О поведении функции Шеннона сложности реализации систем мономов схемами композиции

С. А. Корнеев[1]

В работе исследуется сложность реализации (минимально возможное число операций) систем мономов схемами, использующими двухвходовую операцию композиции, которую можно рассматривать как обобщение операции умножения. Установлено, что асимптотика роста функции Шеннона, характеризующей максимальную сложность среди систем из p мономов от q переменных с показателями степеней не более K, при условии $pq \log K \to \infty$ и некоторых дополнительных ограничениях имеет вид $\min(p, q) \log_2 K + \frac{pq}{\log_2(pq)}$.

Ключевые слова: система мономов, сложность вычисления, схемная сложность, схема композиции, функция Шеннона.

Изучается сложность вычисления (величина, равная минимальному числу операций) систем мономов схемами композиции. Схемы композиции представляют собой вычислительную модель с возможностью многократного использования результатов промежуточных вычислений, в которой единственной операцией является операция композиции двух мономов. Эта операция была предложена А. И. Ширшовым [1] как обобщение операции умножения. Схемы, использующие эту операцию, — схемы композиции — исследовались, например, в работах [2, 3, 4, 5].

Для мономов $U_1 = {x_1}^{a_1} {x_2}^{a_2} \dots {x_q}^{a_q}$ и $U_2 = {x_1}^{b_1} {b_2}^{b_2} \dots {x_q}^{a_q}$ будем говорить, что *моном* U_1 *содержится в мономе* U_2 (или что *моном* U_2 *содержит моном* U_1) и использовать обозначение $U_1 \le U_2$, если выполнены условия $a_k \le b_k$, $k = 1, \dots, q$. Если же хотя бы одно из этих условий не выполнено, то будем говорить, что *моном* U_1 *не содержится в мономе* U_2 (*моном* U_2 *не содержит моном* U_1) и использовать обозначение $U_1 \not\le U_2$. Моном с нулевым набором степеней будем называть *нулевым мономом*.

Пусть для мономов $U = {x_1}^{a_{11}} {x_2}^{a_{12}} \dots {x_q}^{a_{1q}}$, $V = {x_1}^{a_{21}} {x_2}^{a_{22}} \dots {x_q}^{a_{2q}}$ и $R = {x_1}^{b_1} {x_2}^{b_2} \dots {x_q}^{b_q}$ выполнены условия $R \le U$ и $R \le V$. Тогда моном

$$(U, V)_R = \frac{UV}{R} = {x_1}^{a_{11}+a_{21}-b_1} {x_2}^{a_{12}+a_{22}-b_2} \dots {x_q}^{a_{1q}+a_{2q}-b_q}$$

[1] *Корнеев Сергей Александрович* — аспирант каф. дискретной математики мех.-мат. ф-та МГУ, e-mail: korneev.sa.42@gmail.com.

Korneev Sergey Aleksandrovich — graduate student, Lomonosov Moscow State University, Faculty of Mechanics and Mathematics, Chair of Discrete Mathematics.

называется *композицией мономов U и V относительно монома R*. Отметим, что операция умножения мономов является частным случаем операции композиции, в этом случае R — нулевой моном.

Для удобства изложения определим схему композиции как схему из двухвходовых функциональных элементов (см., например, [6, 7, 8]), реализующих композицию мономов. Отметим, что схему композиции также можно определять как последовательность слов [2] или мономов [3, 4, 5], удовлетворяющую определённым условиям.

Схемой композиции над системой мономов $M = \{U_1, \ldots, U_r\}$ будем называть схему из двухвходовых функциональных элементов, удовлетворяющую следующим условиям:

а) на входы схемы подаются мономы $U_1, \ldots, U_r$;

б) каждый элемент вычисляет композицию двух подаваемых на его входы мономов относительно некоторого монома R (вообще говоря, своего для каждого элемента);

в) если на входы элемента E подаются мономы U и V, то соответствующий элементу E моном R удовлетворяет условиям $R \leq U$ и $R \leq V$.

Будем говорить, что *схема композиции S реализует систему мономов $V_1, \ldots, V_p$*, если эти мономы вычиляются на её выходах.

Если элемент E схемы S вычисляет моном U как композицию мономов U_1 и U_2 относительно монома R, то равенство $U = (U_1, U_2)_R$ будем называть *правилом вычисления монома U элементом E схемы S*.

Если S — схема композиции, то под *сложностью $l_{sh}(S)$ схемы композиции S* будем понимать число элементов в ней.

Пусть M и M_0 — системы мономов. Следуя [3], положим $l_{sh}(M) = \min l_{sh}(S)$, где минимум берётся по всем схемам композиции, реализующим систему M над множеством переменных $\{x_1, \ldots, x_q\}$. Величину $l_{sh}(M)$ будем называть *сложностью реализации системы мономов M схемами композиции*. Аналогично, величину $l_{sh}(M/M_0)$, определяемую равенством $l_{sh}(M/M_0) = \min l_{sh}(S)$, где минимум берётся по всем схемам композиции, реализующим систему мономов M над системой мономов M_0, будем называть *сложностью реализации системы мономов M над системой мономов M_0 схемами композиции*. Если для схемы S, реализующей систему мономов M над системой мономов M_0, выполнено условие $l_{sh}(S) = l_{sh}(M/M_0)$, то такую схему будем называть *минимальной схемой композиции* (реализующей систему мономов M над системой мономов M_0). Очевидно, что минимальная схема композиции не может содержать двух одинаковых элементов.

