Секция 1

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 519.1 DOI 10.17223/2226308X/11/1

О ПЕРЕМЕШИВАЮЩИХ ГРАФАХ НЕЛИНЕЙНЫХ ПОДСТАНОВОК ДВОИЧНЫХ РЕГИСТРОВ СДВИГА

В. С. Григорьев

Исследован класс $R(n,m)$ подстановок n-мерного векторного пространства, реализуемых двоичными регистрами левого сдвига длины n с одной обратной связью $f(x_1,\ldots,x_n) = x_1 \oplus \psi(x_2,\ldots,x_n)$, зависящей существенно от m переменных, $3 \leqslant m \leqslant n$. Получена двусторонняя оценка экспонента перемешивающих орграфов $\Gamma(g)$ с множеством вершин $V = \{1,2,\ldots,n\}$ нелинейных подстановок $g \in R(n,m)$:

$$n + \left\lceil \frac{n-1}{m-1} \right\rceil - 1 \;\leqslant\; \exp\Gamma(g) \;\leqslant\; \Delta(D) + n + \left\lfloor \frac{(n-2)^2}{2} \right\rfloor - 1,$$

где $D(g) = \{i_1,\ldots,i_m\}$ — множество номеров существенных переменных функции обратной связи (ячеек съёма на регистре сдвига), $1 = i_1 < \ldots < i_m \leqslant n$, $m \leqslant n$; $\Delta(D)$ — наибольшее расстояние между соседними ячейками съёма на регистре сдвига: $\Delta(D) = \max\{i_2 - i_1, \ldots, i_m - i_{m-1}, n - i_m\}$. Получены верхние оценки суммы и отношения экспонентов перемешивающих орграфов подстановки g из класса $R(n,m)$ и обратной к ней подстановки g^{-1}:

$$\exp\Gamma(g) + \exp\Gamma(g^{-1}) \leqslant 2\left(\Delta(D) + \left\lfloor \frac{n^2}{m} \right\rfloor\right) + i_m,$$

$$\frac{\exp\Gamma(g)}{\exp\Gamma(g^{-1})} \leqslant \frac{\Delta(D) + n + \left\lfloor \frac{(n-2)^2}{2} \right\rfloor - 1}{n + \left\lceil \frac{n-1}{m-1} \right\rceil - 1}.$$

Ключевые слова: *матрично-графовый подход, перемешивающий граф преобразования, примитивный граф, экспонент орграфа, регистр сдвига, число Фробениуса.*

Введение

Положительным свойством преобразований векторных пространств, используемых в системах криптографической защиты информации, является полное перемешивание входных данных, то есть зависимость каждого бита выходного вектора от всех входных битов. Такие преобразования называются *совершенными*. При большой размерности пространства реализация совершенных преобразований затруднена в силу необходимости реализации большого количества связей между элементами входа и выхода. Поэтому полное перемешивание входных данных часто реализуется с помощью определённого количества итераций несовершенного преобразования. В связи с этим для

различных преобразований векторных пространств возникает задача оценки числа итераций, необходимого для достижения полного перемешивания.

Пусть подстановка $g(x_1, \ldots, x_n)$ задается системой булевых координатных функций

$$g(x_1, \ldots, x_n) = \{g_1(x_1, \ldots, x_n), \ldots, g_n(x_1, \ldots, x_n)\},$$

где функция g_j вычисляет j-й бит выходного вектора, $j = 1, 2, \ldots, n$.

Перемешивающим орграфом $\Gamma(g)$ подстановки g называется n-вершинный орграф, в котором существует дуга (i, j) тогда и только тогда, когда $i \in S(g_j)$, $i, j \in \{1, 2, \ldots, n\}$, где $S(g_j)$ — множество номеров существенных переменных функции g_j. Орграф $\Gamma(g)$ называется *примитивным*, если при некотором натуральном $t \geqslant 1$ орграф $\Gamma^t(g)$ полный. Наименьшее натуральное γ, при котором орграф $\Gamma^\gamma(g)$ полный, называется *экспонентом* орграфа и обозначается $\exp\Gamma(g)$.

Для полного перемешивания входов с помощью преобразования g необходима примитивность перемешивающего орграфа $\Gamma(g)$. Для оценки соответствующего количества итераций преобразования используется матрично-графовый подход, направленный на распознавание свойства примитивности перемешивающего орграфа преобразования и определение его экспонента.

Свойство примитивности и значения экспонентов для разных классов матриц и орграфов изучались многими авторами [1 – 3]. Получены как универсальные оценки экспонентов [4, 5], так и оценки для частных классов орграфов. Для приложений представляет интерес исследование взаимосвязи экспонентов перемешивающих орграфов прямой и обратной подстановок векторного пространства. Эти вопросы изучены мало. В общем случае экспоненты прямой и обратной подстановок не совпадают. Первые результаты были получены для регистровых подстановок. В [2, с. 12] установлено, что орграф $\Gamma(g)$ подстановки g примитивный тогда и только тогда, когда примитивен орграф $\Gamma(g^{-1})$. При этом $\exp\Gamma(g) = \exp\Gamma(g^{-1})$, если $i_k + i_{m+2-k} = n + 2$, $k = 2, \ldots, m$.

