УДК 519.1

СТРУКТУРНЫЕ СВОЙСТВА МИНИМАЛЬНЫХ ПРИМИТИВНЫХ ОРГРАФОВ

Ф. В. Лебедев

ООО «АСП Лабс», г. Москва, Россия

Описаны классы n-вершинных минимальных примитивных орграфов с числом дуг $(n+3)$, приведены их степенные структуры. Установлена зависимость структурных свойств n-вершинных минимальных примитивных орграфов от числа дуг. В частности, получена оценка количества классов таких графов с $(n+k)$ дугами.

Ключевые слова: *примитивная матрица, примитивный орграф, сильносвязный орграф.*

DOI 10.17223/20710410/41/7

STRUCTURAL PROPERTIES OF MINIMAL PRIMITIVE DIGRAPHS

P. V. Lebedev

Ltd «ASP Labs», Moscow, Russia

E-mail: plebedev@asplabs.ru

Let $\Gamma^P(n,m)$ be the set of all minimal primitive n-vertex digraphs with m arcs. The purpose of the research is to describe the new classes of digraphs $\Gamma \in \Gamma^P(n,n+3)$ and their graph degree structures $D(\Gamma)$. This problem is important for the analysis of mixing properties of round transformations, e.g. symmetric iterative block ciphers. A matrix M is said to be primitive if there is a power $M^e = \left(m_{i,j}^{(e)}\right)$ such that $m_{i,j}^{(e)} > 0$ for all i and j; the least power e with this property is called an exponent of M. The conceptions of the primitiveness and exponent of the matrix M expand to the digraph Γ with the adjacency matrix M. The minimal primitive digraph is a digraph of which adjacency matrix loses its primitiveness property after replacing any positive element by zero. The main results of our research are the following: 1) for the minimal primitive digraph $\Gamma \in \Gamma^P(n,n+3)$, graph degree structures $D(\Gamma)$ are described via solutions of the equation $n_{1,2}+n_{2,1}+2n_{1,3}+2n_{2,2}+2n_{3,1}+3n_{1,4}+3n_{2,3}+ +3n_{3,2}+3n_{4,1}+\ldots+(n-2)n_{n-1,1}=6$ and represented in the table of $D(\Gamma)$ values; 2) it is proved that $D(\Gamma)$, for digraphs from the set $\Gamma^P(n,n+k)$, are determined and can be calculated by $D(\Gamma)$ for $\Gamma \in \Gamma^P(n-1,n+k-2)$; 3) it is proved that the number of classes of digraphs $\Gamma^P(n,n+k)$ could be estimated via solutions of the equation $n_{1,2}+n_{2,1}+2n_{1,3}+2n_{3,1}+3n_{1,4}+3n_{4,1}+4n_{1,5}+4n_{5,1}+\ldots+kn_{1,k+1}+kn_{k+1,1}=2k$ and graph degree structures for $\Gamma \in \Gamma^P(n-1,n+k-2)$; 4) $N_3 \leqslant 34$ and $N_2 \leqslant 9$, where N_i is the number of classes in $\Gamma^P(n,n+i)$.

Keywords: *primitive matrix, primitive digraph, strongly connected digraph.*

Введение

Зачастую криптографические преобразования представляют собой систему булевых функций, заданную координатными функциями $f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)$. Особенность такой системы в том, что её надёжность напрямую зависит от перемешивания входов. Чем больше существенных переменных у каждой координатной функции системы, тем она надёжнее. Наилучший эффект достигается тогда, когда каждая координатная функция существенно зависит от каждой переменной, в таком случае имеется так называемое полное перемешивание входов. Перемешивание входов можно охарактеризовать с помощью ориентированного графа, которому можно сопоставить неотрицательную матрицу, называемую матрицей смежности графа, поэтому для исследования связей между элементами удобно применять матрично-графовый подход [1]. Обзор известных результатов по этому направлению дан в [2]. Сложность реализации системы характеризуется, в частности, числом связей (дуг орграфа Γ). Минимальные примитивные матрицы (МПМ) и орграфы (МПО) представляют интерес с точки зрения экономной реализации коммуникативной системы. Результаты исследования МПО содержатся в [3], где описаны структурные свойства n-вершинных МПО с $(n+1)$ и $(n+2)$ дугами.