Заметим, что матрица из целых неотрицательных чисел

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1q} \\ a_{21} & a_{22} & \dots & a_{2q} \\ \dots & \dots & \dots & \dots \\ a_{p1} & a_{p2} & \dots & a_{pq} \end{pmatrix}$$

однозначно задаёт систему мономов

$$M_A = \{{x_1}^{a_{11}} {x_2}^{a_{12}} \dots {x_q}^{a_{1q}}, {x_1}^{a_{21}} {x_2}^{a_{22}} \dots {x_q}^{a_{2q}}, \dots, {x_1}^{a_{p1}} {x_2}^{a_{p2}} \dots {x_q}^{a_{pq}}\}.$$

Сложностью $l_{sh}(A)$ реализации матрицы A будем называть сложность реализации соответствующей этой матрице системы мономов M_A. В дальнейшем во всех терминах и обозначениях сложности будем допускать замену системы мономов на соответствующую матрицу (и наоборот).

Интерес к задаче о сложности вычисления системы мономов схемами композиции обусловлен несколькими факторами.

Во-первых, задача об исследовании разных свойств, в том числе и связанных с вопросами сложности, известной в алгебре (см., например, [1]) операции композиции, возникает естественным образом.

Во-вторых, операция композиции двух мономов является обобщением обычной операции умножения двух мономов (в том смысле, что операция умножения является частным случаем операции композиции — композицией относительно нулевого монома). Задачи о сложности вычисления схемами композиции одного монома от одной переменной, одного монома от нескольких переменных или системы из нескольких мономов от одной переменной имеют простое решение с точным ответом[1]) (см., например, [2]):

$$l_{sh}(x^a) = \lceil \log a \rceil ,$$

$$l_{sh}({x_1}^{a_1} {x_2}^{a_2} \dots {x_q}^{a_q}) = \left\lceil \log \max_{k:1 \le k \le q} a_k \right\rceil + q - 1,$$

$$l_{sh}({x_1}^{a_1}, {x_2}^{a_2}, \dots, {x_p}^{a_p}) = \lceil \log a_1 \rceil + \sum_{k=2}^{p} \left\lceil \log \left(\frac{a_k}{a_{k-1}} \right) \right\rceil , \quad 0 < a_1 < \dots < a_p,$$

причем в этих случаях точное значение сложности реализации схемами композиции асимптотически совпадает с величиной сложности реализации классическими схемами умножения (про эту вычислительную модель см., например, [9, 10]). Таким образом, этот подход позволяет выделить содержательную часть доказательства верхних и нижних оценок, отделив ее от технически сложной и трудоемкой, но не содержательной части.

[1]) Здесь и далее под записью $\log x$ понимается $\log_2 x$.

Еще одна важная составляющая интереса к исследованию сложности реализации систем мономов схемами композиции сформировалась уже в процессе изучения возможностей и свойств этой вычислительной модели. Выяснилось, что в этой модели имеют место интересные эффекты, отсутствующие, или, по крайней мере, неизвестные в близких вычислительных моделях — схемах умножения, схемах умножения и деления, а также схемах умножения с дополнительными входами, на которые подаются величины, обратные к исходным входным переменным (подробнее про эти модели см., например, [10]).

В частности, оказалось, что в отличие от классических схем из элементов умножения, а также схем из элементов умножения и деления, для схем композиции не работают соображения двойственности — известны примеры систем из n мономов от n переменных, задаваемых матрицами показателей степеней, которые получаются друг из друга путем транспонирования и при этом имеют принципиальное различие в сложности реализации схемами композиции [3].

В работе [11] было выявлено еще одно существенное отличие модели схем композиции от классических моделей. Для схем умножения и схем умножения-деления при реализации системы из двух мономов и при реализации системы мономов от двух переменных сложность по существу определяется некоторой квадратной подматрицей порядка 2 матрицы показателей степеней переменных в мономах (более того, для вычислительной модели, допускающей операции умножения и деления, при реализации системы из p мономов от q переменных схемами из элементов умножения и деления сложность по существу определяется некоторой квадратной подматрицей порядка $\min(p, q)$ матрицы показателей степеней в мономах). Аналогичный факт справедлив и при реализации системы из двух мономов схемами композиции [4]. Однако в случае вычисления системы из p мономов ситуация принципиально иная.

Следующий пример демонстрирует, что при фиксированном p даже удаление одного произвольного монома может изменить асимптотику роста сложности реализации матрицы размера $p \times 2$ схемами композиции, и следовательно, эта асимптотика не только не определяется подматрицей размера 2×2, но даже, вообще говоря, не определяется никакой подматрицей размера $(p-1) \times 2$.

