Пример. Для перемешивающего орграфа $\Gamma(\varphi^g)$ регистра сдвига с одной обратной связью при $n = 8$, $r = 32$, $D = D_2 = \{0, 3, 4, 6, 7\}$ из формулы (5) следует оценка $\exp\Gamma(\varphi^g) \leqslant 11$ (здесь $\rho(D) = 3$).

а) Оценим $\exp\Gamma(\varphi^{g,\mu})$ перемешивающего орграфа $\Gamma(\varphi^{g,\mu})$ регистра с двумя обратными связями при тех же значениях n, r, D. Пусть $m = 3$. Тогда при любом Δ из (6) следует оценка $\exp\Gamma(\varphi^{g,\mu}) \leqslant 7$. Минимум оценки (6) достигается при $\rho(\Delta) = 1$: $\exp\Gamma(\varphi^{g,\mu}) \leqslant 5$.

б) Оценим $\exp\Gamma(\varphi^{g,\mu})$ при тех же значениях n, r, m и при $D_1 = \{0, 6, 7\}$, $\Delta = \{3, 4\}$. В этом случае $\rho(D_1) = 6$, $\rho(\Delta) = 7$ (т. е. $\rho(\Delta) \geqslant \rho(D_1) + 1$) и $\varepsilon = \varepsilon' = 7$. Из (6) следует оценка $\exp\Gamma(\varphi^{g,\mu}) \leqslant 13$, а из (5) — оценка $\exp\Gamma(\varphi^g) \leqslant 11$.

Выводы

Проведено сравнение верхних оценок экспонентов перемешивающих орграфов $\Gamma(\varphi^g)$ и $\Gamma(\varphi^{g,\mu})$ преобразований регистров сдвига φ^g и $\varphi^{g,\mu}$ с одной и двумя обратными связями, построенных на основе МАГ. Получены условия, при которых оценка $\exp\Gamma(\varphi^{g,\mu})$ ниже оценки $\exp\Gamma(\varphi^g)$. Добавление второй обратной связи улучшает перемешивающие свойства регистра $\varphi^{g,\mu}$. При одинаковых множествах точек съёма D у регистров φ^g и $\varphi^{g,\mu}$ перемешивающие свойства лучше у регистра с двумя обратными связями. Экспоненты перемешивающих орграфов $\Gamma(\varphi^{g,\mu})$ близки к наименьшим значениям при $m = \lceil n/2 \rceil - 1$, $\{m, n-1\} \in D \cap \Delta$. Если величина $\min\{\rho(D), \rho(\Delta)\}$ близка к 1, то оценка $\exp\Gamma(\varphi^{g,\mu})$ улучшается до 50 %.

ЛИТЕРАТУРА

1. *Дорохова* (*Коренева*) *А. М.* Оценки экспонентов перемешивающих графов некоторых модификаций аддитивных генераторов // Прикладная дискретная математика. Приложение. 2014. № 7. С. 60–64.
2. *Коренева А. М., Фомичёв В. М.* О существенных переменных функции переходов модифицированного аддитивного генератора // Прикладная дискретная математика. Приложение. 2016. № 9. С. 51–54.
3. *Коренева А. М., Фомичёв В. М.* Перемешивающие свойства модифицированных аддитивных генераторов // Дискретный анализ и исследование операций. 2017. № 2. С. 47–67.
4. *Коренева А. М.* О примитивности перемешивающих орграфов биективных регистров сдвига с двумя обратными связями // Прикладная дискретная математика. 2017 (в печати).

УДК 519.17 DOI 10.17223/2226308X/10/35

СТРОЕНИЕ ЛОКАЛЬНО ПРИМИТИВНЫХ ОРГРАФОВ

С. Н. Кяжин

Исследованы свойства строения $i \times j$-примитивного орграфа, используемые при расчёте $i \times j$-экспонента орграфа. Показано, что $i \times j$-примитивный орграф есть или компонента сильной связности (ксс), или множество ксс, соединённых определённым образом простыми путями, все вершины которых, за исключением, быть может, начальной и конечной, являются ациклическими. Множество ксс разбивается на $k + 1$ ярусов в соответствии с удалённостью от вершины i. Описано строение перемешивающего графа преобразования множества состояний генератора последовательностей с перемежающимся шагом, построенного на основе регистров сдвига длин m, n, r. Показано, что $i \times (m+n)$- и $i \times (m+n+r)$-примитивный перемешивающий граф преобразования множества V_{m+n+r} состояний генератора

состоит из трёх ксс. В обоих случаях ($i\times(m+n)$- и $i\times(m+n+r)$-примитивность) множество ксс разбивается на 2 яруса.