В данной работе проведено исследование структурных свойств n-вершинных МПО с $(n+3)$ дугами, что является расширением известных результатов и логическим продолжением [3]. Основные обозначения, используемые в работе:

- $\Gamma^P(n, m)$ — множество минимальных примитивных орграфов с числом вершин n и числом дуг m;
- K^* — система контуров;
- $D(\Gamma)$ — степенная структура орграфа Γ;
- $n_{r,s}$ — количество вершин с полустепенью захода r и полустепенью исхода s;
- p_i — полустепень захода вершины i;
- q_i — полустепень исхода вершины i;
- $[i, j]$ — простой путь в орграфе Γ из вершины i в вершину j.

1. Подход к описанию структурных свойств минимальных примитивных орграфов

Заметим, что матрица и соответствующий ей граф одновременно либо примитивны, либо непримитивны, поэтому в работе используется язык теории графов. В [3] вводится понятие степенной структуры орграфа — таблицы положительных чисел $n_{r,s}$ при всех допустимых значениях r и s, описывающих количество заходящих и исходящих дуг вершины n. В [3] также впервые вводятся понятия примитивной (минимальной примитивной) системы контуров — такой, что натянутый на неё подграф примитивен, и K^*-изолированной дуги — не принадлежащей ни одному из контуров системы K^*. В [3] доказаны теоремы, являющиеся основными в области изучения структурных свойств МПО.

Теорема 1 [3]. Если граф $\Gamma \in \Gamma^P(n, m)$ при некоторых натуральных n и m, K^* — примитивная (минимальная примитивная) система контуров в Γ и в Γ имеется K^*-изолированная дуга, то при любом натуральном k имеется орграф Γ_k из $\Gamma^p(n+k, m+k)$, являющийся k-расширением графа Γ и содержащий систему K^*. Если при этом орграф Γ минимальный, то имеется k-расширение Γ_k, являющееся минимальным примитивным графом.

Теорема 2 [3]. При $n \geqslant 3$ орграф $\Gamma \in \Gamma^p(n, n+1)$ тогда и только тогда, когда Γ есть объединение простых контуров взаимно простых длин l и λ, общая часть которых есть путь длины q, где $l > \lambda$; $l + \lambda - q = n + 1$; $0 \leqslant q \leqslant n - 2$; при $q = 2$ общая часть контуров есть вершина.

Классы n-вершинных МПО с $(n+k)$ дугами можно описать системой из двух уравнений, одно из которых перечисляет удвоенное число дуг в графе (в соответствии с теоремой Эйлера [4]), а другое — число вершин в данном графе:

$$2n_{1,1} + 3n_{1,2} + 3n_{2,1} + 4n_{1,3} + 4n_{2,2} + 4n_{31} + \ldots + nn_{n-1,1} = 2(n + k); \quad (1)$$

$$n_{1,1} + n_{1,2} + n_{2,1} + n_{1,3} + n_{2,2} + n_{3,1} + n_{1,4} + n_{2,3} + n_{3,2} + n_{4,1} + \ldots + n_{n-1,1} = n. \quad (2)$$

Систему, состоящую из уравнений (1) и (2), обозначим (*). Решив её, можно описать все классы минимальных примитивных орграфов, принадлежащие $\Gamma^P(n, n+k)$. Заметим, что уравнения системы (*) относятся к классу диофантовых уравнений, описанных в [5], однако интерес представляют только неотрицательные решения, поскольку они являются количественными характеристиками графа. Вычитая из уравнения (1) удвоенное уравнение (2), получим

$$n_{1,1} + n_{2,1} + 2n_{1,3} + 2n_{2,2} + 2n_{3,1} + 3n_{1,4} + 3n_{2,3} + 3n_{3,2} + 3n_{4,1} + \ldots + (n-2)n_{n-1,1} = 2k. \quad (3)$$

При $k = 1$ уравнение (3) имеет вид

$$n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{2,2} + 2n_{3,1} = 2. \quad (4)$$

Уравнение (4) описывает случай, когда число дуг превосходит число вершин орграфа на единицу и имеет два решения в целых неотрицательных числах, соответственно имеется два класса $\Gamma^P(n, n+1)$.