Пусть p — чётное число (это непринципиально, пример легко обобщается на случай нечётного p). Рассмотрим матрицу

$$A = \begin{pmatrix} 2^{2n} & 1 \\ 2^{2n} & 2^{3n} \\ 2^{4n} & 2^{3n} \\ 2^{4n} & 2^{5n} \\ \dots & \dots \\ 2^{pn} & 2^{(p-1)n} \\ 2^{pn} & 2^{(p+1)n} \end{pmatrix}.$$

Обозначим через $A^{(k)}$ матрицу, полученную из матрицы A удалением k-й строки. Тогда

$$l_{sh}(A) = (2p+1)n + 1, \quad l_{sh}(A^{(k)}) = (2p-1)n + 1.$$

Рассмотрим последовательности матриц A_n и $A_n^{(k_n)}$, которые получаются из матриц A и $A^{(k)}$, соответственно, при $n = 1, 2, 3, \dots$ и произвольных $k_n \in \{1, 2, \dots, p\}$. Тогда

$$\lim_{n\to\infty} \frac{l_{sh}(A_n)}{l_{sh}(A_n^{(k_n)})} = 1 + \frac{1}{p - \frac{1}{2}},$$

т. е. асимптотика роста последовательности матриц $A_n^{(k_n)}$ отличается от асимптотики роста последовательности матриц A_n.

Приведенные отличия свойств функционала сложности вычисления систем мономов схемами композиции и функционалов сложности в классических вычислительных моделях не оставляют места для удивления по поводу того факта, что, несмотря на то, что при вычислении одного монома от нескольких переменных и при вычислении нескольких степеней одной переменной задача нахождения сложности в классе схем композиции принципиально проще аналогичной задачи в классе схем умножения, уже при вычислении системы из двух мономов от нескольких переменных и при вычислении системы из нескольких мономов от двух переменных эти задачи уже сопоставимы (при нахождении асимптотики роста сложности) [4, 9, 12], а в случае реализации системы из трех мономов от трех переменных асимптотика роста сложности в классе схем умножения известна [13, 14], а в классе схем композиции — нет.

Таким образом, в случае реализации систем мономов схемами композиции исследование вопросов сложности дало удовлетворительные результаты только в тех случаях, когда либо число переменных, либо число мономов не превосходит двух. Попытки установить асимптотику роста сложности в более общих случаях сталкиваются с принципиальными

трудностями, часть из которых описана выше. Обычно в таких случаях задачу исследования сложности реализации произвольной функции (в данном случае — системы мономов) заменяют существенно более простой задачей исследования асимптотического поведения функционала Шеннона, характеризующего максимальное значение сложности функций из некоторого класса.

Пусть $l(A)$, $l_2(A)$, $l_F(A)$ — сложность реализации (минимально возможное число операций в соответствующей модели) системы мономов, задаваемой матрицей A, схемами умножения, схемами умножения-деления и схемами умножения с дополнительными входами, на которые подаются величины, обратные к исходным входным переменным, соответственно. Определим функции Шеннона для этих моделей, а также для модели схем композиции.

$$L(p,q,K) = \max_{\substack{A:A=(a_{ij})_{p\times q}\\ 0\le a_{ij}\le K}} l(A), \quad L_2(p,q,K) = \max_{\substack{A:A=(a_{ij})_{p\times q}\\ -K\le a_{ij}\le K}} l_2(A).$$

$$L_F(p,q,K) = \max_{\substack{A:A=(a_{ij})_{p\times q}\\ -K\le a_{ij}\le K}} l_F(A), \quad L_{sh}(p,q,K) = \max_{\substack{A:A=(a_{ij})_{p\times q}\\ 0\le a_{ij}\le K}} l_{sh}(A).$$

В 1980 году Н. Пиппенджер, опираясь на свой результат об обобщённых вентильных схемах [15], основанный, в свою очередь, на результатах О. Б. Лупанова [16] и Э. И. Нечипорука [17], установил асимптотику роста функции Шеннона для классической модели.

Утверждение 1 [9]. *Пусть* $pq\log K \to \infty$. *Тогда*

$$L(p,q,K) = \min(p,q)\log K + \frac{pq\log(K+1)}{\log(pq\log K)}(1+o(1)) + O(p+q).$$

В работе [18] на основе результатов [10] при слабых ограничениях установлена асимптотика роста функции Шеннона $L_2(p,q,K)$.

Утверждение 2 [18]. *Пусть* $pq\log K \to \infty$. *Тогда*

$$L_2(p,q,K) = \min(p,q)\log K + \\ + \frac{pq\log(2K+1)}{\log(pq\log K)}\left(1 + O\left(\frac{\log\log pq\log K}{\log pq\log K}\right)^{1/2}\right) + O(\max(p,q)).$$

Для схем умножения с дополнительными входами, на которые подаются величины, обратные к исходным входным переменным, в работе [19] установлена асимптотика роста функции Шеннона, но при несколько более сильных ограничениях. Эти ограничения связаны с некоторыми нетривиальными особенностями данной модели, в частности, с тем, что в ней не работают в достаточной мере соображения двойственности.

Утверждение 3 [19]. *Пусть* $pq\log K \to \infty$. *Тогда справедливы неравенства*

$$L_F(p,q,K) \le \min(p,q+1)\log K + \\ + \frac{pq\log(2K+1)}{\log(pq\log K)}\left(1+O\left(\frac{\log\log pq\log K}{\log pq\log K}\right)^{1/2}\right)+O(\max(p,q)),$$

$$L_F(p,q,K) \ge \max\left(\min(p,q+1)\log K, \frac{pq\log(2K+1)}{\log(pq\log K)}\right)+O(\max(p,q)).$$

В данной работе при условии $pq\log K \to \infty$ и некоторых дополнительных ограничениях установлена асимптотика роста функции Шеннона сложности реализации систем мономов схемами композиции. Наличие этих ограничений во многом объясняется вышеописанными трудностями при исследовании сложности в вычислительной модели схем композиции.

