

УДК 519.6

СВОЙСТВА ПУТЕЙ В ГРАФАХ И МУЛЬТИГРАФАХ

В. М. Фомичев

*Институт проблем информатики РАН, г. Москва, Россия***E-mail:** fomichev@nm.ru

Для n -вершинного сильносвязного орграфа оценена длина кратчайшего полного пути и, при наличии петли в графе, экспонент матрицы смежности вершин. Получена полиномиальная оценка субэкспонента системы матриц смежности вершин n -вершинных графов $\Gamma_1, \dots, \Gamma_r$, объединение которых сильно связно. Полученные результаты могут использоваться для исследования существенных переменных координатных функций, определяющих композиции преобразований множества конечных слов.

Ключевые слова: *полный путь, кратчайший путь, экспонент, субэкспонент.*

Введение

Решение ряда прикладных задач методами теории графов часто увязывается с исследованием свойств множества путей в определенных графах. К таким задачам в криптологии относится, например, исследование существенной зависимости функций от переменных [1, гл. 10]. В криптографических системах аутентификации изучение множеств существенных переменных функций важно для построения преобразований, распространяющих искажения [1, 2]. В криптографических системах шифрования эти задачи решаются для оценки эффективности алгебраических атак, основанных на последовательном опробовании элементов ключа [3, с. 397].

Важным понятием в теории графов является расстояние (длина кратчайшего пути) между двумя вершинами графа, которое может определяться двояко для пары одинаковых вершин. Если в транспортных задачах естественно рассматривать графы без петель и предполагать, что расстояние между двумя одинаковыми вершинами равно 0, то в некоторых других задачах, например при исследовании существенной зависимости от переменных композиций функций, допускается наличие петель в графе и полагается, что расстояние от x до x равно длине кратчайшего цикла, проходящего через вершину x . В соответствии с этим следует различать и другие производные понятия теории графов: «эксцентриситет вершины», «радиус графа», «диаметр графа» и др. Часто используются определения первого типа, связанные с расстояниями в графе (см., например, [4, с. 262]); в данной же работе — определения второго типа, которые в большей мере отвечают прикладным задачам криптологии.

Далее в соответствии с [5, 6 и др.] положим, что множество ребер графа, так же как и множество дуг орграфа, может содержать петли, а мультимножество ребер неориентированного (дуг ориентированного) мультиграфа содержит параллельные ребра (дуги), в частности, может содержать параллельные петли. В помеченном мультиграфе параллельные ребра (дуги) различаются, если им присвоены разные метки. Заметим — объединение нескольких графов (орграфов) с одинаковым множеством вершин может быть как графом (орграфом), так и мультиграфом.

Некоторые теоретико-графовые задачи состоят в определении путей с заданными характеристиками (с фиксированными начальной и конечной вершинами, с фиксиро-

ванной длиной) в различных графах и мультиграфах. Напомним [7, с. 143, следствие 1 теоремы 2], что в n -вершинном графе Γ число путей длины ℓ из вершины i в вершину j определяется элементом $m_{ij}^{(\ell)}$ матрицы M^ℓ , где M — матрица смежности вершин графа Γ , $i, j \in \{1, \dots, n\}$, $\ell \geq 1$. Вместе с тем эта теорема может использоваться не во всех случаях. Например:

- 1) указанная теорема требует уточнения для помеченных графов (мультиграфов), чтобы различать пути длины ℓ из i в j с разными метками;
- 2) при больших n, ℓ высока вычислительная сложность подсчета матриц M^ℓ , $\ell \geq 1$.

Данная работа посвящена получению оценок длин путей с определенными свойствами в n -вершинных ориентированных и неориентированных графах и мультиграфах. Без ущерба для общности рассмотрим лишь связные (не обязательно сильносвязные) ориентированные графы и мультиграфы.

1. Свойства систем неотрицательных матриц

Матрица $M = (m_{ij})$ над полем действительных чисел положительна (неотрицательна), если положительны (неотрицательны) все ее элементы. Это свойство записывается так: $M > 0$ ($M \geq 0$). Заметим, что множество квадратных неотрицательных матриц размера n содержит множество матриц смежности вершин n -вершинных графов.

