3. *Harary F. and Hayes J. P.* Node fault tolerance in graphs // Networks. 1996. V. 27. P. 19–23.
4. *Mukhopadhyaya K. and Sinha B. P.* Hamiltonian graphs with minimum number of edges for fault-tolerant topologies // Inform. Process. Lett. 1992. V. 44. P. 95–99.
5. *Hsu L. H. and Lin C. K.* Graph Theory and Interconnection Networks. CRC Press, 2009.
6. *Абросимов М. Б.* О неизоморфных оптимальных 1-отказоустойчивых реализациях некоторых графов // Теоретические проблемы информатики и её приложений. Саратов: СГУ, 2000. Вып. 3. С. 3–10.
7. *Абросимов М. Б.* О неизоморфных минимальных реберных 1-расширениях графов // Теоретические проблемы информатики и её приложений. Саратов: СГУ, 2004. Вып. 6. С. 3–9.
8. *Абросимов М. Б.* Графовые модели отказоустойчивости. Саратов: Изд-во Сарат. ун-та, 2012.
9. *Абросимов М. Б.* О сложности некоторых задач, связанных с расширениями графов // Матем. заметки. 2010. № 5(88). С. 643–650.
10. *Абросимов М. Б.* Минимальные вершинные расширения циклов с числом вершин не более одиннадцати. Саратов: СГУ, 2001. 17 с. Деп. в ВИНИТИ 14.08.2001, № 1869-В2001.
11. *Абросимов М. Б., Кузнецов Н. А.* О количестве минимальных вершинных и рёберных 1-расширений циклов с числом вершин до 17 // Прикладная дискретная математика. Приложение. 2012. № 5. С. 84–86.
12. *Бринкман Г., Абросимов М. Б.* О количестве минимальных расширений циклов с числом вершин до 26 и 28 // Дискретная математика, теория графов и их приложения: Тез. докл. Междунар. науч. конф. Минск, 11–14 ноября 2013 г. Мн.: Институт математики НАН Беларуси, 2013. С. 7–9.
13. *Brinkmann G.* Fast generation of cubic graphs // J. Graph Theory. 1996. V. 23. P. 139–140.
14. *Brinkmann G., Goedgebeur J., and McKay B. D.* Generation of cubic graphs // Discr. Math. Theor. Comp. Sci. 2011. V. 13(2). P. 69–80.
15. *Grund R.* Konstruktion schlichter Graphen mit gegebener Gradpartition // Bayreuther Mathematische Schriften. 1993. B. 44. S. 73–104.
16. *Сухов С. А.* DSR Generator. Свид. о гос. регистрации программы для ЭВМ № 2016610073. Зарегистрирована в Реестре программ для ЭВМ 11 января 2016 г.

УДК 519.1 DOI 10.17223/2226308X/9/41

ОБ ОДНОМ НАСЛЕДСТВЕННОМ ПРИЗНАКЕ В ЦИКЛИЧЕСКИХ ПОЛУГРУППАХ ГРАФОВ

Я. Э. Авезова, В. М. Фомичев

В циклической полугруппе орграфов исследован признак наличия петель в вершинах из заданного множества. Для показателя этого признака через длины контуров орграфа (образующего элемента циклической полугруппы) получены достижимые оценки и формулы для подсчёта точного значения. Применение формул показано на примере. Результаты позволяют оценить экспоненты широкого класса примитивных систем орграфов.

Ключевые слова: *признак, показатель признака, экспонент системы графов.*

Введение

Важной задачей в криптографических приложениях является определение экспонента системы орграфов $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_m\}$, обозначаемого $\exp \hat{\Gamma}$ (равносильное определение экспонента системы матриц дано в [1, с. 202]). Один из способов получения оценки $\exp\hat{\Gamma}$ основан на построении примитивного орграфа Γ', являющегося словом в алфавите $\hat{\Gamma}$, то есть элементом полугруппы $\langle\hat{\Gamma}\rangle$, и оценке $\exp\Gamma'$, где, согласно универсальному критерию примитивности [2], орграф Γ' примитивный, если и только если он сильносвязный и имеет простые контуры взаимно простых длин.

Примитивный орграф Γ' может быть получен как произведение непримитивных орграфов, составляющих некоторую систему. Одно из условий примитивности орграфа Γ' связано, в частности, с наличием петель в определённом подмножестве вершин орграфа Γ_j^t при некотором $j \in \{1, \ldots, m\}$ и некотором натуральном t. В частности, пример такой системы $\hat{\Gamma}$ из двух графов рассмотрен в [3]. Настоящая работа посвящена исследованию свойства орграфа, связанного с наличием петель в определённом подмножестве вершин.