Для доказательства основного результата (сформулированного ниже в виде теоремы) потребуется неколько лемм. Утверждение леммы 1 очевидно, доказательство леммы 2 можно найти в работе [4], утверждение леммы 3 легко следует из утверждения 1.

Лемма 1. *Если существуют схемы, реализующие систему мономов* M_1 *над системой мономов* M_0 *и систему мономов* M *над системой мономов* M_1, *то*

$$l_{sh}(M/M_0) \le l_{sh}(M/M_1) + l_{sh}(M_1/M_0).$$

Лемма 2 [4]. *Пусть мономы* $U = {x_1}^{a_1}{x_2}^{a_2}\dots{x_q}^{a_q}$ *и* $V = {x_1}^{b_1}{x_2}^{b_2}\dots{x_q}^{b_q}$ *удовлетворяют условиям* $a_k \ge b_k > 0$, $k = 1,\dots,q$. *Тогда*

$$l_{sh}(U/V) = \left\lceil \log \max_{k:1\le k\le q}\frac{a_k}{b_k}\right\rceil.$$

Лемма 3. *Пусть* $pq \to \infty$. *Тогда*

$$L_{sh}(p,q,1) \le \frac{pq}{\log(pq)}(1+o(1)) + O(p+q).$$

Обозначим через $M_d(p,q)$ класс булевых матриц $A = (a_{ij})$ размера $p \times q$ с единицами на главной диагонали, т. е. удовлетворяющих условиям

$$a_{ii} = 1, \quad i = 1,\dots,\min(p,q).$$

Положим

$$L_{sh}^{(d)}(p,q) = \max_{A\in M_d(p,q)} l_{sh}(A).$$

Лемма 4. *Пусть* $pq \to \infty$. *Тогда*[2])

$$L_{sh}^{(d)}(p,q) \gtrsim \frac{pq}{\log(pq)}.$$

Доказательство. Рассмотрим схемы из функциональных элементов в неполном базисе $\{\vee\}$, которые реализуют систему дизъюнкций, задаваемую булевой матрицей. Обозначим через $l_\vee(A)$ сложность вычисления в этой модели системы дизъюнкций, задаваемой матрицей A. Легко видеть, что тогда $l_{sh}(A) = l_\vee(A)$.

Количество матриц в классе $M_d(p,q)$ равно $2^{pq-\min(p,q)}$. Отсюда, учитывая условие $pq \to \infty$, получаем мощностную оценку (см., например, [20], теорема Д.1)

$$\max_{A\in M_d(p,q)} l_\vee(A) \gtrsim \frac{pq-\min(p,q)}{\log(pq-\min(p,q))} \gtrsim \frac{pq}{\log(pq)},$$

из которой следует

$$L_{sh}^{(d)}(p,q) = \max_{A\in M_d(p,q)} l_{sh}(A) = \max_{A\in M_d(p,q)} l_\vee(A) \gtrsim \frac{pq}{\log(pq)},$$

что и требовалось. □

Лемма 5. *Пусть* $pq\log K \to \infty$. *Тогда*

$$L_{sh}(p,q,K) \gtrsim \min(p,q)\log K + \frac{pq}{\log(pq)}.$$

Доказательство. Пусть A' — булева матрица с единицами на главной диагонали, для которой выполнено условие $l_{sh}(A') = L_{sh}^{(d)}(p,q)$, A — матрица, полученная из матрицы A' заменой всех диагональных элементов на K, S — минимальная схема, реализующая матрицу A.

Будем последовательно преобразовывать схему S, заменяя её элементы на элементы, реализующие операции композиции сдвух специальных типов. Операции композиции обоих типов обладают следующим свойством: моном R, относительно которого выполняется операция композиции, однозначно определяется исходными мономами.

1. Операция φ типа G по двум мономам U_1 и U_2, содержащим переменные не более чем в первой степени, вычисляет моном U, содержащий все переменные мономов U_1 и U_2 в первой степени:

[2]) Здесь и далее запись $a_n \gtrsim b_n$ обозначает, что $\overline{\lim\limits_{n\to\infty}} \frac{b_n}{a_n} \le 1$.

$$U_1 = {x_1}^{a_1}{x_2}^{a_2}\dots{x_q}^{a_q}, U_2 = {x_1}^{b_1}{x_2}^{b_2}\dots{x_q}^{b_q},$$
$$R = R(U_1,U_2) = {x_1}^{\min(a_1,b_1)}{x_2}^{\min(a_2,b_2)}\dots{x_q}^{\min(a_q,b_q)}$$
$$\varphi(U_1,U_2) = (U_1,U_2)_R = {x_1}^{\max(a_1,b_1)}{x_2}^{\max(a_2,b_2)}\dots{x_q}^{\max(a_q,b_q)},$$
$$a_k \in \{0,1\}, \quad b_k \in \{0,1\}, \quad k = 1,2,\dots,q.$$

