— в функциональном графе $G_{f,2}$ при $n = 3 \cdot 2^k(2m+1)$ множество вершин, принадлежащих деревьям, разбивается на 2^k уровней, причём каждая вершина дерева имеет ровно четырёх предков;
— при чётном n функциональный граф $G_{f,2}$ содержит четыре неподвижные точки, при нечётном n — две неподвижные точки;
— если $n = 2^k(2m+1)$, то все длины циклов функционального графа $G_{f,2}$ являются делителями $2^k(2^s-1)$, где $s = \min\{j : j > 0,\ 2^j \equiv \pm 1 \pmod{2m+1}\}$.

ЛИТЕРАТУРА

1. *Харари Ф.* Теория графов. М.: УРСС, 2003.
2. *Евдокимов А. А., Пережогин А. Л.* Дискретные динамические системы циркулянтного типа с линейными функциями в вершинах сети // Дискретный анализ и исследование операций. 2011. Т. 3. № 3. С. 39–48.

УДК 519.6

О ЛОКАЛЬНОЙ ПРИМИТИВНОСТИ ГРАФОВ И НЕОТРИЦАТЕЛЬНЫХ МАТРИЦ

С. Н. Кяжин

Положительным криптографическим свойством генератора гаммы, построенного на основе управляющего и генерирующего блоков, является существенная зависимость элементов состояний генерирующего блока от всех знаков начального состояния генератора. Для изучения такого рода зависимостей в рамках матрично-графового подхода введено понятие локальной примитивности неотрицательных матриц и графов. Получены условия локальной примитивности матриц. Установлена связь характеристик локальной примитивности частного класса матриц (графов) с конструктивными параметрами генераторов гаммы.

Ключевые слова: *экспонент, локальный экспонент, примитивная матрица, примитивный граф, локальная примитивность.*

Пусть $M_0(n)$ — множество всех квадратных неотрицательных матриц порядка n, $A \in M_0(n)$, $J = \{j_1, \ldots, j_r\}$, $\varnothing \neq J \subseteq \{1, \ldots, n\}$; $A(J^2)$ — подматрица порядка r, полученная из A вычёркиванием строк и столбцов с номерами $j \neq j_1, \ldots, j_r$. Множество матриц, для которых подматрица $A(J^2)$ неотрицательна, обозначим $M_0(J^2)$.

Матрицу A назовем J^2-положительной, если положительна подматрица $A(J^2)$. Обозначим $M_+(J^2)$ полугруппу по умножению J^2-положительных матриц.

Матрица A называется квазиположительной, если все её строки и столбцы отличны от нулевых. Матрица A называется J^2-квазиположительной, если квазиположительной является подматрица $A(J^2)$. Обозначим $Q(J^2)$ множество J^2-квазиположительных матриц.

Квазиположительную матрицу A назовём J^2-примитивной, если положительна подматрица $A^t(J^2)$ матрицы A^t при любом натуральном $t \geqslant \gamma$; наименьшее такое число γ назовём J^2-экспонентом матрицы A и обозначим J^2-exp$A$. Множество J^2-примитивных матриц обозначим $P(J^2)$.

Подматрицу размера $n \times r$, полученную из A вычёркиванием столбцов с номерами $j \neq j_1, \ldots, j_r$, обозначим $A(J)$ и назовём её в соответствующих условиях J-положительной (J-квазиположительной, J-примитивной). Множества таких матриц обозначим соответственно $M_+(J)$, $Q(J)$ и $P(J)$. Наименьшее натуральное число γ, при кото-

ром подматрицы $A^t(J)$ строго положительны при любом $t \geqslant \gamma$, назовём J-экспонентом матрицы A и обозначим J-exp$A$.

Обозначим $S(J^2)$ группу подстановочных матриц порядка n, для которых любой элемент $i \notin J$ неподвижный.

Утверждение 1. При любом непустом подмножестве $J \subseteq \{1, \ldots, n\}$, $n > 1$, имеет место:

1) $M_+(J^2) \subset P(J^2) \subset Q(J^2)$;
2) $S(J^2) \subset Q(J^2)$, при этом $S(J^2) \cup P(J^2) = \varnothing$;
3) множество $Q(J^2)$ образует моноид относительно умножения, $M_+(J^2)$ — идеал моноида $Q(J^2)$.

Пусть $A, B \in M_0(n)$, $A = (a_{ij})$, $B = (b_{ij})$, определим отношение

$$A \leqslant B \Leftrightarrow a_{ij} \leqslant b_{ij}, \quad i, j = 1, \ldots, n.$$

Утверждение 2.

1) Пусть $J \leqslant I$, тогда если матрица A не J^2-примитивная, то она не I^2-примитивная; если матрица A является I^2-примитивной, то она J^2-примитивная и J^2-exp$A \leqslant I^2$-exp$A$; аналогичные соотношения верны для J-примитивности и I-примитивности.
2) Если матрица A не J^2-примитивная, то и матрица $A(J^2)$ не примитивная; если матрица $A(J^2)$ примитивная, то матрица A является J^2-примитивной и J^2-exp$A \leqslant$ exp$A(J^2)$.
3) Если $A \leqslant B$ и A является J^2-примитивной, то и B является J^2-примитивной и J^2-exp$A \leqslant J^2$-exp$B$.

