ЛИТЕРАТУРА

1. *Hayes J. P.* A graph model for fault-tolerant computing system // IEEE Trans. Comput. 1976. V. C25. No. 9. P. 875–884.
2. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012. 192 с.
3. *Абросимов М. Б.* Минимальные вершинные расширения направленных звезд // Дискретная математика. 2011. Т. 23. №2. С. 93–102.
4. *Абросимов М. Б., Долгов А. А.* Семейства точных расширений турниров // Прикладная дискретная математика. 2008. №1. С. 101–107.

УДК 519.6 DOI 10.17223/2226308X/8/43

УСЛОВИЯ ПРИМИТИВНОСТИ СИСТЕМЫ ДВУХ ГРАФОВ

Я. Э. Авезова, В. М. Фомичев

Получены достаточные условия примитивности системы двух n-вершинных орграфов в случае, когда один из орграфов не содержит ациклических вершин, в частности, когда содержит гамильтонов контур. Получена оценка экспонента системы двух орграфов через экспонент их произведения. Результаты могут быть использованы для оценки перемешивающих свойств итеративных функций, построенных на основе разветвления преобразования на два заданных преобразования.

Ключевые слова: *примитивный граф, экспонент графа, гамильтонов цикл.*

Пусть $S = \{A, B\}$ — система двух неотрицательных матриц порядка n. Получим условия, при которых система S является примитивной. По определению система S примитивная, если мультипликативная полугруппа $\langle A, B\rangle$ содержит положительную матрицу. Длина наименьшего слова в алфавите S, соответствующего положительной матрице, называется экспонентом системы S, обозначается $\exp S$. Далее слово $w = C_1 \cdot \ldots \cdot C_l$ в алфавите S (то есть $C_i \in S$, $i = 1, \ldots, l$) отождествляется с матрицей, равной произведению $C_1 \cdot \ldots \cdot C_l$.

Один из способов получения оценки $\exp S$ состоит в построении примитивного слова w. Если длина слова w равна l, то $\exp S \leqslant l \cdot \exp w$. Получим условия на матрицы A и B, при которых слово AB примитивное. Воспользуемся аппаратом теории графов, что при исследовании примитивности равносильно. Если Γ_1 есть часть графа Γ_2, то обозначим это $\Gamma_1 \leqslant \Gamma_2$.

Обозначим $\Gamma(A)$ n-вершинный орграф с матрицей смежности A. Пусть орграф $\Gamma(A)$ не содержит ациклических вершин, то есть состоит из k непересекающихся компонент сильной связности, $1 \leqslant k \leqslant n$.

Лемма 1. Если $\Gamma(B)$ имеет петли в каждой вершине, то $\Gamma(A) \leqslant \Gamma(AB)$.

Следствие 1. В условиях леммы множество простых контуров орграфа $\Gamma(AB)$ содержит все простые контуры орграфа $\Gamma(A)$.

Для орграфа $\Gamma(A)$, не содержащего ациклических вершин, построим k-вершинный орграф $\Gamma_A(B)$ с помощью отождествления некоторых вершин орграфа $\Gamma(B)$: вершины i и j орграфа $\Gamma(B)$ отождествляются, если и только если эти вершины принадлежат одной компоненте сильной связности орграфа $\Gamma(A)$.

Лемма 2. Если орграф $\Gamma_A(B)$ сильносвязный, то орграф $\Gamma(AB)$ тоже сильносвязный.

В соответствии с универсальным критерием примитивности [1], орграф Γ примитивный, если и только если Γ сильносвязный и длины его простых контуров взаимно просты. Используя универсальный критерий, получим достаточные условия примитивности орграфа $\Gamma(AB)$.

Теорема 1. Пусть орграф $\Gamma(A)$ содержит контуры длин $l_1, \ldots, l_k$, $(l_1, \ldots, l_k) = 1$, орграф $\Gamma(B)$ имеет петли в каждой вершине, орграф $\Gamma_A(B)$ сильносвязный. Тогда орграф $\Gamma(AB)$ примитивный и $\exp S \leqslant 2 \exp(AB)$.

Пусть орграф $\Gamma(A)$ гамильтонов. Не ограничивая общности, положим, что полный цикл есть $(1, 2, \ldots, n)$. Тогда в орграфе $\Gamma(B)$ вершине i с полустепенью исхода q_i соответствует множество дуг $\{(i, b_{i,1}), \ldots, (i, b_{i,q_i})\}$, $i = 1, \ldots, n$. Обозначим

$$d_B = \text{НОД}(\rho(i, b_{i,j})\colon i = 1, \ldots, n, j = 1, \ldots, q_i),$$

где $\rho(i, j) = i - j$, если $i \geqslant j$, и $\rho(i, j) = n + i - j$, если $i < j$.

Теорема 2. Пусть орграф $\Gamma(A)$ содержит гамильтонов цикл $(1, 2, \ldots, n)$, орграф $\Gamma(B)$ имеет петли в каждой вершине и $(n, d_B) = 1$. Тогда орграф $\Gamma(AB)$ примитивный и $\exp S \leqslant 2 \exp(AB)$.

Пример 1. На рис. 1 иллюстрируется теорема 1 для матриц порядка 6 (6-вершинных графов). При отождествлении вершинам $1, 2, 3$ орграфов $\Gamma(A)$ и $\Gamma(B)$ соответствует вершина α в $\Gamma_A(B)$, вершинам $4, 5$ — вершина β, вершине 6 — вершина γ.

$$A = \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&0&0&0&0&0\\ 0&0&0&0&1&0\\ 0&0&0&1&0&0\\ 0&0&0&0&0&1 \end{pmatrix} \quad B = \begin{pmatrix} 1&0&0&1&0&0\\ 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 0&0&0&1&0&0\\ 0&0&0&0&1&1\\ 0&0&1&0&0&1 \end{pmatrix} \quad AB = \begin{pmatrix} 0&1&0&0&0&0\\ 0&0&1&0&0&0\\ 1&0&0&1&0&0\\ 0&0&0&0&1&1\\ 0&0&0&1&0&0\\ 0&0&1&0&0&1 \end{pmatrix}$$

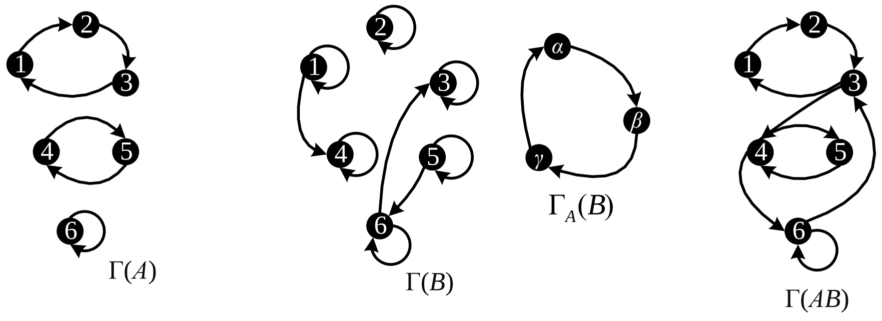

Рис. 1. Пример, иллюстрирующий теорему 1

Полученные результаты могут быть использованы для оценки перемешивающих свойств итеративных функций, построенных на основе разветвления преобразования на два заданных преобразования [2].

ЛИТЕРАТУРА

1. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 116–121.
2. *Когос К. Г., Фомичев В. М.* О разветвлениях криптографических функций на преобразования с заданным признаком // Прикладная дискретная математика. 2012. № 1(15). С. 50–54.