2. Операция ψ_i типа G_i, $i = 1,\dots,q$ по двум мономам U_1 и U_2, содержащим переменную x_i в степенях a_i и b_i, соответственно, а все остальные переменные — не более чем в первой степени, вычисляет моном, содержащий переменную x_i в степени $a_i + b_i$, а все остальные переменные мономов U_1 и U_2 — в первой степени:

$$U_1 = {x_1}^{a_1}\dots{x_i}^{a_i}\dots{x_q}^{a_q}, U_2 = {x_1}^{b_1}\dots{x_i}^{b_i}\dots{x_q}^{b_q},$$
$$R_i = R_i(U_1,U_2) =$$
$$= {x_1}^{\min(a_1,b_1)}\dots{x_{i-1}}^{\min(a_{i-1},b_{i-1})}{x_{i+1}}^{\min(a_{i+1},b_{i+1})}\dots{x_q}^{\min(a_q,b_q)},$$
$$\psi_i(U_1,U_2) = (U_1,U_2)_{R_i} = {x_1}^{\max(a_1,b_1)}\dots{x_i}^{a_i+b_i}\dots{x_q}^{\max(a_q,b_q)},$$
$$a_k \in \{0,1\}, \quad b_k \in \{0,1\}, \quad a_i \in \mathbb{N}\cup\{0\}, \quad b_i \in \mathbb{N}\cup\{0\},$$
$$k = 1,\dots,i-1,i+1,\dots,q, \quad i = 1,\dots,q.$$

Пронумеруем все элементы схемы S так, чтобы на вход каждого элемента подавался моном, приписанный входу схемы, или моном, вычисляемый на выходе элемента с меньшим номером (см., например, [21], примечание 1). Заменим элементы схемы S в порядке возрастания их номеров по следующим правилам:
1. Если на выходе элемента вычисляется моном, содержащий переменные не более чем в первой степени, то заменим его на элемент, реализующий операцию типа G.
2. Если на выходе элемента вычисляется моном, содержащий переменную x_i хотя бы во второй степени, то заменим его на элемент, реализующий операцию типа G_i.

При таком преобразовании каждый элемент схемы S будет заменён на элемент, реализующий операцию одного из типов $G, G_1, \dots, G_{\min(p,q)}$ (это следует из вида матрицы A и минимальности схемы S). В результате получим некоторую схему композиции S_0, которая реализует некоторую матрицу A_0. Нетрудно заметить, что матрица A_0 может отличаться от матрицы A только в диагональных элементах (они могут увеличиться).

Для каждого i, $i = 1,\dots,\min(p,q)$, построим мультимножество $T_i(S_0)$ из мономов, содержащих переменную x_i в первой степени и подаваемых на входы элементов схемы S_0, реализующих операцию типа G_i. Если

для некоторого i в мультимножестве $T_i(S_0)$ есть моном, каждая переменная которого содержится в одном из других мономов мультимножества $T_i(S_0)$ (в том числе, если в это мультимножество входит ещё один такой же моном), то выберем в схеме S_0 любой элемент, реализующий операцию типа G_i, на вход которого подаётся этот моном. Удалим этот элемент, а на его выход подадим моном, который подавался на другой вход. В результате получим некоторую схему S_1, реализующую матрицу A_1, которая может отличаться от матрицы A только в диагональных элементах.

Так как при удалении элемента схема меняется, то для каждого следующего шага мультимножества строятся заново. Пусть уже построена схема S_k, $k = 1, 2, \ldots$, реализующая матрицу A_k.

Для каждого i, $i = 1, \ldots, \min(p, q)$, построим мультимножество $T_i(S_k)$ из мономов, содержащих переменную x_i в первой степени и подаваемых на входы элементов схемы S_k, реализующих операцию типа G_i. Если для некоторого i в мультимножестве $T_i(S_k)$ есть моном, каждая переменная которого содержится в одном из других мономов мультимножества $T_i(S_k)$, то выберем в схеме S_k любой элемент, реализующий операцию типа G_i, на вход которого подаётся этот моном. Удалим этот элемент, а на его выход подадим моном, который подавался на другой вход. В результате получим некоторую схему S_{k+1}, реализующую матрицу A_{k+1}, которая может отличаться от матрицы A только в диагональных элементах.

Будем продолжать этот процесс, пока на некотором шаге m не будет выполнено следующее условие: для любого i, $i = 1, \ldots, \min(p, q)$, каждый моном из мультимножества $T_i(S_m)$ содержит переменную, которая не содержится ни в одном другом мономе из мультимножества $T_i(S_m)$.

Пронумеруем все элементы схемы S_m так, чтобы на вход каждого элемента подавался моном, приписанный входу схемы, или моном, вычисляемый на выходе элемента с меньшим номером. Удалим из схемы S_m элемент с наименьшим номером, реализующий операцию типа G_i, для мономов U_1 и U_2, подаваемых на входы которого, выполнено условие $U_1 \leq U_2$ (или $U_2 \leq U_1$). На выход этого элемента подадим моном U_2 (соответственно, U_1). Будем продолжать этот процесс, пока такие элементы не закончатся. В результате получим некоторую схему S_{m+1}, реализующую матрицу A_{m+1}, которая может отличаться от матрицы A только в диагональных элементах.

