construction of Cages // J. Graph Theory. 1999. V. 30. P. 137–146.
9. *Смарт Н.* Алгоритмы возведения в степень // Криптография. М.: Техносфера, 2005.