Секция 5

ПРИКЛАДНАЯ ТЕОРИЯ КОДИРОВАНИЯ, АВТОМАТОВ И ГРАФОВ

УДК 519.1 DOI 10.17223/2226308X/11/31

КРИТЕРИЙ ПРИМИТИВНОСТИ И ОЦЕНКИ ЭКСПОНЕНТОВ МНОЖЕСТВА ОРГРАФОВ С ОБЩИМ МНОЖЕСТВОМ КОНТУРОВ

Я. Э. Авезова

Пусть $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов с множеством вершин V, орграф $U^{(p)}$ — объединение орграфов $\Gamma_1 \cup \ldots \cup \Gamma_p$ без учёта кратности дуг, $p > 1$, и множество простых контуров $\hat{C} = \{C_1, \ldots, C_m\}$, $m \geqslant 1$, является общим для $\hat{\Gamma}$, то есть каждый орграф множества $\hat{\Gamma}$ содержит все контуры множества $\hat{C}$. Для случая $C_1^* \cup \ldots \cup C_m^* = V$, где C_i^* — множество вершин контура C_i, $i = 1, \ldots, m$, получены критерии примитивности и оценки экспонентов множеств орграфов с общими контурами. При $m > 1$ множество орграфов $\hat{\Gamma}$ с общим множеством контуров $\hat{C}$ примитивное, если и только если орграф $U^{(p)}$ примитивный, и $\exp\hat{\Gamma} \leqslant$ $\leqslant ((p-1)h + 1)\exp U^{(p)}$, где h — показатель V_{loop}-признака в полугруппе $\langle\Gamma(\hat{C})\rangle$, $\Gamma(\hat{C}) = C_1 \cup \ldots \cup C_m$ (наименьшее натуральное число h, при котором $\big(\Gamma(\hat{C})\big)^h$ имеет петли во всех вершинах). При $m = 1$ критерий примитивности и оценка экспонента уточнены: если все орграфы множества $\hat{\Gamma}$ имеют общий гамильтонов контур, то множество $\hat{\Gamma}$ примитивное, если и только если НОД длин всех простых контуров $U^{(p)}$ равен 1, и $\exp\hat{\Gamma} \leqslant (2n-1)p + \sum\limits_{\tau=1}^{p}(F(L_\tau) + d_\tau - l_1^\tau)$, где $L_\tau = \{l_1^\tau, \ldots, l_{m(\tau)}^\tau\}$ — множество длин всех простых контуров орграфа Γ_τ, $l_1^\tau < \ldots < l_{m(\tau)}^\tau = n$, $d_\tau = \text{НОД}(L_\tau)$, $L_\tau/d_\tau = \{l_1^\tau/d_\tau, \ldots, l_{m(\tau)}^\tau/d_\tau\}$, $F(L_\tau) =$ $= d_\tau\Phi(L_\tau/d_\tau)$, $\Phi(L_\tau/d_\tau)$ — число Фробениуса, $\tau = 1, \ldots, p$.

Ключевые слова: *гамильтонов контур, показатель признака, примитивность множества орграфов, экспонент орграфа, экспонент множества орграфов.*

Введение

Пусть $\hat{\Gamma} = \{\Gamma_1, \ldots, \Gamma_p\}$ — множество орграфов с множеством вершин $V = \{0, \ldots, n-1\}$, все дуги орграфа Γ_τ помечены числом τ, $\tau = 1, \ldots, p$, $p > 1$. Множеству $\hat{\Gamma}$ соответствует мультиграф $\Gamma^{(p)} = \Gamma_1 \cup \ldots \cup \Gamma_p$, в котором любой путь длины s помечен непустым множеством слов длины s. Орграф, полученный из $\Gamma^{(p)}$ удалением всех меток и отождествлением кратных дуг, будем обозначать $U^{(p)}$. Если множество $\hat{\Gamma}$ примитивное, то мультиграф $\Gamma^{(p)}$ и орграф $U^{(p)}$ сильносвязные [1, 2]. Множество $\hat{\Gamma}$ примитивное, если и только если при некотором натуральном s существует метка $w_1 \ldots w_s$ (слово длины s в алфавите $\{1, \ldots, p\}$), такая, что имеется путь из i в j с этой меткой при любых $i, j \in V$ [3]. Наименьшее такое s называется экспонентом множества $\hat{\Gamma}$ и обозначается $\exp\hat{\Gamma}$. Примитивность множества орграфов — одно из обобщений понятия примитивности, которое является ключевым в матрично-графовом подходе к исследованию перемешивающих свойств итеративных блочных шифров и генераторов гаммы. Оценка экспонента произвольного множества орграфов является сложной задачей. В [3, 4]