1 к л а с с: $n_{1,2} = n_{2,1} = n_{1,3} = n_{3,1} = 0$, $n_{2,2} = 1$. Пример графа приведен на рис. 1.

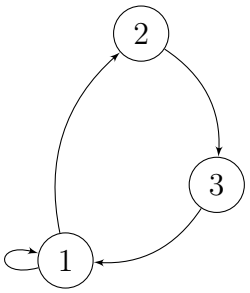

Рис. 1. Граф Γ, $n = 3$, $D(\Gamma) = \{(1,1)^2, (2,2)^1\}$

В соответствии с теоремой 1 степенная структура графов первого класса имеет следующий вид: $D(\Gamma_k) = \{(1,1)^{k+2}, (2,2)^1\}$.

2 к л а с с: $n_{1,2} = n_{2,1} = 1, n_{1,3} = n_{3,1} = 0$. Пример графа представлен на рис. 2. Степенная структура графов второго класса имеет вид $D(\Gamma_k) = \{(1,1)^{k+2}, (1,2)^1, (2,1)^1\}$.

Применяя данный подход к исследованию структурных свойств МПО, приведём ещё одну формулировку теоремы 2.

Теорема 3. Если минимальный примитивный орграф $\Gamma \in \Gamma^P(n, n+1)$, то $D(\Gamma)$ принадлежит классам, описанным в табл. 1.

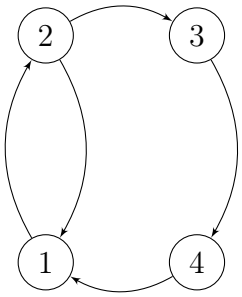

Рис. 2. Граф Γ, $n = 4$, $D(\Gamma) = \{(1,1)^2, (1,2)^1, (2,1)^1\}$

Таблица 1

Классы минимальных примитивных орграфов $\Gamma \in \Gamma^p(n, n+1)$

№ п/п	n	$D(\Gamma)$
1	$\geqslant 3$	$\{(1,1)^{n-1}, (2,2)^1\}$
2	$\geqslant 4$	$\{(1,1)^{n-2}, (1,2)^1, (2,1)^1\}$

Данный подход впервые предложен в [3] и отражён в теореме 4.

Теорема 4. Если минимальный примитивный орграф $\Gamma \in \Gamma^P(n, n+2)$, то $D(\Gamma)$ принадлежит классам, описанным в табл. 2.

Таблица 2

Классы минимальных примитивных орграфов $\Gamma \in \Gamma^p(n, n+2)$

№ п/п	n	$D(\Gamma)$
1	$\geqslant 5$	$\{(1,1)^{n-1}, (3,3)^1\}$
2	$\geqslant 5$	$\{(1,1)^{n-2}, (2,1)^1, (2,3)^1\}$
3	$\geqslant 5$	$\{(1,1)^{n-2}, (1,2)^1, (3,2)^1\}$
4	$\geqslant 5$	$\{(1,1)^{n-2}, (2,2)^2\}$
5	$\geqslant 4$	$\{(1,1)^{n-3}, (3,1)^1, (1,3)^1\}$
6	$\geqslant 6$	$\{(1,1)^{n-3}, (1,3)^1, (2,1)^2\}$
7	$\geqslant 6$	$\{(1,1)^{n-3}, (1,2)^2, (3,1)^1\}$
8	$\geqslant 6$	$\{(1,1)^{n-3}, (2,1)^1, (1,2)^1, (2,2)^1\}$
9	$\geqslant 6$	$\{(1,1)^{n-4}, (2,1)^2, (1,2)^2\}$

Заметим, что с ростом разницы числа дуг и вершин количество решений значительно увеличивается, соответственно сложность описания классов МПО возрастает.

Так как в любом графе сумма всех полустепеней исхода равна сумме всех полустепеней захода, можно сказать, что числа $n_{r,s}$ связаны следующим равенством:

$$\sum k_{r_i,s_i} r_i = \sum k_{r_i,s_i} s_i, \tag{5}$$

где k_{r_i,s_i} — коэффициент при n_{r_i,s_i}, $k_{r_i,s_i} = r_i + s_i - 2$.

2. Структурные свойства n-вершинных МПО с $(n+3)$ дугами

Теорема 5. Если минимальный примитивный орграф $\Gamma \in \Gamma^P(n, n+3)$, то $D(\Gamma)$ принадлежит классам, приведённым в табл. 3.