Для схемы S_{m+1} аналогично построим семейство мультимножеств $T_i(S_{m+1})$, $i = 1, \ldots, \min(p, q)$. Для них также будет выполнено условие: для любого i, $i = 1, \ldots, \min(p, q)$ каждый моном из мультимножества $T_i(S_{m+1})$ содержит переменную, которая не содержится ни в одном другом мономе из мультимножества $T_i(S_{m+1})$. Пусть диагональные

элементы матрицы A_{m+1} равны $k_1, k_2, \ldots, k_{\min(p,q)}$. Тогда для всех i,$i = 1, \ldots, \min(p,q)$, каждый моном, содержащий переменную x_i в первой степени и подаваемый на вход элемента схемы S_{m+1}, реализующего операцию типа G_i, содержит переменную, которая не содержится ни в одном другом таком мономе, и поэтому $|T_i(S_{m+1})| < q$. Заметим также, что в схеме S_{m+1} каждый моном, содержащий переменную x_i, используется для порождения монома, соответствующего i-й строке матрицы A_{m+1}, не более одного раза, и поэтому $k_i \le |T_i(S_{m+1})|$.

Отсюда получаем неравенства

$$k_i < q, \quad i = 1, \ldots, \min(p,q). \tag{1}$$

Удаление одного элемента схемы может уменьшить степень только одной переменной только одного из мономов, реализуемых на выходах схемы, причём не более чем в два раза, и поэтому

$$l_{sh}(S_{m+1}) \le l_{sh}(S) - \sum_{i=1}^{\min(p,q)} \left\lceil \log\left(\frac{K}{k_i}\right) \right\rceil. \tag{2}$$

Пронумеруем все элементы схемы S_{m+1} так, чтобы на вход каждого элемента подавался моном, приписанный входу схемы, или моном, вычисляемый на выходе элемента с меньшим номером. Не меняя структуры схемы S_{m+1}, заменим её элементы, реализующие операции типа G_i, $i = 1, \ldots, \min(p,q)$, в порядке возрастания их номеров на элементы, реализующие операции типа G. В результате получим схему S', которая реализует матрицу A'.

Покажем, что

$$\min(p,q)\log q = o\left(\min(p,q)\log K + \frac{pq}{\log(pq)}\right). \tag{3}$$

Если величины p и q ограничены, то $K \to \infty$, откуда

$$\min(p,q)\log q = o\left(\min(p,q)\log K\right).$$

Пусть теперь хотя бы одна из величин p, q неограниченна. Рассмотрим два случая:

1. Если $p \le q$, то величина q неограниченна, и поэтому

$$\min(p,q)\log q = p\log q = o\left(\frac{pq}{\log q}\right) = o\left(\frac{pq}{\log(pq)}\right).$$

2. Если $q \le p$, то величина p неограниченна, и поэтому

$$\min(p,q)\log q = q\log q = o\left(\frac{pq}{\log(pq)}\right).$$

Наконец, используя (1), (2), (3) и лемму 4, получаем

$$L_{sh}(p,q,K) \geq l_{sh}(A) = l_{sh}(S) = l_{sh}(S_{m+1}) + \sum_{i=1}^{\min(p,q)} \left\lceil \log\left(\frac{K}{k_i}\right)\right\rceil =$$
$$= l_{sh}(S') + \sum_{i=1}^{\min(p,q)} \log\left(\frac{K}{k_i}\right) \geq l_{sh}(A') + \sum_{i=1}^{\min(p,q)} \log\left(\frac{K}{q}\right) =$$
$$= L_{sh}^{(d)}(p,q) + \min(p,q)\log K - \min(p,q)\log q \gtrsim$$
$$\gtrsim \min(p,q)\log K + \frac{pq}{\log(pq)},$$

что и требовалось. □

Лемма 6. *Пусть* $pq\log K \to \infty$. *Тогда*

$$L_{sh}(p,q,K) \leq p\log K + \frac{pq}{\log(pq)}(1+o(1)) + O(p+q).$$

Доказательство. Пусть $A = (a_{ij})$ — произвольная матрица размера $p\times q$ из целых неотрицательных чисел, элементы которой не превосходят K, и пусть A_1 — матрица, полученная из матрицы A заменой всех положительных элементов на 1. Используя леммы 1, 2 и 3, получаем

$$l_{sh}(A) \leq l_{sh}(A_1) + \sum_{i=1}^{p} \left\lceil \log \max_{j:1\leq j\leq q} a_{ij}\right\rceil \leq$$
$$\leq p\log K + \frac{pq}{\log(pq)}(1+o(1)) + O(p+q),$$

что и требовалось. □

Лемма 7. *Пусть* $pq\log K \to \infty$. *Тогда*

$$L_{sh}(p,q,K) \leq q\log K + (p+1)q.$$

Доказательство. Рассмотрим систему мономов

$$M_0 = \{{x_i}^{2^k} : i = 1,2,\ldots,q; k = 0,1,\ldots,\lceil\log K\rceil\}.$$

Используя леммы 1 и 2, получаем

$$l_{sh}(A) \leq l_{sh}(M_0) + l_{sh}(A/M_0) \leq q\lceil\log K\rceil + pq \leq q\log K + (p+1)q,$$

что и требовалось. □

Теорема. *Пусть* $pq \log K \to \infty$ *и дополнительно выполнено хотя бы одно из условий:*

а) $p \le q$;

б) $p = o(\log K)$;

в) $\log K = o(q/\log p)$.

