УДК 519.1 DOI 10.17223/2226308X/9/24

ПЕРЕМЕШИВАЮЩИЕ СВОЙСТВА ДВУХКАСКАДНЫХ ГЕНЕРАТОРОВ

С. Н. Кяжин, В. М. Фомичев

С помощью матрично-графового подхода оценены перемешивающие свойства двухкаскадных генераторов: на основе последовательного соединения регистров сдвига; генераторов 1-2 шага; с перемежающимся шагом. Получены условия локальной примитивности (квазипримитивности) перемешивающих графов генераторов и верхние оценки соответствующих локальных экспонентов (квазиэкспонентов), которые при многих значениях параметров близки по порядку к сумме длин регистров генератора.

Ключевые слова: *регистр сдвига, генератор 1-2 шага, генератор с перемежающимся шагом, локальная примитивность, локальный экспонент.*

Введение

Важным свойством генератора гаммы является зависимость знаков гаммы γ_i от всех знаков начального состояния при $i > i_0$, где i_0 определяет длину холостого хода генератора. Для этого свойства необходима примитивность (локальная примитивность) перемешивающего графа преобразования множества состояний генератора.

Пусть $N_n = \{1, \ldots, n\}$; $I, J \subseteq N_n$, $I \neq \varnothing$, $J \neq \varnothing$; M — 0,1-матрица порядка $n{>}1$; $M(I \times J)$ — её подматрица размера $|I| \times |J|$, полученная из M удалением строк с номерами $i \notin I$ и столбцов с номерами $j \notin J$. Матрица M называется примитивной ($I \times J$-примитивной), если существует такое натуральное число γ, что $M^t > 0$ ($M^t(I \times J) > 0$) при любом $t \geqslant \gamma$. Наименьшее такое γ называется экспонентом ($I \times J$-экспонентом) матрицы M, обозначается $\exp M$ ($I \times J$-$\exp M$).

Матрица M называется $I \times J$-квазипримитивной, если при некотором натуральном δ подматрица $M^t(I \times J)$ не имеет нулевых строк для любого $t \geqslant \delta$. Наименьшее такое δ называется $I \times J$-квазиэкспонентом матрицы M, обозначается $I \times J$-$\mathrm{qexp}\, M$.

Под примитивностью ($I \times J$-примитивностью, $I \times J$-квазипримитивностью) орграфа Γ понимается соответствующее свойство его матрицы смежности M, при этом соответствующие экспоненты и локальные экспоненты орграфа Γ и матрицы M равны.

Цель работы — применить ранее полученные условия примитивности [1, с. 226] и локальной примитивности [2] орграфов для оценки перемешивающих свойств некоторых двухкаскадных генераторов.

Обозначим: V_r — множество двоичных r-мерных векторов; $S(f)$ — множество номеров существенных переменных функции f; s — сумма длин регистров генератора, $(x_1, \ldots, x_s)$ — начальное состояние регистров, m, n, r — длины регистров (m — управляющего, n, r — генерирующих), $m, n, r > 1$; h — преобразование множества V_s состояний генератора; h_i^t — i-я координатная функция преобразования h^t, $i = 1, \ldots, s$; $\Gamma(h)$ — перемешивающий s-вершинный орграф преобразования h; γ_t — t-й знак гаммы, $t = 1, 2, \ldots$

1. Последовательное соединение регистров сдвига

Пусть генератор построен на основе последовательного соединения двоичных регистров правого сдвига длины m и n с булевыми функциями обратной связи $f_1(x_1, \ldots, x_m)$ и $f_2(x_{m+1}, \ldots, x_{m+n})$ соответственно. Положим $S(f_1) = \{b_1, \ldots, b_\nu\}$,

$S(f_2) = \{c_1, \ldots, c_\mu\}$, где $1 \leqslant b_1 < \ldots < b_\nu = m$, $m+1 \leqslant c_1 < \ldots < c_\mu = m+n$, НОД$(b_1, \ldots, b_\nu) = d_1$, НОД$(c_1 - m, \ldots, c_\mu - m) = d_2$.