При последовательном возведении в степени $1, 2, \dots, \ell, \dots$ квадратная неотрицательная матрица M может на некотором шаге стать положительной. В этом случае матрица M называется примитивной [8], а наименьшее натуральное ℓ , при котором $M^\ell > 0$, называется экспонентом матрицы M (обозначается $\text{exp } M$). Если такого ℓ не существует, то $\text{exp } M = \infty$.

Субэкспонентом матрицы M (обозначается $\text{sbxp } M$) называется наименьшее натуральное число ℓ , при котором $M_\Sigma^\ell > 0$, где

$$M_\Sigma^\ell = M + M^2 + \dots + M^\ell.$$

Если M — матрица смежности вершин некоторого графа Γ , то в силу следствия 1 теоремы 2 [7, с. 143] $\text{sbxp } M$ совпадает с диаметром графа Γ .

Понятия экспонента и субэкспонента обобщены на систему квадратных неотрицательных матриц $\mathfrak{M} = \{M_1, \dots, M_p\}$ одинакового размера [1, гл. 10]. Пусть $N_p = \{1, \dots, p\}$, N_p^* — множество всех слов в алфавите N_p . Слову $w = s_1 \dots s_\ell$ из N_p^* при заданной системе матриц M однозначно соответствует матрица $M_{s_1} \dots M_{s_\ell}$, являющаяся элементом мультипликативной полугруппы $\langle \mathfrak{M} \rangle$ неотрицательных матриц, порожденной системой $\mathfrak{M}$. Обозначим $M_{s_1} \dots M_{s_\ell} = M(w) = (m_{ij}(w))$.

Экспонентом системы матриц $\mathfrak{M}$ (обозначается $\text{exp } \mathfrak{M}$) называется наименьшая длина ℓ слова $w \in N_p^*$, при котором $M(w) > 0$. Если такого слова не существует, то полагаем $\text{exp } \mathfrak{M} = \infty$.

Субэкспонентом системы матриц $\mathfrak{M}$ (обозначается $\text{sbxp } \mathfrak{M}$) называется наименьшая длина ℓ слова $w = s_1 \dots s_\ell$ из N_p^* , при котором $M_\Sigma(w) > 0$, где

$$M_\Sigma(w) = M_{s_1} + M_{s_1} \cdot M_{s_2} + \dots + M(w).$$

Если такое слово не существует, то полагаем $\text{sbxp } \mathfrak{M} = \infty$.

Утверждение 1. Для любой системы $\mathfrak{M}$ квадратных неотрицательных матриц одинакового размера $\text{sbxp } \mathfrak{M} \leq \text{exp } \mathfrak{M}$.

Заметим, что имеются системы матриц с конечным субэкспонентом и бесконечным экспонентом. Такова, например, любая система подстановочных матриц порядка n , порождающая группу, изоморфную транзитивной группе подстановок степени n . В частности, подстановочная матрица, соответствующая полноцикловой подстановке, имеет конечный субэкспонент и бесконечный экспонент.

На множестве матриц (над полем R) заданного размера имеется частичный порядок: $M \geq M'$ тогда и только тогда, когда $m_{ij} \geq m'_{ij}$ для всех допустимых i, j , где $M' = (m'_{ij})$. Указанный частичный порядок индуцирует квазипорядок на множестве систем матриц (над полем R) заданного размера: $\mathfrak{M} \geq \mathfrak{M}'$ тогда и только тогда, когда для любой матрицы $M' \in \mathfrak{M}'$ имеется матрица $M \in \mathfrak{M}$, такая, что $M \geq M'$. Непосредственно из определений следуют «монотонные» свойства.

Утверждение 2. Если $\mathfrak{M} \geq \mathfrak{M}'$ или $\mathfrak{M} \supseteq \mathfrak{M}'$, где $\mathfrak{M}, \mathfrak{M}'$ — системы квадратных неотрицательных матриц одинакового размера, то $\text{sbxp } \mathfrak{M} \leq \text{sbxp } \mathfrak{M}'$ и $\text{exp } \mathfrak{M} \leq \text{exp } \mathfrak{M}'$.