Работа посвящена классу нелинейных регистровых подстановок векторных пространств, широко используемому в системах защиты информации. Получены оценки экспонентов перемешивающих орграфов регистровых подстановок через числа множества $D(g)$, а также новые результаты о взаимосвязи экспонентов прямой и обратной подстановок.

1. Двусторонняя оценка экспонента

Через $g(x_1, \ldots, x_n) \in R(n, m)$ обозначим подстановку двоичного регистра левого сдвига длины n с обратной связью $f(x_1, \ldots, x_n) = x_1 \oplus \psi(x_2, \ldots, x_n)$:

$$g(x_1, \ldots, x_n) = (x_2, \ldots, x_n, x_1 \oplus \psi(x_2, \ldots, x_n)) = (y_1, \ldots, y_n). \tag{1}$$

Преобразование $g^{-1}(x_1, \ldots, x_n)$ реализуется двоичным регистром правого сдвига длины n с обратной связью $y_n \oplus \varphi(y_1, \ldots, y_{n-1})$:

$$g^{-1}(y_1, \ldots, y_n) = (y_n \oplus \varphi(y_1, \ldots, y_{n-1}), y_1, \ldots, y_{n-1}) = (x_1, \ldots, x_n), \tag{2}$$

где $\psi(x_2, \ldots, x_n) \oplus \varphi(y_1, \ldots, y_{n-1}) = \psi(x_2, \ldots, x_n) \oplus \varphi(x_2, \ldots, x_n) \equiv 0$.

Обозначим $D'(g) = D(g^{-1}) = \{j_1, \ldots, j_m\} = \{i_2 - 1, \ldots, i_m - 1, n\}$ — множество номеров существенных переменных функции обратной связи преобразования g^{-1}, где $1 \leqslant j_1 < \ldots < j_m = n$.

Для нелинейной подстановки $m = |D| \geqslant 3$. Действительно, если функция обратной связи $f(x_1, \ldots, x_n) = x_1 \oplus \psi(x_2, \ldots, x_n)$ нелинейная, то функция усложнения

$\psi(x_2,\ldots,x_n)$ содержит хотя бы один моном степени не меньше 2. Следовательно, функция обратной связи имеет, кроме x_1, ещё не менее двух существенных переменных.

В соответствии с (1) множество дуг n-вершинного перемешивающего орграфа $\Gamma(g)$ подстановки g состоит из дуг гамильтонова контура $(n,\ldots,2,1)$ и дуг $(i_2,n),\ldots,(i_m,n)$. Следовательно, орграф $\Gamma(g)$ содержит m простых контуров с длинами из множества $L=\{l_1,\ldots,l_m\}=\{n-i_m+1,\ldots,n-i_2+1,n\}$, где $1\leqslant l_1<\ldots<l_m=n$ и НОД$\{l_1,\ldots,l_m\}=1$.

В соответствии с (2) множество дуг n-вершинного перемешивающего орграфа $\Gamma(g^{-1})$ подстановки g^{-1} состоит из гамильтонова контура $(1,2,\ldots,n)$ и дуг $(i_2-1,1)$, $\ldots,(i_m-1,1)$. Следовательно, орграф $\Gamma(g^{-1})$ содержит m простых контуров с длинами из множества $L'=\{l'_1,\ldots,l'_m\}=\{n-l_{m-1},\ldots,n-l_1,n\}=\{i_2-1,\ldots,i_m-1,n\}$.

Заметим, что НОД$\{l_1,\ldots,l_m\}=1$, если и только если НОД$\{l'_1,\ldots,l'_m\}=1$. В соответствии с универсальным критерием орграф $\Gamma(g)$ примитивный, если и только если он сильносвязный и НОД$\{l_1,\ldots,l_m\}=1$.

Через $\Phi(L)$ обозначим функцию Фробениуса для множества L натуральных аргументов:

$$\Phi(L)=\max\{t\in\mathbb{N}:t\notin\langle L\rangle\},$$

где $\langle L\rangle$ — аддитивная полугруппа, порождённая множеством L. Для получения верхней оценки экспонента $\Gamma(g)$ используем оценку [5, с. 645]

$$\exp\Gamma(g)\leqslant\max_{1\leqslant i,j\leqslant n}\rho(i,n,j)+\Phi(L)+1,$$

где $\rho(i,n,j)$ — длина кратчайшего пути в орграфе $\Gamma(g)$ из вершины i в вершину j, проходящего через вершину n (общую вершину всех m контуров).