Тогда

$$L_{sh}(p,q,K) = \left(\min(p,q)\log K + \frac{pq}{\log(pq)}\right)(1+o(1)) + O(p+q).$$

Доказательство. Нижняя оценка сразу следует из леммы 5. Докажем верхнюю оценку.

Если $p \le q$, то верхняя оценка непосредственно вытекает из леммы 6. Пусть теперь $p > q$ и $p = o(\log K)$. Тогда из леммы 7 получаем

$$L_{sh}(p,q,K) \le q\log K + (p+1)q = \\ = q\log K(1+o(1)) = \min(p,q)\log K(1+o(1)).$$

Наконец, пусть $p > q$ и $\log K = o(q/\log p)$. Тогда из леммы 6 получаем

$$L_{sh}(p,q,K) \le p\log K + \frac{pq}{\log(pq)}(1+o(1)) + O(p+q) = \\ = \frac{pq}{\log(pq)}(1+o(1)) + O(p+q).$$

Во всех случаях установлена требуемая верхняя оценка.

□

Список литературы

[1] Ширшов А.И., "Некоторые алгоритмические проблемы для алгебр Ли", *Сибирский математический журнал*, **3** (1962), 292–296.

[2] Мерекин Ю.В., "О порождении слов с использованием операции композиции", *Дискретный анализ и исследование операций. Сер.* 1., **10**:4 (2003), 70–78.

[3] Трусевич Е.Н., "О сложности вычисления некоторых систем одночленов схемами композиции", *Вестник Московского университета. Сер.* 1. *Математика. Механика.*, 2014, № 5, 18–22.

[4] Корнеев С.А., "О сложности реализации системы из двух мономов схемами композиции", *Дискретная математика*, **32**:2 (2020), 15–31.

[5] Корнеев С.А., "Об асимптотическом поведении функций шенноновского типа, характеризующих сложность вычисления систем мономов", *Учёные записки Казанского университета. Серия Физико-математические науки*, **162**:3 (2020), 300–311.

[6] Лупанов О.Б., *Асимптотические оценки сложности управляющих систем*, Издательство Московского университета, Москва, 1984, 138 с.

[7] Сэвидж Д.Е., *Сложность вычислений*, Издательство «Факториал», Москва, 1998, 368 с.

[8] Храпченко В.М., "Нижние оценки сложности схем из функциональных элементов", *Кибернетический сборник. Новая серия. Вып.* 21, Мир, Москва, 1984, 3–54.

[9] Pippenger N., "On the evaluation of powers and monomials", *SIAM J. Comput*, **9**:2 (1980), 230–250.

[10] Кочергин В.В., "О задачах Беллмана и Кнута и их обобщениях", *Фундаментальная и прикладная математика*, **20**:6 (2015), 159–189.

[11] Корнеев С.А., "О сложности реализации системы мономов от двух переменных схемами композиции", *Прикладная дискретная математика*, 2021, №53, 103–119.

[12] Кочергин В.В., "О сложности вычисления систем одночленов от двух переменных", *Труды* VII *Международной конференции «Дискретные модели в теории управляющих систем»*, МАКС Пресс, Москва, 2006, 185–190.

[13] Кочергин В.В., "О сложности вычисления системы из трёх одночленов от трёх переменных", *Математические вопросы кибернетики, вып.* 15, Физматлит, Москва, 2006, 79–155.

[14] Кочергин В.В., "Простое доказательство верхней оценки сложности вычисления трёх одночленов трёх переменных", *Вестник Московского университета. Сер.* 1. *Математика. Механика.*, Издательство Московского университета, Москва, 2019, 3–8.

[15] Pippenger N., "The minimum number of edges in graphs with prescribed paths", *Math. Systems Theory*, **12**:4 (1979), 325–346.

[16] Лупанов О.Б., "О вентильных и контактно-вентильных схемах", *Доклады АН СССР*, **111**:6 (1956), 1171–1174.

[17] Нечипорук Э.И., "О топологических принципах самокорректирования", *Проблемы кибернетики, вып.* 21, Наука, Москва, 1969, 5–102.

[18] Кочергин В.В., "Об аддитивных вычислениях систем целочисленных линейных форм", *Вестник Московского университета. Сер.* 1. *Математика. Механика*, 1993, №6, 97–101.

[19] Кочергин В.В., "О максимальной сложности вычисления систем элементов свободной абелевой группы", *Вестник московского университета. Сер.* 1. *Математика. Механика*, 2007, №3, 14–19.

[20] Лупанов О.Б., "Об одном подходе к синтезу управляющих систем — принципе локального кодирования", *Проблемы кибернетики, вып.* 10, Наука, Москва, 1965, 31–110.

[21] Лупанов О.Б., "О синтезе некоторых классов управляющих систем", *Проблемы кибернетики, вып.* 14, Физматгиз, Москва, 1963, 64–97.

On the behavior of the Shannon function of the implementation complexity of monomials system

Korneev Sergei Aleksandrovich

In this paper, we examined the computational complexity (minimum possible number of operations) of systems of monomials by circuits using two-input composition operation, which can be considered as a generalization of multiplication operation. We found

that growth asymptotic of the Shannon function, characterizing the maximum complexity among systems of p monomials of q variables with exponents no more than K, given that $pq \log K \to \infty$ and some additional restrictions, has the form $\min(p, q) \log_2 K + \frac{pq}{\log_2(pq)}$.