Уравнения гаммообразования: $\gamma_t = h^t_{m+n}(x_1, \ldots, x_{m+n})$. Таким образом, для анализа свойств гаммы генератора представляет интерес величина $N_{m+n} \times \{m+n\}$-exp $\Gamma(h)$.

Утверждение 1. Орграф $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным, если и только если $d_2 = 1$, в этом случае

$$N_{m+n} \times \{m+n\}\text{-exp}\,\Gamma(h) \leqslant n + \max\{m, \rho_2\} + g(c_1 - m, \ldots, c_\mu - m),$$

где $\rho_2 = \max\limits_{l=1,\ldots,\mu} \{c_l - c_{l-1}\}$; $c_0 = m$.

Следствие 1. Если $c_1 = m+1$, то $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным и $N_{m+n} \times \{m+n\}$-exp $\Gamma(h) = n - 1 + \max\{m, \rho_2\}$.

Утверждение 2. Орграф $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным, если и только если $(d_1, d_2) = 1$, в этом случае

$$N_m \times \{m+n\}\text{-exp}\,\Gamma(h) \leqslant \rho_1 + m + n + g(b_1, \ldots, b_\nu, c_1 - m, \ldots, c_\mu - m),$$

где $\rho_1 = \max\limits_{l=1,\ldots,\nu} \{b_l - b_{l-1}\}$; $b_0 = 1$.

Следствие 2. Если $c_1 = m+1$, то $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным и $N_m \times \{m+n\}$-exp $\Gamma(h) = m + n - 1$.

2. Генератор 1-2 шага

Генератор 1-2 шага построен на основе управляющего и генерирующего линейных регистров сдвига (ЛРС) длины m и n. Преобразование h нелинейное в силу неравномерности движения генерирующего регистра, определяемого управляющей функцией $u(x_1, \ldots, x_m)$.

Пусть управляющий и генерирующий регистры правого сдвига имеют соответственно длины $m > 2$ и $n > 2$ и функции обратной связи $f_{\text{у}}(x_1, \ldots, x_m)$ и $f_{\text{г}}(x_{m+1}, \ldots, x_{m+n})$. Положим $S(f_{\text{у}}) = \{b_1, \ldots, b_\nu\}$, $S(f_{\text{г}}) = \{c_1, \ldots, c_\mu\}$, где $1 \leqslant b_1 < \ldots < b_\nu = m$, $m+1 \leqslant c_1 < \ldots < c_\mu = m+n$.

Уравнения гаммообразования имеют вид $\gamma_t = h^t_{m+n}(x_1, \ldots, x_{m+n})$. Оценим величину $N_{m+n} \times \{m+n\}$-exp $\Gamma(h)$, важную для анализа гаммы генератора.

Утверждение 3. Граф $\Gamma(h)$ является $N_{m+n} \times \{m+n\}$-примитивным и

$$N_{m+n} \times \{m+n\}\text{-exp}\,\Gamma(h) = \max\{m, \rho\} + \lambda(\lambda - 1) + \lceil n/2 \rceil, \tag{1}$$

где $\lambda = \lceil (c_1 - m)/2 \rceil$; $\rho = \max\{\lceil (c_2 - c_1)/2 \rceil, \ldots, \lceil (c_\mu - c_{\mu-1})/2 \rceil\}$.

Следствие 3. Граф $\Gamma(h)$ является $N_m \times \{m+n\}$-примитивным и

$$N_m \times \{m+n\}\text{-exp}\,\Gamma(h) = m + \lambda(\lambda - 1) + \lceil n/2 \rceil. \tag{2}$$

Приведём числовые примеры. Пусть $m = 7$, $n = 20$, $S(u) = \{m\}$.

При $S(f_{\text{г}}) = \{m+n-1, m+n\}$ выполнено $\lambda = \lceil (n-1)/2 \rceil = 10$, $\rho = 1$. Тогда из (1) и (2) следует: $N_7 \times \{27\}$-exp $\Gamma(h) = N_{27} \times \{27\}$-exp $\Gamma(h) = 107$.