С точки зрения теории признаков в полугруппах подмножество квадратных положительных матриц размера n можно рассматривать как полугрупповой признак в полугруппе квадратных неотрицательных матриц размера n [1, разд. 9.1], показатель этого признака в системе образующих $\mathfrak{M}$ совпадает с $\text{exp } \mathfrak{M}$.

2. Число путей с заданной меткой в объединении орграфов

В графе Γ с множеством вершин $\{1, \dots, n\}$ обозначим через $d_{i,j}$ длину кратчайшего пути из вершины i в вершину j (расстояние от i до j), тогда диаметр графа Γ есть

$$\text{diam } \Gamma = \max\{d_{i,j} : i, j = 1, \dots, n\}.$$

Пусть Γ_s — граф с множеством вершин $\{1, \dots, n\}$, где все дуги помечены числом s , и $M_s = (m_{ij}(s))$ — матрица смежности вершин графа Γ_s , $s = 1, \dots, p$. Тогда объединение графов $\Gamma^{(p)} = \Gamma_1 \cup \dots \cup \Gamma_p$ в зависимости от объединяемых множеств дуг есть либо граф, либо мультиграф, которому соответствует система матриц смежности $\mathfrak{M} = \{M_1, \dots, M_p\}$. Любой путь длины ℓ в мультиграфе (графе) $\Gamma^{(p)}$ помечен словом из N_p^* длины ℓ . Далее рассмотрим мультиграф $\Gamma^{(p)}$, рассуждения для графа проводятся аналогично.

Для данных мультиграфов верно обобщение следствия 1 теоремы 2 [7, с. 143].

Теорема 1. В мультиграфе $\Gamma^{(p)}$ число путей длины ℓ из вершины i в вершину j с меткой $w = (s_1, \dots, s_\ell)$ равно $m_{ij}(w)$.

Доказательство. Индукция по ℓ .

Для $\ell = 1$ теорема следует из определения матриц M_s , $s = 1, \dots, p$, и определения мультиграфа $\Gamma^{(p)}$.

Пусть теорема доказана для $\ell - 1$, где $\ell > 1$, для любой пары вершин (i, j) мультиграфа $\Gamma^{(p)}$ и для любого слова $u = (s_1, \dots, s_{\ell-1}) \in N_p^*$.

Докажем теорему для ℓ , для любой пары (i, j) вершин мультиграфа $\Gamma^{(p)}$ и для любого слова $w \in N_p^*$.

По определению $M(w) = M(u) \cdot M_{s_\ell}$, отсюда получаем по правилу умножения матриц

$$m_{ij}(w) = \sum_{r=1}^n m_{ir}(u) m_{rj}(s_\ell). \quad (1)$$

По предположению индукции $m_{ir}(u)$ есть число путей длины $\ell - 1$ с меткой u из i в r в мультиграфе $\Gamma^{(p)}$. Тогда $m_{ir}(u) m_{rj}(s_\ell)$ есть число путей длины ℓ с меткой w из i

в j в $\Gamma^{(p)}$, таких, что вершина r предшествует вершине j . Суммируя по r , получаем общее число путей длины ℓ с меткой w из i в j в $\Gamma^{(p)}$. ■

Следствие 1. $\text{diam } \Gamma^{(p)} \leq \text{sbxp } \mathfrak{M}$, в частности, если $\Gamma_1 = \dots = \Gamma_p = \Gamma$, то $\text{diam } \Gamma = \text{sbxp } M$.

Доказательство.

В соответствии с теоремой 1 $M_\Sigma(w) > 0$ тогда и только тогда, когда для любой пары вершин (i, j) в $\Gamma^{(p)}$ имеется путь из i в j , у которого метка совпадает с началом слова w . Значит, если $M_\Sigma(w) > 0$, то $\text{diam } \Gamma^{(p)}$ не превышает длину слова w , так как по определению диаметр мультиграфа есть максимум по всем парам (i, j) длин кратчайших путей из i в j без ограничения на метки. Отсюда $\text{diam } \Gamma^{(p)} \leq \text{sbxp } \mathfrak{M}$.