Таблица 3

Классы минимальных примитивных орграфов $\Gamma \in \Gamma^p(n, n+3)$

№ п/п	n	$D(\Gamma)$
1	$\geqslant 6$	$\{(1,1)^{n-1}, (4,4)^1\}$
2	$\geqslant 6$	$\{(1,1)^{n-2}, (2,1)^1, (3,4)^1\}$
3	$\geqslant 6$	$\{(1,1)^{n-2}, (1,2)^1, (4,3)^1\}$
4	$\geqslant 6$	$\{(1,1)^{n-2}, (2,2)^1, (3,3)^1\}$
5	$\geqslant 7$	$\{(1,1)^{n-3}, (2,1)^1, (1,2)^1, (3,3)^1\}$
6	$\geqslant 5$	$\{(1,1)^{n-2}, (1,3)^1, (4,2)^1\}$
7	$\geqslant 7$	$\{(1,1)^{n-3}, (1,2)^2, (4,2)^1\}$
8	$\geqslant 6$	$\{(1,1)^{n-2}, (3,1)^1, (2,4)^1\}$
9	$\geqslant 7$	$\{(1,1)^{n-3}, (2,1)^2, (2,4)^1\}$
10	$\geqslant 6$	$\{(1,1)^{n-3}, (2,2)^1, (1,2)^1, (3,2)^1\}$
11	$\geqslant 8$	$\{(1,1)^{n-4}, (2,1)^1, (1,2)^2, (3,2)^1\}$
12	$\geqslant 6$	$\{(1,1)^{n-2}, (2,3)^1, (3,2)^1\}$
13	$\geqslant 7$	$\{(1,1)^{n-3}, (1,3)^1, (2,1)^1, (3,2)^1\}$
14	$\geqslant 6$	$\{(1,1)^{n-3}, (2,2)^1, (2,1)^1, (2,3)^1\}$
15	$\geqslant 8$	$\{(1,1)^{n-4}, (1,2)^1, (2,1)^2, (2,3)^1\}$
16	$\geqslant 7$	$\{(1,1)^{n-3}, (3,1)^1, (1,2)^1, (2,3)^1\}$
17	$\geqslant 7$	$\{(1,1)^{n-4}, (2,1)^3, (1,4)^1\}$
18	$\geqslant 7$	$\{(1,1)^{n-3}, (2,1)^1, (3,1)^1, (1,4)^1\}$
19	$\geqslant 7$	$\{(1,1)^{n-4}, (1,2)^3, (4,1)^1\}$
20	$\geqslant 7$	$\{(1,1)^{n-3}, (1,2)^1, (1,3)^1, (4,1)^1\}$
21	$\geqslant 6$	$\{(1,1)^{n-3}, (2,2)^3\}$
22	$\geqslant 7$	$\{(1,1)^{n-4}, (2,2)^2, (1,2)^1, (2,1)^1\}$
23	$\geqslant 5$	$\{(1,1)^{n-4}, (2,2)^2, (1,3)^1, (3,1)^1\}$
24	$\geqslant 7$	$\{(1,1)^{n-5}, (2,2)^1, (1,2)^2, (2,1)^2\}$
25	$\geqslant 7$	$\{(1,1)^{n-4}, (2,2)^1, (1,3)^1, (2,1)^2\}$
26	$\geqslant 7$	$\{(1,1)^{n-4}, (2,2)^1, (3,1)^2, (1,2)^2\}$
27	$\geqslant 7$	$\{(1,1)^{n-5}, (3,1)^1, (2,1)^1, (1,2)^3\}$
28	$\geqslant 6$	$\{(1,1)^{n-4}, (1,3)^1, (3,1)^1, (2,1)^1, (1,2)^1\}$
29	$\geqslant 8$	$\{(1,1)^{n-5}, (1,3)^1, (1,2)^1, (2,1)^3\}$
30	$\geqslant 9$	$\{(1,1)^{n-6}, (1,2)^3, (2,1)^3\}$