Ключевые слова: *локально примитивный орграф, компонента сильной связности, перемешивающий граф, генератор с перемежающимся шагом.*

Орграф Γ называется $i\times j$-примитивным (локально примитивным), если существует такое натуральное γ, что в Γ имеются пути из i в j длины t при любом $t\geqslant\gamma$, наименьшее такое γ называется $i\times j$-экспонентом (локальным экспонентом) орграфа Γ. Отсюда $i\times j$-примитивность орграфа Γ полностью определяется свойствами непустого множества путей из i в j.

В [1] показано, что оценка локального экспонента сильно зависит от строения локально примитивного орграфа. С целью оптимизации существующих [1] и получения новых оценок локального экспонента для различных классов орграфов целесообразно описать строение локального примитивного орграфа в общем виде.

Обозначим $\Gamma(i,j)$ компоненту сильной связности орграфа Γ, содержащую множество всех путей из i в j. Для вершин i,j орграфа Γ ксс U орграфа Γ называется i,j-связывающей (кратко i,j-ксс), если в $\Gamma(i,j)$ есть путь, проходящий через некоторую вершину ксс U.

Утверждение 1 [2]. Если орграф Γ является $i\times j$-примитивным, то Γ содержит i,j-ксс.

При описании $i\times j$-примитивного орграфа различаются 2 случая.

С л у ч а й 1: вершины i,j принадлежат общей ксс (в частности, $i=j$).

Утверждение 2 [1]. Если вершины i,j принадлежат ксс U, то орграф Γ является $i\times j$-примитивным тогда и только тогда, когда ксс U примитивная.

С л у ч а й 2: вершина i недостижима из вершины j. Без ущерба для общности положим, что обе вершины i,j не принадлежат i,j-ксс.

Простой путь $(i,i_1,\ldots,i_l,j)$ в орграфе Γ назовём ациклическим, если вершины $i_1,\ldots,i_l$ ациклические.

В общем случае $\Gamma(i,j)$ состоит из всех i,j-ксс и ациклических простых путей, соединяющих i,j-ксс и вершины i,j. Разобьём множество вершин на $k+1$ блоков (ярусов), $k<n$. К 0-му ярусу относится вершина i, к k-му ярусу — вершина j. К 1-му ярусу отнесём все i,j-ксс, достижимые из вершины i с помощью ациклического простого пути. Вершина 0-го яруса i соединяется с вершиной j с помощью простых ациклических путей, если таковые есть в Γ. Каждая i,j-ксс U 1-го яруса имеет множество предшественников $P(U)$, содержащее вершину i.

Пусть описаны 1-й, ..., $(t-1)$-й ярусы и множества предшественников для каждой i,j-ксс этих ярусов, $t<k$. К t-му ярусу отнесём все i,j-ксс, не входящие в 1-й, ..., $(t-1)$-й ярусы и достижимые из i,j-ксс $(t-1)$-го яруса с помощью ациклического простого пути. Множество предшественников $P(U)$ для i,j-ксс U t-го яруса состоит из всех вершин, из которых достижима U. Ксс U t-го яруса соединена с вершиной j и с вершинами i,j-ксс 1-го, ..., t-го ярусов, не входящих в $P(U)$, с помощью простых ациклических путей, если таковые есть в Γ. Построение завершено после описания 1-го, ..., $(k-1)$-го ярусов и множеств предшественников для каждой i,j-ксс этих ярусов.

Пример. На рис. 1 изображён граф $\Gamma(1,14)$, содержащий четыре $1,14$-ксс U_1, U_2, U_3, U_4 с множествами вершин $\{2,3\}$, $\{4,5,6\}$, $\{8,9\}$, $\{12,13\}$ соответственно.