получены условия примитивности и оценки экспонентов некоторых частных классов множеств перемешивающих орграфов регистровых преобразований. Особенностью таких орграфов является наличие гамильтонова контура. В данной работе представлено обобщение результатов [3, 4], в частности получены критерий примитивности и универсальная оценка экспонента для множества орграфов с общим гамильтоновым контуром, а также критерий примитивности и оценка экспонента множества орграфов с общим множеством контуров.

1. Критерий примитивности множества орграфов с общим гамильтоновым контуром

Введем обозначения: $\langle X\rangle$ — подполугруппа, порождённая подмножеством X мультипликативной полугруппы; если $L=\{l_1,\ldots,l_m\}\subset\mathbb{N}$, то НОД$(L)=(l_1,\ldots,l_m)=d$ — наибольший общий делитель чисел $l_1,\ldots,l_m$; при $d=1$: $\Phi(L)=\Phi(l_1,\ldots,l_m)$ — число Фробениуса, т. е. наибольшее целое число, не принадлежащее аддитивной полугруппе $\langle L\rangle$; при $d>1$: $L/d=\{l_1/d,\ldots,l_m/d\}$, $F(L)=d\Phi(L/d)$ ($F(L)=\Phi(L)$ при $d=1$).

Контур C называется общим контуром множества $\hat{\Gamma}$, если каждый орграф этого множества имеет контур C. Установлен критерий примитивности множества $\hat{\Gamma}$ с общим гамильтоновым контуром.

Теорема 1. Пусть $\hat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$ — множество орграфов с общим гамильтоновым контуром, $p>1$. Множество $\hat{\Gamma}$ примитивное, если и только если НОД длин всех простых контуров орграфа $U^{(p)}$ равен 1. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp\hat{\Gamma}\leqslant(2n-1)p+\sum_{\tau=1}^{p}\bigl(F(L_\tau)+d_\tau-l_1^\tau\bigr). \tag{1}$$

2. Критерий примитивности множества орграфов с общим множеством контуров

При исследовании примитивности множества орграфов с общим множеством контуров обратимся к понятию признака наличия петель в орграфе в вершинах из заданного множества [5]. Подмножество H полугруппы G, состоящее из всех элементов G, обладающих определённым свойством, называется признаком H (H-признаком) в полугруппе G [1, с. 178]. В мультипликативной полугруппе всех n-вершинных орграфов признаком (обозначается P_{loop}) является, в частности, множество всех орграфов, имеющих петли в каждой вершине множества P, $\varnothing\neq P\subseteq V$. Показателем P_{loop}-признака в циклической полугруппе $\langle\Gamma\rangle$ называется наименьшее натуральное h, при котором $\Gamma^h\in P_{\text{loop}}$. Оценки и точное значение показателя P_{loop}-признака получены в [5].

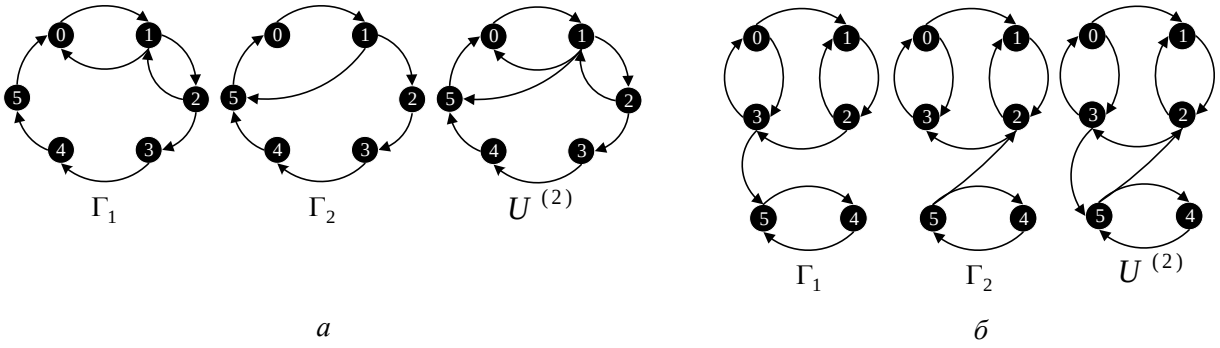
В орграфе Γ обозначим C^* — множество вершин контура C; $\hat{C}=\{C_1,\ldots,C_m\}$ — множество простых контуров, $m>1$; $\Gamma(\hat{C})=C_1\cup\ldots\cup C_m$ — часть орграфа Γ.