При условии $\Gamma_1 = \dots = \Gamma_p = \Gamma$ верно и обратное неравенство в силу отсутствия меток в графе Γ , то есть в этом случае $\text{diam } \Gamma^{(p)} = \text{sbxp } \mathfrak{M}$. ■

3. О длинах путей между заданными вершинами

В некоторых приложениях возникает задача определения в графе Γ всех длин путей из вершины i в вершину j . В частности, существует ли натуральное число λ_{ij} , такое, что для любого $\ell \geq \lambda_{ij}$ в графе Γ имеется путь длины ℓ из вершины i в вершину j ?

В графе Γ всякий путь, проходящий через вершину, в которой имеется петля, назовем путем с петлей. Ниже используем следующую лемму.

Лемма 1. Если в графе Γ имеется путь из i в j длины λ с петлей, то для любого $\ell \geq \lambda$ имеется путь из i в j длины ℓ .

Обозначим в графе Γ , где i, j, r — вершины графа:

$d_{i,r,j}$ — длину кратчайшего пути из i в j , проходящего через r , где $d_{i,r,j} = d_{i,j}$ при $r \in \{i, j\}$;

$\text{diam}^r \Gamma = \max\{d_{i,r,j} : i, j = 1, \dots, n\}$ — назовем эту величину r -диаметром графа;

$e(i) = \max\{d_{i,j} : j = 1, \dots, n\}$ — эту величину называют эксцентриситетом вершины i ;

$p(i) = \max\{d_{j,i} : j = 1, \dots, n\}$ — назовем эту величину периферийностью вершины i .

В случае неориентированного графа $e(i) = p(i)$, $i = 1, \dots, n$.

Лемма 2. При $n \geq 2$ в n -вершинном сильносвязном орграфе Γ :

а) если $r \notin \{i, j\}$, то $\text{diam } \Gamma \leq \text{diam}^r \Gamma \leq p(r) + e(r) \leq 2n - 2$;

б) если $r \in \{i, j\}$, то $\text{diam } \Gamma = \text{diam}^r \Gamma \leq n$.

Доказательство. Если $r \notin \{i, j\}$, то по определению

$$\text{diam}^r \Gamma = \max\{d_{i,r} + d_{r,j} : i, j = 1, \dots, n\},$$

где $d_{i,r} \leq p(r) \leq n - 1$, $d_{r,j} \leq e(r) \leq n - 1$. Значит, $\text{diam}^r \Gamma \leq p(r) + e(r) \leq 2n - 2$ при $n \geq 2$.

Если $r \in \{i, j\}$, то $\text{diam}^r \Gamma = \max\{d_{i,j} : i, j = 1, \dots, n\} \leq n$. ■

Замечание 1. Оценка $\text{diam}^r \Gamma \leq 2n - 2$ достижима при любом $n \geq 2$. В частности, она достигается для n -вершинного графа с множеством дуг $\{(i, i + 1), (i + 1, i) : i = 1, \dots, n - 1\}$; в этом случае $\text{diam}^n \Gamma = d_{1,n,1} = 2n - 2$.

Теорема 2. Если n -вершинный граф Γ сильно связан и имеет петлю в вершине r , то для любых $i, j \in \{1, \dots, n\}$ и любого $\ell \geq \text{diam}^r \Gamma$ имеется путь из i в j длины ℓ .

Доказательство. Так как граф Γ сильно связан, то для любых $i, j \in \{1, \dots, n\}$ имеется путь с петлей из i в j , проходящий через r ; длина $d_{i,r,j}$ кратчайшего такого

пути не превышает $\text{diam}^r \Gamma$. Вместе с тем в соответствии с определением величины $\text{diam}^r \Gamma$ в Γ найдется пара вершин (u, v) , такая, что $d_{u,r,v} = \text{diam}^r \Gamma$. Отсюда по лемме 1 получаем требуемое утверждение. ■

Следствие 2. При $n \geq 2$ для матрицы M смежности вершин графа Γ верно: $\exp M \leq \text{diam}^r \Gamma \leq 2n - 2$.