Для локального экспонента примитивного орграфа $\Gamma(g)$ справедлива оценка [6, с. 104]

$$(i,j)-\exp\Gamma(g)\leqslant\rho(i,n,j)+\Phi(L)+1,$$

где $\rho(i,n,j)=i-\gamma+1+n-j$; γ — индекс ближайшей слева ячейки съёма к ячейке j. В соответствии с (1) для примитивного орграфа $\Gamma(g)$

$$\max_{1\leqslant i,j\leqslant n}\rho(i,n,j)=\max_{1\leqslant i\leqslant n}\rho(i,n,1)=\Delta(D)+n-1.$$

Отсюда получаем

$$\exp\Gamma(g)\ \leqslant\ \Delta(D)+n+\Phi(L). \tag{3}$$

Технических трудностей при подсчёте оценки (3) можно избежать, воспользовавшись оценкой числа $\Phi(L)$. В соответствии с [7, с. 62] $\Phi(l_1,\ldots,l_{m-1},n)\leqslant\Phi(n-2,n-1,n)=$ $=\lfloor(n-2)^2/2\rfloor-1$. Следовательно,

$$\exp\Gamma(g)\leqslant\Delta(D)+n+\left\lfloor(n-2)^2/2\right\rfloor-1\leqslant n^2/2. \tag{4}$$

Нижняя оценка экспонента равна длине кратчайшего пути из i в j, проходящего через вершину n в орграфе $\Gamma(g)$, в случае, когда точки съёма примерно равноудалены друг от друга на регистре:

$$\exp\Gamma(g)\geqslant n+\left\lceil\frac{n-1}{m-1}\right\rceil-1. \tag{5}$$

2. Оценки суммы и отношения экспонентов перемешивающих орграфов прямой и обратной подстановок

На основе оценок чисел Фробениуса [8, с. 49–50] получена верхняя оценка экспонентов перемешивающих орграфов прямой и обратной подстановок.

Теорема 1. Для любой подстановки $g \in R(n, m)$ справедлива оценка

$$\exp\Gamma(g) + \exp\Gamma(g^{-1}) \leqslant 2\left(\Delta(D) + \left\lfloor \frac{n^2}{m} \right\rfloor\right) + i_m \leqslant \frac{2n^2}{3} + 3n - 7. \tag{6}$$

Из полученной двусторонней оценки следует оценка отношения экспонентов:

$$\frac{\exp\Gamma(g)}{\exp\Gamma(g^{-1})} \leqslant \frac{\Delta(D) + n + \left\lfloor \dfrac{(n-2)^2}{2} \right\rfloor - 1}{n + \left\lceil \dfrac{n-1}{m-1} \right\rceil - 1} < \frac{n}{2}. \tag{7}$$

Заключение

Для примитивных перемешивающих орграфов $\Gamma(g)$ нелинейных подстановок g из класса $R(n, m)$ получена двусторонняя оценка экспонентов. Верхняя оценка (4) не превосходит $n^2/2$, что улучшает абсолютную оценку Виландта [3, с. 102], а также при $l > n/2$ — оценку [9, с. 227], использующую длину l кратчайшего простого контура. Нижняя оценка (5) экспонентов уменьшается от $3n/2 - 1$ до n, когда значения m пробегают от 3 до n. В (6) показано, что сумма оценок экспонентов для прямой и обратной подстановок не превосходит $2n^2/3+3n-7$. Отношение оценок (7) экспонентов для прямого и обратного преобразований не превосходит $n/2$.

ЛИТЕРАТУРА

1. *Когос К. Г., Фомичев В. М.* Положительные свойства неотрицательных матриц // Прикладная дискретная математика. 2012. № 4(18). С. 5–13.
2. *Григорьев В. С., Фомичев В. М.* О примитивности перемешивающих подстановок регистров сдвига // Прикладная дискретная математика. Приложение. 2017. № 10. С. 14–16.
3. *Фомичев В. М.* Оценки экспонентов примитивных графов // Прикладная дискретная математика. 2011. № 2(12). С. 101–112.
4. *Фомичев В. М.* Новая универсальная оценка экспонентов графов // Прикладная дискретная математика. 2014. № 3(33). С. 78–84.
5. *Dulmage A. L. and Mendelsohn N. S.* Gaps in the exponent set of primitive matrices // Illinois J. Math. 1964. V. 8. Iss. 4. P. 642-656.
6. *Фомичев В. М., Кяжин С. Н.* Локальная примитивность матриц и орграфов // Дискретный анализ и исследование операций. 2017. Т. 24. № 1. С. 97–119.
7. *Lewin M.* A bound for a solution of a linear Diophantine problem // J. London Math. Soc. 1972. No. 6. P. 61–69.
8. *Alfonsin R. J.* The Diophantine Frobenius Problem. Oxford University Press, 2005. 260 p.
9. *Сачков В. Н., Тараканов В. Е.* Комбинаторика неотрицательных матриц. М.: ТВП, 2000.