1. Полугрупповой признак наличия петель в заданном подмножестве вершин орграфов

Подмножество H полугруппы G, состоящее из всех элементов G, обладающих определённым свойством, называется признаком H (H-признаком) в полугруппе G. Если $H \leqslant G$ — подполугруппа, то H называется полугрупповым признаком в G [1, с. 178].

Пусть G — полугруппа орграфов с множеством вершин $V = \{1, \ldots, n\}$, $\varnothing \neq P \subseteq V$. В полугруппе G полугрупповым признаком (обозначим его P_{loop}) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P.

Пусть $\Gamma \in G$. Обозначим $\langle\Gamma\rangle$ циклическую полугруппу, порождённую орграфом Γ. Показателем P_{loop}-признака в полугруппе $\langle\Gamma\rangle$ называется наименьшее натуральное t, при котором $\Gamma^t \in P_{\text{loop}}$ (обозначается $\operatorname{pok} P_{\text{loop}}$ или кратко l_P). Заметим, что $l_V = \operatorname{ord} g$, если Γ — граф подстановки g множества V.

Утверждение 1. Признак P_{loop} в полугруппе $\langle\Gamma\rangle$ не пуст, если и только если каждая вершина из P является циклической.

2. Оценки показателя признака наличия петель в заданном подмножестве вершин орграфов

Рассмотрим орграф Γ, все вершины которого из множества P являются циклическими. Обозначим в Γ: $\hat{C} = \{C_1, \ldots, C_k\}$ — множество k простых контуров; $l(C)$ — длина контура C; $V(C)$ — множество вершин контура C; $L(i)$ — множество длин контуров, проходящих через вершину i; $L^{[m]}(i)$ — множество не превосходящих натурального числа m длин контуров, проходящих через вершину i; $\Lambda(i)$ — множество длин простых контуров, проходящих через вершину i; $C_{\min,i}$ — кратчайший простой контур, проходящий через вершину i, $i \in V$.

Утверждение 2. Показатель признака P_{loop} равен

$$l_P = \min \bigcap_{i \in P} L(i). \tag{1}$$

Поскольку через каждую вершину $i \in P$ проходит бесконечно много контуров, применение (1) для вычисления точного значения показателя признака P_{loop} затруднительно. Для уточнения формулы получим ряд оценок l_P.

Запишем, что система контуров $\hat{C} = \{C_1, \ldots, C_k\}$ содержит множество P, если $P \subseteq V(C_1) \cup \ldots \cup V(C_k)$. Систему контуров $\hat{C} = \{C_1, \ldots, C_k\}$ назовём связной, если связной является часть графа Γ, совпадающая с $C_1 \cup \ldots \cup C_k$. Связную систему контуров, содержащую множество P, назовём P-сокращённой, если после удаления любого контура оставшаяся подсистема либо не является связной, либо не содержит множество P. P-сокращённую систему $\hat{C} = \{C_1, \ldots, C_k\}$ назовём минимальной в Γ, если сумма длин её контуров принимает наименьшее значение. Заметим, что P-сокращённых и минимальных систем в орграфе Γ может быть несколько.

Далее полагаем $P = \{1, \ldots, p\}$.

Лемма 1. Пусть орграф Γ содержит связную систему контуров $\hat{C} = \{C_1, \ldots, C_k\}$, $k \geqslant 1$. Тогда в Γ имеется контур длины $l(\hat{C}) = l(C_1)+\ldots+l(C_k)$, обходящий однократно каждый контур системы $\hat{C}$.

Теорема 1. Если в орграфе Γ связная система контуров $\hat{C} = \{C_1, \ldots, C_k\}$ содержит множество P, то верны оценки

$$\max\{l(C_{\min,i})\colon i \in P\} \leqslant l_P \leqslant l(\hat{C}). \tag{2}$$

Верхняя оценка (2) принимает наименьшее значение, если система $\hat{C}$ P-сокращённая и минимальная.

Теорема 2. Для любого разбиения множества $P = P_1 \cup \ldots \cup P_r$ выполнено

$$l_P \leqslant \text{НОК}(l_{P_1}, \ldots, l_{P_r}). \tag{3}$$

Следствие 1 (для минимального разбиения множества P). Верна оценка

$$l_P \leqslant \min\{\text{НОК}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}\}. \tag{4}$$

Оценка (4) позволяет уточнить (1), заменив бесконечные множества конечными.

Следствие 2. При $m = \text{НОК}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}$ выполнено

$$l_P = \min \bigcap_{i \in P} L^{[m]}(i). \tag{5}$$

Уточним равенство (5) с использованием верхней оценки (2).