Доказательство. Из теоремы 2 получаем в соответствии со следствием 1 теоремы 2 [7, с. 143], что $M^\ell > 0$ при любом $\ell \geq \text{diam}^r \Gamma$, где по лемме 2 $\text{diam}^r \Gamma \leq 2n - 2$ при $n \geq 2$. ■

Тем самым абсолютная оценка $\exp M \leq n^2 - 2n + 2$ для n -вершинных сильносвязных графов [9] уточнена для графов с петлей.

4. О длине кратчайшего полного пути в сильносвязном орграфе

Следствие 1 позволяет поставить вопрос: существует ли мультиграф $\Gamma^{(p)}$ с конечным диаметром и бесконечным $\text{sbxr } \mathfrak{M}$? Здесь получен отрицательный ответ и выведена верхняя оценка для $\text{sbxr } \mathfrak{M}$.

Заметим, если мультиграф $\Gamma^{(p)}$ не сильносвязный, то $\text{sbxr } \mathfrak{M} = \infty$ в соответствии с теоремой 1 и $\text{diam } \Gamma^{(p)} = \infty$ в соответствии с определением диаметра графа. Следовательно, поставленный вопрос относится исключительно к сильносвязным мультиграфам $\Gamma^{(p)}$.

В любом сильносвязном орграфе (мультиграфе) имеется полный, то есть проходящий через все вершины цикл (путь). Оценим длину кратчайшего из полных циклов (путей).

Теорема 3. В n -вершинном сильносвязном орграфе Γ имеются:

- а) при $n \geq 4$ полный цикл длины не более $\lambda(n) = (n^2 - n)/2$;
- б) при $n \geq 4$ полные пути длины не более $\lambda(n) - 1$ с началом в любой вершине;
- в) при $n \geq 2$ полный путь длины не более $\lambda'(n) = \lambda(n) - n + 2$ с началом в некоторой вершине.

Доказательство. Длину пути z в Γ , равную числу дуг пути, обозначим $\text{len}(z)$. Используя индукцию по k , докажем вспомогательное утверждение: в Γ имеется путь длины не более $\lambda'(k)$, проходящий через k различных вершин, $k = 2, 3, \dots, n$. При $k = n$ вспомогательное утверждение равносильно утверждению «в» теоремы.

По условию орграф Γ сильносвязный, значит, в Γ имеется путь длины 1, проходящий через 2 разные вершины, с началом в любой вершине. Так как $\lambda'(2) = 1$, то утверждение верно при $k = 2$.

Пусть утверждение верно при $k < n$, где $n > 2$, докажем его при $k + 1$. Обозначим через $z(k)$ путь длины не более $\lambda'(k)$, проходящий через k различных вершин. Без ущерба для общности положим, что $z(k)$ есть путь из 1 в k , проходящий через вершины $1, \dots, k$. Так как Γ сильносвязный, то в нем имеется путь z из k в некоторую вершину, отличную от $1, \dots, k$. Длина $\text{len}(z)$ кратчайшего такого пути не превышает k , так как путь z является простым и все его вершины, кроме первой и последней, образуют бесповторную выборку размера не более $k - 1$ из множества $\{1, \dots, k - 1\}$.

Если $\text{len}(z) \leq k - 1$, то искомым путь $z(k + 1)$ определим как соединение путей $z(k)$ и z . Действительно, $z(k + 1)$ есть путь, проходящий через $k + 1$ различных вершин, и его длина $\text{len}(z(k + 1))$ удовлетворяет оценкам

$$\text{len}(z(k + 1)) \leq \lambda'(k) + k - 1 = \lambda'(k + 1).$$

Если $\text{len}(z) = k$, то искомым путем $z(k+1)$ определим как z . Следовательно, при $k \geq 2$ в обоих случаях $\text{len}(z(k+1)) \leq \lambda'(k+1)$. Утверждение «в» доказано.