При $S(f_{\text{г}}) = \{m+2, m+n\}$ выполнено $\lambda = 1$, $\rho = \lceil (n-2)/2 \rceil = 9$. Тогда из (1) и (2) следует: $N_7 \times \{27\}$-exp $\Gamma(h) = 17$, $N_{27} \times \{27\}$-exp $\Gamma(h) = 19$.

3. Генератор с перемежающимся шагом

Генератор с перемежающимся шагом построен на базе двоичных ЛРС: управляющего ЛРС длины m и двух генерирующих ЛРС длины n и r с функциями обратной связи $f_{\text{у}}(x_1,\dots,x_m)$, $f_1(x_{m+1},\dots,x_{m+n})$ и $f_2(x_{m+n+1},\dots,x_{m+n+r})$ соответственно. В зависимости от знака управления сдвигается информация либо в первом, либо во втором генерирующем ЛРС, в силу чего преобразование h генератора нелинейное.

Пусть $J_1=\{m+1,\dots,m+n\}$, $J_2=\{m+n+1,\dots,m+n+r\}$, $S(f_{\text{у}})=\{b_1,\dots,b_\nu\}$, $S(f_1)=\{c_1,\dots,c_\mu\}$, $S(f_2)=\{d_1,\dots,d_\sigma\}$, где $1\leqslant b_1<\ldots<b_\nu=m$, $m+1\leqslant c_1<\ldots<c_\mu=m+n$ и $m+n+1\leqslant d_1<\ldots<d_\sigma=m+n+r$.

Уравнения гаммообразования имеют вид:

$$\gamma_t=h^t_{m+n}(x1,\dots,xm+n)\oplus h^t_{m+n+r}(x_1,\dots,x_m,x_{m+n+1},\dots,x_{m+n+r}).$$

Таким образом, для анализа свойств гаммы генератора представляют интерес величины $N_{m+n+r}\times\{m+n,m+n+r\}$-$\exp\Gamma(h)$ и $N_{m+n+r}\times\{m+n,m+n+r\}$-$\operatorname{qexp}\Gamma(h)$.

Утверждение 4. Граф $\Gamma(h)$ является:

а) $N_m\times\{m+n,m+n+r\}$-, $(N_m\cup J_1)\times\{m+n\}$- и $(N_m\cup J_2)\times\{m+n+r\}$-примитивным, при этом

$$\begin{gathered}N_m\times\{m+n,m+n+r\}\text{-}\exp\Gamma(h)=m+\max\{n,r\}-1,\\ N_m\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=m+\min\{n,r\}-1,\\ \delta_1=(N_m\cup J_1)\times\{m+n\}\text{-}\exp\Gamma(h)=m+n-1,\\ \delta_2=(N_m\cup J_2)\times\{m+n+r\}\text{-}\exp\Gamma(h)=m+r-1;\end{gathered}$$

б) не $N_{m+n+r}\times\{m+n,m+n+r\}$-примитивным, но $N_{m+n+r}\times\{m+n,m+n+r\}$-квазипримитивным, и

$$N_{m+n+r}\times\{m+n,m+n+r\}\text{-}\operatorname{qexp}\Gamma(h)=\max\{\min\{\delta_1,\delta_2\},n-1,r-1\}.$$

ЛИТЕРАТУРА

1. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.

УДК 512.64, 519.21, 519.72 DOI 10.17223/2226308X/9/25

АНАЛОГИ ТЕОРЕМЫ ШЕННОНА ДЛЯ ЭНДОМОРФНЫХ НЕМИНИМАЛЬНЫХ ШИФРОВ

Н. В. Медведева, С. С. Титов

Рассматриваются некоторые аналоги теоремы Шеннона для эндоморфных совершенных по Шеннону (абсолютно стойких к атаке по шифртексту) шифров. Построены примеры минимальных по включению совершенных и транзитивных шифров.

Ключевые слова: *совершенные шифры, эндоморфные шифры, неминимальные шифры.*

В основе изучения совершенных шифров лежит математическая модель шифра. Впервые вероятностная модель шифра рассмотрена в фундаментальной работе