Доказательство. Если сильносвязный орграф $\Gamma \in \Gamma^P(n, n+3)$, то числа $n_{r,s}$ связаны системой (*) при $k = 3$. Составим уравнение, описывающее данные классы МПО, аналогично уравнению (4):

$$n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{2,2} + 2n_{3,1} + 3n_{1,4} + 3n_{2,3} + 3n_{3,2} + 3n_{4,1} + \ldots + (n-2)n_{n-1,1} = 6. \quad (6)$$

Определим решения уравнения (6) относительно целых неотрицательных чисел $n_{r,s}$ и укажем примитивные графы без петель, соответствующие полученным решениям. Заметим, что $n_{r,s} = 0$ при $r + s > 8$, следовательно, уравнение (6) равносильно следующему упрощённому уравнению:

$$\begin{gathered} n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{2,2} + 2n_{3,1} + 3n_{1,4} + 3n_{2,3} + 3n_{3,2} + 3n_{4,1} + 4n_{1,5} + 4n_{2,4} + \\ + 4n_{3,3} + 4n_{4,2} + 4n_{5,1} + 5n_{1,6} + 5n_{2,5} + 5n_{3,4} + 5n_{4,3} + 5n_{5,2} + 5n_{6,1} + 6n_{1,7} + \\ + 6n_{2,6} + 6n_{3,5} + 6n_{4,4} + 6n_{5,3} + 6n_{6,2} + 6n_{7,1} = 6. \end{gathered} \quad (7)$$

Пусть $n_{r,s} = 1$, а все остальные переменные равны нулю, тогда в Γ имеется вершина i, где $p_i = r$, $q_i = s$, то есть имеются дуги $(i, a), (i, b), \ldots, (i, r)$, где $i, a, b, \ldots, r$ различны. Орграф Γ — сильносвязный, значит, в Γ имеются простые пути $[a, i], [b, i], \ldots, [r, i]$.

Так как $p_i = s$, эти пути сходятся в s путей, при этом в Γ имеется вершина $j \neq i$, где $p_j \neq s$. Тогда при некоторых r и s имеем противоречие. Таким образом описываются классы МПО в [4]. Имеется 30 классов решения уравнения (7).

1-й к л а с с. Положим $n_{4,4} = 1$. В этом случае Γ есть объединение четырёх контуров, пересечение множеств вершин которых состоит из единственной вершины, а любая другая вершина принадлежит только одному из контуров. Пример графа приведён на рис. 3.

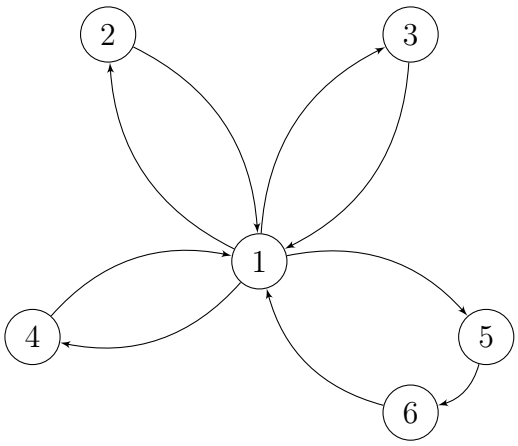

Рис. 3. Граф Γ, $n = 6$, $D(\Gamma) = \{(1,1)^5, (4,4)^1\}$

Степенная структура данного класса МПО имеет вид $D(\Gamma_k) = \{(1,1)^{k+5}, (4,4)^1\}$.

Если $n_{3,5} = 1$, то все остальные переменные в уравнении (7) равны нулю, следовательно, необходима ещё хотя бы одна вершина, чтобы уравнять количество входящих и исходящих дуг в графе. Отсюда следует, что если $n_{i,j} = 1$, $i + j = 8$, $i \neq j$, то уравнение (7) не имеет решений.

Рассмотрим упрощённое уравнение

$$\begin{gathered} n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{2,2} + 2n_{3,1} + 3n_{1,4} + 3n_{2,3} + 3n_{3,2} + 3n_{4,1} + 4n_{1,5} + 4n_{2,4} + \\ + 4n_{3,3} + 4n_{4,2} + 4n_{5,1} + 5n_{1,6} + 5n_{2,5} + 5n_{3,4} + 5n_{4,3} + 5n_{5,2} + 5n_{6,1} = 6, \end{gathered} \tag{8}$$

оно имеет ещё 29 решений. Путём аналогичных рассуждений получаем оставшиеся 29 классов. ■

3. Зависимость структурных свойств n-вершинных МПО от числа дуг

Определение 1. Назовём вершину, у которой полустепень исхода совпадает с полустепенью захода и равна 1, *моновершиной*.