Без ущерба для общности положим, что построенный полный путь $z(n)$ есть путь из вершины 1 в вершину n . Соединив путь $z(n)$ с кратчайшим путем z' из вершины n в вершину 1 (длина его $\text{len}(z')$ не превышает $n-1$), получим полный цикл в Γ . Если $\text{len}(z') \leq n-2$, то длина полного цикла не превышает $\lambda(n)$. Если $\text{len}(z') = n-1$, то путь z' является полным. Соединив путь z' с кратчайшим путем z'' из вершины 1 в вершину n (длина $\text{len}(z'')$ не превышает $n-1$), получим также полный цикл в Γ длины не больше $2n-2$. Следовательно, при $n \geq 4$ в обоих случаях длина полного цикла не превышает $\lambda(n)$. Утверждение «а» доказано.

Если из построенного полного цикла удалить любую дугу, то получим полный путь (начало можно выбрать произвольно) длины не более $\lambda(n)-1$, где $n \geq 4$. Утверждение «б» также доказано. ■

Замечание 2. Оценки теоремы 2 совпадают по порядку с точными оценками, что подтверждается примером $2n$ -вершинного орграфа Γ с множеством дуг E :

$$E = \{(2n, i), (i, n+1) : i = 1, \dots, n\} \cup \{(j, j+1) : j = n+1, n+2, \dots, 2n-1\}.$$

В графе Γ длина полного цикла равна $n(n+1)$, длина полного пути из 1 в n равна n^2-1 .

Замечание 3. Теорема 3 верна и для любого n -вершинного сильносвязного мультиграфа.

Теорема 4. Если n -вершинный мультиграф $\Gamma^{(p)}$ сильносвязный, то при $n \geq 4$

$$\text{sbxp } \mathfrak{M} \leq \frac{(n^2-2)(n-1)}{2}.$$

Доказательство. В соответствии с определением $\text{sbxp } \mathfrak{M}$ достаточно построить слово $w = s_1 \dots s_\ell \in N_p^*$, $\ell \leq \frac{(n^2-2)(n-1)}{2}$, при котором $M_\Sigma(w) > 0$. Опишем n шагов построения, где на i -м шаге строится начальный отрезок слова w , при котором положительны все элементы первых i строк матрицы $M_\Sigma(w)$, $i = 1, \dots, n$.

Для $w = s_1 \dots s_\ell$ положим: $w(\tau) = s_1 \dots s_\tau$, где $\tau = 1, \dots, \ell$.

1-й шаг. В сильносвязном мультиграфе $\Gamma^{(p)}$ имеется полный цикл C_1 длины $\ell(1)$, где $\ell(1) \leq \lambda(n)$ по утверждению «а» теоремы 3. Пусть 1 — начальная вершина цикла C_1 и $w(\ell(1))$ — метка цикла C_1 (слово длины $\ell(1)$ в алфавите N_p^*). Тогда в $\Gamma^{(p)}$ имеется путь из 1 в j длины $\tau(j)$, где $1 \leq \tau(j) \leq \ell(1)$, отсюда по теореме 1 имеем $m_{1j}(w(\tau(j))) > 0$, $j = 1, \dots, n$. Следовательно, все элементы первой строки матрицы $\sum_{j=1}^n M(w(\tau(j)))$ положительны. Отсюда положительны все элементы первой строки матрицы $M_\Sigma(w(\ell(1)))$, так как

$$M_\Sigma(w(\ell(1))) = \sum_{i=1}^{\ell(1)} M(w(i)) \geq \sum_{j=1}^n M(w(\tau(j))).$$

Пусть выполнены $i-1$ шагов построения, то есть построено слово $w(\ell(i-1))$, такое, что положительны все элементы первых $i-1$ строк матрицы $M_\Sigma(w(\ell(i-1)))$, $1 < i \leq n$.