Следствие 3. Если в Γ связная система контуров $\hat{C}$ содержит множество P, то формула (5) верна при $m = \min\{l(\hat{C}), \min\{\text{НОК}\{(\lambda_1, \ldots, \lambda_p) \in \Lambda(1) \times \ldots \times \Lambda(p)\}\}\}$.

Следствие 4. Пусть орграф Γ содержит компоненты сильной связности $\Gamma_1, \ldots, \Gamma_r$ с множествами вершин $V_1, \ldots, V_r$ соответственно и $P_i = P \cap V_i$, $i = 1, \ldots, r$. Тогда верна оценка (3).

Проиллюстрируем примером полученные результаты для показателя P_{loop}.

Пример 1. Граф Γ (рис. 1) состоит из компонент сильной связности Γ_1 и Γ_2. Компонента сильной связности Γ_1 представляет собой связную систему простых контуров $C_1 = (1, 2, 3)$, $C_2 = (3, 4)$ и $C_3 = (4, 5, 6, 7, 8)$ длин 3, 2 и 5 соответственно. Компонента сильной связности Γ_2 есть связная система простых контуров $C_4 = (9, 10)$, $C_5 = (10, 11)$ и $C_6 = (10, 11, 12)$ длин 2, 2 и 3 соответственно. Для орграфа Γ при некоторых P посчитаны оценки показателя l_P с помощью оценок (2) и (4) (табл. 1 и 2), а также точное значение показателя l_P (табл. 3) с помощью (5) или следствия 3.

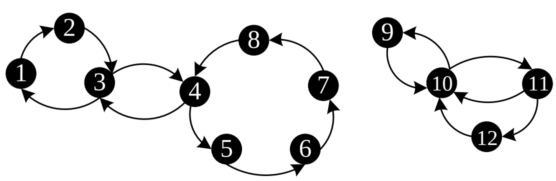

Рис. 1. Орграф Γ

Таблица 1

Верхняя оценка (2) показателя l_P для различных P

P	Минимальная связная система, содержащая P	Оценка (2)
$\{1,5\}$	$\{C_1, C_2, C_3\}$	$l_P \leqslant 3+2+5=10$
$\{1,4\}$	$\{C_1, C_2\}$	$l_P \leqslant 3+2=5$
$\{9,11\}$	$\{C_4, C_5\}$	$l_P \leqslant 2+2=4$

Таблица 2

Верхняя оценка (4) показателя l_P для различных P

P	$\Lambda(i)$, $i \in P$	Оценка (4)
$\{1,5\}$	$\Lambda(1)=\{3\}$, $\Lambda(5)=\{5\}$	$l_P \leqslant \text{НОК}(3,5)=15$
$\{1,4\}$	$\Lambda(1)=\{3\}$, $\Lambda(4)=\{2,5\}$	$l_P \leqslant \min\{\text{НОК}(3,2), \text{НОК}(3,5)\}=6$
$\{9,11\}$	$\Lambda(9)=\{2\}$, $\Lambda(11)=\{2,3\}$	$l_P \leqslant \min\{\text{НОК}(2,2), \text{НОК}(2,3)\}=2$
$\{1,4,9,11\}$	$\Lambda(1)=\{3\}$, $\Lambda(4)=\{2,5\}$, $\Lambda(9)=\{2\}$, $\Lambda(11)=\{2,3\}$	$l_P \leqslant \min\{\text{НОК}(3,2,2,2), \text{НОК}(3,5,2,2)\}$, $\text{НОК}(3,2,2,3), \text{НОК}(3,5,2,3)\}=6$

Таблица 3

Показатель l_P для различных P, посчитанный с помощью (5)

P	m	$L^{[m]}(i)$, $i \in P$	l_P (5)
$\{1,5\}$	10	$L^{[10]}(1)=\{3,5,6,7,8,9,10\}$, $L^{[10]}(5)=\{5,7,9,10\}$	$l_P = \min L^{[10]}(1) \cap L^{[10]}(5) = 5$
$\{1,4\}$	5	$L^{[5]}(1)=\{3,5\}$, $L^{[5]}(4)=\{2,4,5\}$	$l_P = \min L^{[5]}(1) \cap L^{[5]}(4) = 5$
$\{9,11\}$	2	$L^{[2]}(9)=L^{[2]}(11)=\{2\}$	$l_P = 2$
$\{1,4,9,11\}$	6	$L^{[6]}(1)=\{3,5,6\}$, $L^{[6]}(4)=\{2,4,5,6\}$, $L^{[6]}(9)=\{2,4,5,6\}$, $L^{[6]}(11)=\{2,3,4,5,6\}$	$l_P = \min\{5,6\} = 5$

Из табл. 1 следует, что для $P = \{1,5\}$ и $\{1,4\}$ оценка (2) точнее оценки (4), а для $P = \{9,11\}$ соотношение обратное. Для $P = \{1,4,9,11\}$ с помощью следствия 3 получаем оценку $l_P \leqslant \text{НОК}(2,5) = 10$; величина оценки (4) более точная (см. табл. 2), но превышает точное значение, посчитанное в табл. 3.