Утверждение 1. Если существует решение уравнения (5) вида $n_{i_1,i_2} = a_1, \ldots, n_{i_m,i_m+1} = a_m$, то $n_{i_2,i_1} = a_1, \ldots, n_{i_m+1,i_m} = a_m$ также является решением уравнения (5).

Следствие 1. Графы, соответствующие таким решениям, изоморфны.

Утверждение 2. Класс МПО $\Gamma^P(n+p, n+p+k)$ образуется добавлением p вершин и $(p+1)$ дуг в соответствующие множества класса $\Gamma^P(n, n+k-1)$.

Доказательство. Количество вершин в полученном графе составит $(n+p)$, а количество дуг — $(n+k-1+p+1) = n+k+p$, отсюда следует, что количество дуг превышает количество вершин на k. ■

Пример 1. На рис. 4 изображён граф $\Gamma_1 \in \Gamma^P(5,7)$ со степенной структурой $D(\Gamma_1) = \{(1,1)^4, (3,3)^1\}$.

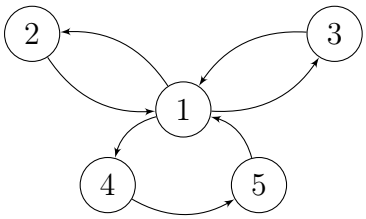

Рис. 4. Граф $\Gamma_1 \in \Gamma^P(5,7)$, $D(\Gamma_1) = \{(1,1)^4, (3,3)^1\}$

Добавим одну вершину и две дуги в соответствующие множества графа Γ_1 так, чтобы получить граф Γ_2, изображённый на рис. 5.

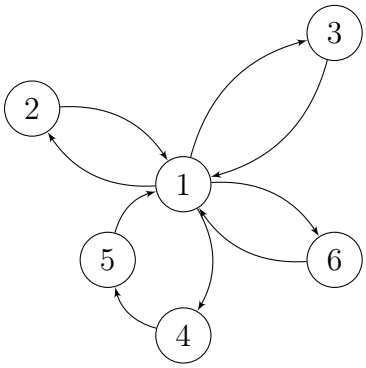

Рис. 5. Граф $\Gamma_2 \in \Gamma^P(6,9)$, $D(\Gamma) = \{(1,1)^5, (4,4)^1\}$

Как видно из рис. 4 и 5, графы Γ_1 и Γ_2 принадлежат множествам МПО, у которых разница между количеством дуг и вершин равна двум и трём соответственно, однако граф Γ_2 имеет на одну вершину больше. Заметим, что изменение степенной структуры говорит об увеличении количества вершин на 1 и количества дуг на 2.

Далее под *типом вершины* понимается характеристика вершины, описывающая количество заходящих и исходящих дуг данной вершины. Важно отметить, что в степенной структуре орграфа описываются все его типы вершин.

Пример 2. Рассмотрим степенную структуру орграфа Γ, принадлежащего 28-му классу $\Gamma^P(n, n+3)$, $D(\Gamma) = \{(1,1)^3, (1,3)^1, (3,1)^1, (2,1)^1, (1,2)^1\}$. Граф Γ имеет пять типов вершин: $(1,1), (1,3), (3,1), (2,1), (1,2)$.

Утверждение 3. Степенные структуры графов из множества $\Gamma^P(n, n+k)$ с точностью до количества моновершин определяются степенными структурами графов из множества $\Gamma^P(n-1, n+k-2)$.

Доказательство. Пусть a и b — вершины графа $\Gamma_1 \in \Gamma^p(n-1, n+k-2)$, при этом допустимо $a = b$. Так как добавляются две новые дуги (обозначим их A и B) и одна новая вершина (обозначим её d), то одна дуга является исходящей из этой вершины, а другая заходящей в неё, значит, $(p_d, q_d) = (1,1)$. Пусть дуга A исходит из a и заходит в d, а дуга B исходит из d и заходит в b, следовательно, степенная структура графа изменится и будет известна с точностью до количества моновершин в силу теоремы 1. ■

Утверждение 4. Степенная структура графа $\Gamma \in \Gamma^p(n, n+k)$ может быть получена из различных степенных структур графов множества $\Gamma^P(n-1, n+k-2)$.