i -й шаг. Обозначим через C'_{i-1} путь длины $\ell(i-1)$ с меткой $w(\ell(i-1))$, начинающийся в i . Пусть конечная вершина пути C'_{i-1} есть $\mu \in \{1, \dots, n\}$. Продолжим слово $w(\ell(i-1))$ до слова $w(\ell(i))$. В $\Gamma^{(p)}$ имеется полный путь C_i длины ℓ_i с началом в μ , где

$\ell_i \leq \lambda(n) - 1$ по утверждению «б» теоремы 3; метку пути C_i обозначим w_i . Построим начинающийся в i путь C'_i длины $\ell(i)$ с помощью последовательного соединения путей C'_{i-1} и C_i , где $\ell(i) = \ell(i-1) + \ell_i$ и метка $w(\ell(i))$ пути C'_i получена соединением меток путей C'_{i-1} и C_i : $w(\ell(i)) = w(\ell(i-1))w_i$. Тогда по построению в $\Gamma^{(p)}$ имеется путь из i в j длины $\theta(j)$, где $\ell(i-1) \leq \theta(j) \leq \ell(i)$, отсюда по теореме 1 имеем $m_{ij}(w(\theta(j))) > 0$, $j = 1, \dots, n$. Значит, все элементы i -й строки матрицы $\sum_{j=1}^n M(w(\theta(j)))$ положительны. Отсюда положительны все элементы i -й строки матрицы $M_\Sigma(w(\ell(i)))$, так как

$$M_\Sigma(w(\ell(i))) = \sum_{s=1}^{\ell(i)} M(w(s)) \geq \sum_{j=1}^n M(w(\theta(j))).$$

С учетом предположения индукции все элементы первых $i-1$ строк матрицы $M_\Sigma(w(\ell(i)))$ также положительны, так как $M_\Sigma(w(\ell(i))) \geq M_\Sigma(w(\ell(i-1)))$. Следовательно, положительны все элементы первых i строк матрицы $M_\Sigma(w(\ell(i)))$, $i = 1, \dots, n$. Значит, искомое слово w совпадает с $w(\ell(n))$.

Так как $\ell(i) = \ell(i-1) + \ell_i$, где $\ell(i) \leq \lambda(n)$ и $\ell_i \leq \lambda(n) - 1$, $i \geq 1$, то верна оценка

$$\ell(n) = \ell(1) + \ell_2 + \dots + \ell_n \leq n\lambda(n) - n + 1 = \frac{(n^2 - n)(n - 1)}{2}.$$

■

Выводы

Для n -вершинного сильносвязного орграфа (мультиграфа) Γ получены оценки:

- 1) при $n \geq 4$ длина кратчайшего полного пути в Γ не превышает $n(n-1)/2$, эта оценка является точной по порядку;
- 2) при наличии петли в Γ экспонент матрицы смежности вершин не превышает $2n-2$, $n \geq 2$.

При $n \geq 4$ субэкспонент системы матриц смежности вершин n -вершинных графов $\Gamma_1, \dots, \Gamma_p$, объединение которых сильно связно, не превышает $(n^2 - 2)(n - 1)/2$.

ЛИТЕРАТУРА

1. Фомичёв В. М. Методы дискретной математики в криптологии. М.: ДИАЛОГ-МИФИ, 2010. 424 с.
2. Шнайер Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. М.: ТРИУМФ, 2002. 816 с.
3. Шеннон К. Работы по теории информации и кибернетике. М.: ИЛ, 1963.
4. Харари Ф., Палмер Э. Перечисление графов. М.: Мир, 1977.
5. Кофман А. Введение в прикладную комбинаторику. М.: Наука, 1975. 480 с.
6. <http://dic.academic.ru> — Словарь терминов теории графов.
7. Берж К. Теория графов и её применение. М.: ИЛ, 1962. 320 с.
8. Сачков В. Н., Ошкин И. Б. Экспоненты классов неотрицательных матриц // Дискретная математика. 1993. Т. 5. Вып. 2. С. 150–159.
9. Wielandt H. Unzerlegbare nicht negative Matrizen // Math. Zeitschr. 1950. V. 52 P. 642–648.