Keywords: set of monomials, computation complexity, circuit complexity, composition circuit, Shannon function.

References

[1] Shirshov A. I., "Nekotoryye algoritmicheskiye problemy dlya algebr Li [Some algorithmic problems for Lie algebras]", *Sibirskiy matematicheskiy zhurnal*, **3** (1962), 292–296 (in Russian).

[2] Merekin Yu. V., "O porozhdenii slov s ispol'zovaniyem operatsii kompozitsii [On the generation of words using the composition operation]", *Diskretnyy analiz i issledovaniye operatsiy. Ser. 1*, **10**:4 (2003), 70–78 (in Russian).

[3] Trusevich E. N., "Complexity of certain systems of monomials in calculation by composition circuits", *Moscow University Mathematics Bulletin*, **69**:5 (2014), 193–197.

[4] Korneev S. A., "On the complexity of implementation of a system of two monomials by composition curcuits", *Discrete Mathematics and Applications*, **31**:2 (2021), 113–125.

[5] Korneev S. A., "Ob asimptoticheskom povedenii funktsiy shennonovskogo tipa, kharakterizuyushchikh slozhnost' vychisleniya sistem monomov [On the asymptotic behavior of Shannon-type functions characterizing the computing complexity of systems of monomials]", *Uchenyye zapiski Kazanskogo universiteta. Seriya Fiziko-matematicheskiye nauki*, **162**:3 (2020), 300–311 (in Russian).

[6] Lupanov O. B., *Asimptoticheskie ocenki slozhnosti upravljajushhih sistem [Asymptotic estimates for complexity of control systems]*, 1984 (in Russian), 138 pp.

[7] Savage J. E., *The Complexity of Computing*, Krieger Pub Co, 1987, 391 pp.

[8] Hrapchenko V. M., "Nizhnie ocenki slozhnosti shem iz funkcional'nyh jelementov [Lower estimates for complexity of circuits of functional elements]", *Kiberneticheskij sbornik. Novaja serija. Vyp.* 21, 1984, 3–54 (in Russian).

[9] Pippenger N., "On the evaluation of powers and monomials", *SIAM J. Comput*, **9**:2 (1980), 230–250.

[10] Kochergin V. V., "On Bellman's and Knuth's problems and their generalizations", *Journal of Mathematical Sciences*, **233**:1 (2018), 103–124.

[11] Korneev S. A., "O slozhnosti realizacii sistemy monomov ot dvuh peremennyh shemami kompozicii [On the complexity of implementation of two-variable system of monomials by composition circuits]", *Prikladnaja diskretnaja matematika*, 2021, № 53, 103–119 (in Russian).

[12] Kochergin V. V., "O slozhnosti vychisleniya sistem odnochlenov ot dvukh peremennykh [On the complexity of computing systems of monomials in two variables]", *Trudy VII Mezhdunarodnoy konferentsii "Diskretnyye modeli v teorii upravlyayushchikh sistem"*, 2006, 185–190 (in Russian).

[13] Kochergin V. V., "O slozhnosti vychislenija sistemy iz trjoh odnochlenov ot trjoh peremennyh [On the computational complexity of three-variable system of three monomials]", *Matematicheskie voprosy kibernetiki, vyp.* 15, 2006, 79–155 (in Russian).

[14] Kochergin V. V., "Prostoe dokazatel'stvo verhnej ocenki slozhnosti vychislenija trjoh odnochlenov trjoh peremennyh [Easy proof for upper estimate of computational complexity of three-variable system of three monomials]", *Vestnik Moskovskogo universiteta. Ser.* 1. *Matematika. Mehanika*, 2019, 3–8 (in Russian).

[15] Pippenger N., "The minimum number of edges in graphs with prescribed paths", *Math. Systems Theory*, **12**:4 (1979), 325–346.

[16] Lupanov O. B., "O ventil'nyh i kontaktno-ventil'nyh shemah [On gating and contact gating curcuits]", *Doklady AN SSSR*, **111**:6 (1956), 1171–1174 (in Russian).

[17] Nechiporuk Je. I., "O topologicheskih principah samokorrektirovanija [On topological principles of self-correction]", *Problemy kibernetiki, vyp.* 21, 1969, 5–102 (in Russian).

[18] Kochergin V. V., "On additive computations of systems of integral linear forms", *Moscow University Mathematics Bulletin*, **48**:6 (1993), 62–64.

[19] Kochergin V. V., "On the maximal complexity of calculations of systems of elements of a free Abelian group", *Moscow University Mathematics Bulletin*, **62**:3 (2007), 95–100.

[20] Lupanov O. B., "Ob odnom podhode k sintezu upravljajushhih sistem — principe lokal'nogo kodirovanija [On one method for synthesis of control systems — local encoding principle]", *Problemy kibernetiki, vyp.* 10, 1965, 31–110 (in Russian).

[21] Lupanov O. B., "O sinteze nekotoryh klassov upravljajushhih sistem [On synthesis of some types of control systems]", *Problemy kibernetiki, vyp.* 14, 1963, 64–97 (in Russian).