Пример 3. Рассмотрим МПО $\Gamma_1, \Gamma_2 \in \Gamma^P(n, n+2)$, которые представлены на рис. 6, и их степенные структуры для $n = 5$: $D(\Gamma_1) = \{(1,1)^3, (2,1)^1, (2,3)^1\}$, $D(\Gamma_2) = \{(1,1)^3, (1,2)^1, (3,2)^1\}$.

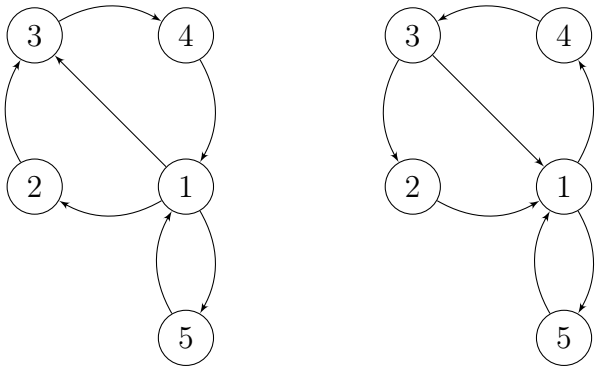

Рис. 6. $\Gamma_1, \Gamma_2 \in \Gamma^P(5, 7)$

Добавив к графу Γ_1 одну вершину и две дуги, можно получить граф Γ_3, такой, что $D(\Gamma_3) = \{(1,1)^3, (3,1)^1, (2,3)^1\}$. Также, определённым образом добавив к графу Γ_2 одну вершину и две дуги, можно получить граф Γ_4, такой, что $D(\Gamma_4) = \{(1,1)^3, (2,3)^1, (3,2)^1\}$. Заметим, что степенные структуры графов Γ_3 и Γ_4, которые представлены на рис. 7, совпадают.

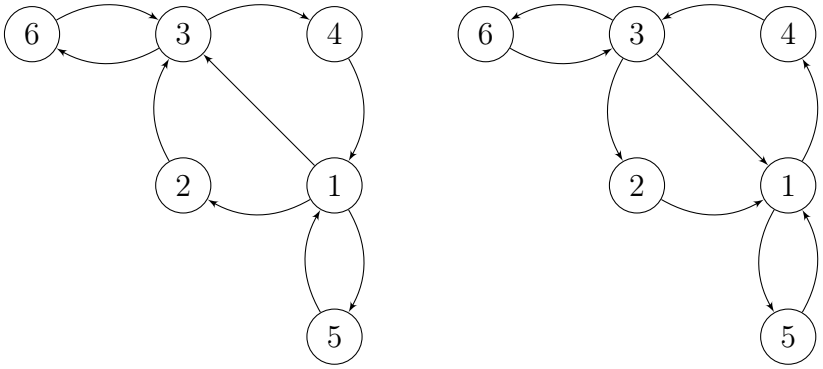

Рис. 7. $\Gamma_3, \Gamma_4 \in \Gamma^P(6, 9)$, $D(\Gamma_3) = D(\Gamma_4) = \{(1,1)^3, (2,3)^1, (3,2)^1\}$

Отметим, что графы Γ_3 и Γ_4 изоморфны и являются частными случаями графов 12-го класса n-вершинных МПО с количеством дуг $(n+3)$ для $n = 6$.

Утверждение 5. Количество классов $\Gamma^P(n, n+k)$ можно оценить с помощью степенных структур классов $\Gamma^P(n-1, n+k-2)$ и количества решений уравнения

$$n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{3,1} + 3n_{1,4} + 3n_{4,1} + 4n_{1,5} + 4n_{5,1} + \ldots + kn_{1,k+1} + kn_{k+1,1} = 2k. \quad (9)$$

Доказательство. Пусть $s_{k-1,i}$ — число типов вершин i-го класса из $\Gamma^P(n-1, n+k-2)$, тогда $\sum\limits_i s_{k-1,i}$ является оценкой сверху количества новых классов, не содержащих вершин, имеющих либо одну заходящую дугу, либо одну исходящую, за