Теорема 2. Пусть $\hat{\Gamma}=\{\Gamma_1,\ldots,\Gamma_p\}$ — множество орграфов с общим множеством контуров $\hat{C}=\{C_1,\ldots,C_m\}$, $p,m>1$, $C_1^*\cup\ldots\cup C_m^*=V$. Множество $\hat{\Gamma}$ примитивное, если и только если орграф $U^{(p)}$ примитивный. Для экспонента примитивного множества орграфов $\hat{\Gamma}$ верна оценка

$$\exp\hat{\Gamma}\leqslant\bigl((p-1)h+1\bigr)\exp U^{(p)}, \tag{2}$$

где h — показатель V_{loop}-признака в полугруппе $\langle\Gamma(\hat{C})\rangle$.

Пример 1. На рис. 1 представлено множество орграфов $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ с общим множеством контуров при $n = 6$. В таблице приведены оценки $\exp\hat{\Gamma}$. На рис. 1, *а* $\Gamma(\hat{C})$ сильносвязный, на рис. 1, *б* $\Gamma(\hat{C})$ не является сильносвязным, в обоих случаях орграфы Γ_1 и Γ_2 непримитивные. Множество $\hat{\Gamma}$ примитивное по теоремам 1 и 2.



а *б*

Рис. 1. Множество $\hat{\Gamma} = \{\Gamma_1, \Gamma_2\}$ и соответствующий орграф $U^{(2)}$

$\hat{\Gamma}$	Общее множество простых контуров $\hat{C}$	h	$\exp U^{(2)}$	$\exp\hat{\Gamma}$	Оценка (1)	Оценка (2)
Рис. 1, *а*	$\{(0,1,\ldots,5)\}$	6	9	11	17	63
Рис. 1, *б*	$\{(0,1,2,3),(0,3),(1,2),(4,5)\}$	2	6	8	–	18

Выводы

Критерий примитивности множества орграфов с общим гамильтоновым контуром (теорема 1) уточняет критерий примитивности множества орграфов с общим множеством контуров (теорема 2). Если общее множество контуров орграфов содержит гамильтонов контур, оценка (1) существенно улучшает оценку (2). Как видно из примера, оценка (2) для экспонента множества орграфов на рис. 1, *а* имеет значение $\exp\hat{\Gamma} \leqslant 63$, что существенно больше, чем по оценке (1).

Перспективным направлением дальнейшей работы является исследование условий примитивности и оценка экспонента множества орграфов с общим множеством контуров в случае, когда $C_1^* \cup \ldots \cup C_m^* \subset V$.

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
2. *Фомичев В. М., Мельников Д. А.* Криптографические методы защиты информации. В 2 ч. Ч. 1. Математические аспекты. М.: Юрайт, 2016. 209 с.
3. *Авезова Я. Э., Фомичев В. М.* Условия примитивности и оценки экспонентов множеств ориентированных графов // Прикладная дискретная математика. 2017. № 135. С. 89–101.
4. *Авезова Я. Э.* О примитивности некоторых множеств перемешивающих орграфов регистровых преобразований // Прикладная дискретная математика. Приложение. 2017. № 10. С. 60–62.
5. *Авезова Я. Э., Фомичев В. М.* Об одном наследственном признаке в циклических полугруппах графов // Прикладная дискретная математика. Приложение. 2016. № 9. С. 105–109.