Результаты показывают, что в некоторых случаях оценки (2) и (4) достижимы. Для многих орграфов с большим числом вершин сложность вычисления оценок показателя l_P по предварительным оценкам меньше, чем сложность определения точного значения. Однако для вычисления по формуле (5) точного значения l_P необходимо вычислить параметр m, являющийся верхней оценкой l_P, и затем построить пересечение множеств $L^{[m]}(1), \ldots, L^{[m]}(p)$.

Перспективное направление дальнейших исследований связано с алгоритмическими вопросами вычисления показателя P_{loop}-признака в полугруппе $\langle\Gamma\rangle$.

Выводы

Доказанные оценки показателя P_{loop}-признака могут быть использованы для оценки экспонентов некоторых примитивных систем орграфов. Полученные условия существенно расширяют область систем орграфов, для которой удаётся получить оценки экспонентов.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.

2. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. №4(18). С. 116–121.

3. *Авезова Я. Э., Фомичев В. М.* Условия примитивности системы двух графов // Прикладная дискретная математика. Приложение. 2015. №8. С. 113–114.

УДК 519.175.3 DOI 10.17223/2226308X/9/42

ПЕРЕЧИСЛЕНИЕ ПОМЕЧЕННЫХ ЦВЕТОЧНО-КОЛЁСНЫХ ГРАФОВ

В. А. Воблый, А. К. Мелешко

Получена точная формула для числа помеченных цветочно-колёсных графов с заданным количеством вершин и лепестков.

Ключевые слова: *корневой граф, граф колесо, цветочно-колёсный граф.*

Точкой сочленения связного графа называется его вершина, после удаления которой вместе с инцидентными ей рёбрами граф становится несвязным. Блок — это связный граф без точек сочленения, а также максимальный связный нетривиальный подграф, не имеющий точек сочленения. Корневой граф имеет одну выделенную вершину, называемую корнем. Колесо W_n — граф с $n \geqslant 4$ вершинами, который образован соединением единственной вершины со всеми вершинами $(n-1)$-цикла [1, с. 63]. Граф W_4 изоморфен полному графу K_4.

Цветочно-колёсный граф с m лепестками — это связный граф с одной точкой сочленения, у которого все m блоков (лепестков) — колёса, причём вершина, являющаяся осью колеса, не может быть точкой сочленения. Цветочно-колёсные графы представляют топологию коммуникационных, компьютерных и других сложных сетей [2]. Кроме того, перечисление графов тесно связано с теорией случайных графов; рандомизация колёсных подграфов сети может использоваться для защиты данных пользователей социальных сетей [3].

Теорема 1. Число $FW(n,m)$ помеченных цветочно-колесных графов с n вершинами и m лепестками при $n \geqslant 7$ и $m \geqslant 2$ равно

$$FW(n,m) = \frac{n!}{m!6^m}\sum_{i=0}^{r}\binom{m}{i}\binom{n-2m-i-2}{m-1}2^i,$$

где $r = \min(m, n-3m-1)$.

Доказательство. Пусть $C_m(z) = \sum\limits_{n=4}^{\infty} FW(n,m)\dfrac{z^n}{n!}$, NW_n — число помеченных колёс с n вершинами, RW_n — число помеченных корневых колёс с n вершинами, $R(z) = \sum\limits_{n=4}^{\infty} RW_n \dfrac{z^n}{n!}$.

Так как метку для оси колеса W_n можно выбрать n способами и число циклов с $n-1$ помеченными вершинами равно $(n-2)!/2$, то $NW_n = n(n-2)!/2$ при $n \geqslant 5$, $NW_4 = 1$.

Поскольку корень колеса W_n не должен быть вершиной-осью колеса, то метку для него можно выбрать $n-1$ способами и при $n \geqslant 5$ имеем $RW_n = (n-1)NW_n = n!/2$. Однако в случае W_4 (полный граф) осью может быть любая вершина и $RW_4 = nNW_4 = 4$. Поэтому имеем

$$R(z) = \frac{z^4}{6} + \frac{1}{2}\sum_{n=5}^{\infty} z^n = \frac{z^4}{6} + \frac{z^5}{2(1-z)}.$$