исключением моновершин. С другой стороны, графы $\Gamma \in \Gamma^P(n, n+k)$ такого вида описываются уравнением (9). Пусть t_k — количество решений уравнения (9), N_k — количество классов $\Gamma^P(n, n+k)$. Зная степенные структуры классов $\Gamma^P(n, n+k-1)$, по утверждению 3 можно получить степенные структуры всех классов $\Gamma^P(n, n+k)$, при этом процесс подсчёта новых классов усложняется согласно утверждению 4. Отсюда следует, что $N_k \leqslant \sum\limits_i s_{k-1,i} + t_k$. ■

Пример 4. Рассмотрим классы $\Gamma^P(n, n+2)$. Согласно теореме 4, имеется 9 классов с различными степенными структурами и 26 типов вершин различных классов, описанных в табл. 2. Имеется 8 классов n-вершинных МПО с $(n+3)$ дугами, приведённых в табл. 3 и удовлетворяющих уравнению

$$n_{1,2} + n_{2,1} + 2n_{1,3} + 2n_{3,1} + 3n_{1,4} + 3n_{4,1} = n. \tag{10}$$

Данные классы описаны в табл. 4.

Таблица 4

Классы минимальных примитивных орграфов $\Gamma \in \Gamma^p(n, n+3)$, удовлетворяющих уравнению (10)

№ п/п	n	$D(\Gamma)$
1	$\geqslant 7$	$\{(1,1)^{n-4}, (2,1)^3, (1,4)^1\}$
2	$\geqslant 7$	$\{(1,1)^{n-3}, (2,1)^1, (3,1)^1, (1,4)^1\}$
3	$\geqslant 7$	$\{(1,1)^{n-4}, (1,2)^3, (4,1)^1\}$
4	$\geqslant 7$	$\{(1,1)^{n-3}, (1,2)^1, (1,3)^1, (4,1)^1\}$
5	$\geqslant 8$	$\{(1,1)^{n-5}, (3,1)^1, (2,1)^1, (1,2)^3\}$
6	$\geqslant 7$	$\{(1,1)^{n-4}, (1,3)^1, (3,1)^1, (2,1)^1, (1,2)^1\}$
7	$\geqslant 8$	$\{(1,1)^{n-5}, (1,3)^1, (1,2)^1, (2,1)^3\}$
8	$\geqslant 9$	$\{(1,1)^{n-6}, (1,2)^3, (2,1)^3\}$

Оценим количество классов $\Gamma^P(n, n+3)$, зная степенные структуры классов $\Gamma^P(n, n+2)$: по утверждению 5 верно $N_3 \leqslant 26+8 = 34$; и количество классов $\Gamma^P(n, n+2)$, зная степенные структуры классов $\Gamma^P(n, n+1)$: по утверждению 5 верно $N_2 \leqslant 5+4 = 9$. Заметим, что в данном случае полученная оценка полностью совпадает с количеством классов $\Gamma^P(n, n+2)$.

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. *Фомичев В. М.* Свойства минимальных примитивных орграфов // Прикладная дискретная математика. 2015. № 2 (28). С. 86–96.
4. *Харари Ф.* Теория графов. М.: Едиториал УРСС, 2003. 296 с.
5. *Бухштаб А. А.* Теория чисел. СПб.: Лань, 2008. 384 с.

REFERENCES

1. *Fomichev V. M.* Metody diskretnoy matematiki v kriptologii [Methods of Discrete Mathematics in Cryptology]. Moscow, Dialog-MEPhI Publ., 2010. 324 p. (in Russian)

2. *Kogos K. G. and Fomichev V. M.* Polozhitel'nye svoystva neotritsatel'nykh matrits [Positive properties of non-negative matrices]. Prikladnaya Diskretnaya Matematika, 2012, no. 4(18), pp. 116–121. (in Russian)
3. *Fomichev V. M.* Svoystva minimal'nykh primitivnykh orgrafov [Properties of minimal primitive digraphs]. Prikladnaya Diskretnaya Matematika, 2015, no. 2(28), pp. 86–96. (in Russian)
4. *Harari F.* Graph Theory. Addison-Wesley, 1969.
5. *Bukhshtab A. A.* Teoriya chisel [Number Theory]. SPb., Lan' Publ., 2008. 384 p. (in Russian)