Утверждение 3. Если матрицы $A, B \in M_0(J^2)$ сопряжены в группе $S(J^2)$, то A и B одновременно или J^2-примитивны, или не J^2-примитивны.

Обозначим через $\Gamma(A)$ орграф, матрицей смежности вершин которого является носитель матрицы A. Известно, что матрица A и граф $\Gamma(A)$ одновременно примитивны или не примитивны.

Теорема 1. Граф $\Gamma(A)$ является J^2-примитивным тогда и только тогда, когда $\Gamma(A)$ имеет сильносвязный примитивный подграф с множеством вершин, содержащим J.

Теорема 2. Связный граф $\Gamma(A)$ является J-примитивным тогда и только тогда, когда $\Gamma(A)$ имеет сильносвязный примитивный подграф U с множеством вершин, содержащим J, и из каждой вершины $i \notin U$ достижимо множество вершин U.

Следствие 1. Пусть J^2-exp$A = \gamma$, J-exp$A = \delta$. Если граф $\Gamma(A)$ является J-примитивным, то $\gamma \leqslant \delta \leqslant \gamma + \max\limits_i \rho(i, U)$, где $\rho(i, U)$ — длина кратчайшего пути из вершины $i \notin U$ в ближайшую вершину $j \in U$.

Ряд генераторов гаммы построен на основе последовательного соединения управляющего и генерирующего автоматов [1, гл. 18], при этом выходная гамма образуется с помощью функции от некоторого подмножества J знаков состояний генерирующего автомата. Положительным криптографическим свойством такого генератора является

существенная зависимость всех знаков множества J от всех знаков начального состояния генератора. В связи с этим рассмотрим автономный автомат без выхода A, построенный как последовательное соединение двух регистров правого сдвига длины n и m соответственно с функциями обратной связи $f(x)$ и $g(x)$.

Пусть V_r — множество двоичных r-мерных векторов, $r = 1, 2, \ldots$; A — автомат с множеством состояний V_{n+m}, выходным алфавитом управляющего регистра V_1 и функцией переходов h:

$$h(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m}) =$$
$$= (f(x_1, \ldots, x_n), x_1, \ldots, x_{n-1}, x_n \oplus g(x_{n+1}, \ldots, x_{n+m}), x_{n+1}, \ldots, x_{n+m-1}).$$

Перемешивающая матрица M (порядка $m+n$) преобразования h генератора имеет вид

$$M = \begin{pmatrix} A & B \\ 0 & C \end{pmatrix},$$

где A — перемешивающая матрица порядка n преобразования управляющего регистра; C — матрица порядка m, совпадающая при фиксированном x_n с перемешивающей матрицей преобразования генерирующего регистра; в матрице $B = (b_{ij})$ порядка $n \times m$ элемент $b_{n,n+1} = 1$, а остальные элементы равны 0.

Теорема 3. Пусть $J = \{n+1, \ldots, n+m\}$, функция $g(x)$ существенно зависит от переменных с номерами $j_1, \ldots, j_r, m$, где $1 \leqslant j_1 < \ldots < j_r < m$, $1 \leqslant r < m$, НОД$(j_1, \ldots, j_r, m) = d \geqslant 1$. Тогда матрица M преобразования генератора J-примитивна, если и только если $d = 1$; в случае J-примитивности верны следующие оценки:

1) $J\text{-exp}\, M \leqslant \max\{n + j_1(m-1), \exp C\}$;
2) $J\text{-exp}\, M \leqslant n + \exp C$.

Величины $\exp C$ и $J\text{-exp}\, M$ можно оценить через характеристики генератора.

1) Из [2, с. 227] следует, что $\exp C \leqslant m + j_1(m-2)$, тогда в соответствии с теоремой 3, п. 1
$$J\text{-exp}\, M \leqslant \max\{m, n + j_1\} + j_1(m-2).$$
2) Пусть среди чисел $j_1, \ldots, j_r, m$ имеется пара взаимно простых чисел, например $(j_1, j_2) = 1$, тогда из [3, теорема 1,*б*] следует, что $\exp C \leqslant 2m + j_2 j_1 - j_2 - 2j_1$. В этом случае в соответствии с теоремой 3, п. 1
$$J\text{-exp}\, M \leqslant \max\{n + j_1(m-1), 2m + j_2 j_1 - j_2 - 2j_1\}.$$

Если, в частности, $j_1 > 2$ и $j_2 \leqslant \dfrac{m(j_1-2)+j_1}{j_1-1}$, то $\exp C \leqslant j_1(m-1)$, то есть оценка теоремы 3, п. 2 точнее. Тогда в соответствии с теоремой 3, п. 2

$$J\text{-exp}\, M \leqslant n + 2m + j_2 j_1 - j_2 - 2j_1.$$

ЛИТЕРАТУРА

1. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
2. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.