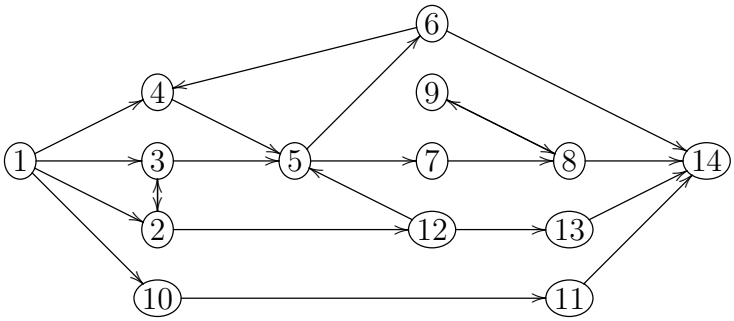

Рис. 1. Орграф $\Gamma(1, 14)$

К 0-му ярусу относится вершина 1, к 1-му — ксс U_1 и U_2, ко 2-му — ксс U_3 и U_4, к 3-му — вершина 14. Множества предшественников: $P(U_1) = \{1\}$, $P(U_2) = \{1, 2, 3, 12, 13\}$, $P(U_3) = P(U_2) \cup \{4, 5, 6, 7\}$, $P(U_4) = \{1, 2, 3\}$.

С помощью этой модели опишем перемешивающий орграф генератора с перемежающимся шагом [3, гл. 18], построенный на базе двоичных регистров правого сдвига: управляющего длины m и двух генерирующих длин n и r, $m, n, r > 1$. В зависимости от управляющего знака сдвигается либо первый, либо второй генерирующий регистр.

Перемешивающий орграф $\Gamma(h)$ преобразования h множества V_{m+n+r} состояний генератора является $i \times (m + n)$- и $i \times (m + n + r)$-примитивным [4] для любого $i \in \{1, \ldots, m\}$; $\Gamma(h)$ содержит $i, (m+n)$-ксс U_1 и U_2 (с множествами вершин $\{1, \ldots, m\}$ и $\{m + 1, \ldots, m + n\}$ соответственно) и $i, (m + n + r)$-ксс U_3 с множеством вершин $\{m + n + 1, \ldots, m + n + r\}$. Для любого $i \in \{1, \ldots, m\}$ в орграфе $\Gamma(i, m + n)$ имеется два яруса: к 0-му ярусу относится ксс U_1, к 1-му — ксс U_2; в орграфе $\Gamma(i, m + n + r)$ также имеется два яруса: к 0-му ярусу относится ксс U_1, к 1-му — ксс U_3.

ЛИТЕРАТУРА

1. *Кяжин С. Н.* О применении условий локальной примитивности и оценок локальных экспонентов орграфов // Прикладная дискретная математика. 2016. № 4(34). С. 81–98.
2. *Кяжин С. Н., Фомичев В. М.* Локальная примитивность графов и неотрицательных матриц // Прикладная дискретная математика. 2014. № 3(25). С. 68–80.
3. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010. 424 с.
4. *Кяжин С. Н., Фомичев В. М.* Перемешивающие свойства двухкаскадных генераторов // Прикладная дискретная математика. Приложение. 2016. № 9. С. 60–62.

УДК 004.056.55 DOI 10.17223/2226308X/10/36

ВЕРСИЯ ПРОТОКОЛА ДИФФИ — ХЕЛЛМАНА, ИСПОЛЬЗУЮЩАЯ ДОПОЛНИТЕЛЬНЫЕ СКРЫТЫЕ МНОЖИТЕЛИ[1]

А. А. Обзор

Приводится версия протокола Диффи — Хеллмана, использующая скрытые множители из подгрупп мультипликативной группы конечного поля. Для раскрытия секрета данного протокола недостаточно решить проблему дискретного логарифма, необходимо также вычислить порядки некоторых элементов группы.

[1]Исследование выполнено за счёт гранта Российского научного фонда (проект №16-11-10002).