Math-Net.Ru

Общероссийский математический портал

С. Б. Гашков, Арифметическая сложность некоторых линейных преобразований, *Матем. заметки*, 2015, том 97, выпуск 4, 529–555

DOI: <https://doi.org/10.4213/mzm10176>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением <http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 3.93.64.190

26 апреля 2023 г., 12:49:02

Арифметическая сложность некоторых линейных преобразований

С. Б. Гашков

Получены точные по порядку квадратичные и чуть более высокие оценки сложности вычисления некоторых линейных преобразований (биномиального, Стирлинга, Лаха, Гаусса, Серпинского, Сильвестра) в базисе $\{x + y\} \cup \{ax : |a| \leq C\}$, состоящем из операции сложения и скалярных умножений на ограниченные константы, а также верхние оценки $O(n \log n)$ для сложности вычисления в базисе, состоящем из всех линейных функций $\{ax + by : a, b \in \mathbb{R}\}$. Нижние оценки вида $\Omega(n \log n)$ получены для базиса из всех монотонных линейных функций $\{ax + by : a, b > 0\}$.

Для конечного арифметического базиса $B_{+,*}/ = \{x \pm y, xy, 1/x, 1\}$ и для базисов $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$, $B_{+,*} = \{x + y, xy, -1\}$ в некоторых случаях получены оценки вида $O(n \log n \log \log n)$. В случае полей характеристики p рассматривались также вычисления в базисе $\{x + y \bmod p\}$.

Библиография: 21 название.

DOI: 10.4213/mzm10176

1. Введение. Далее рассматриваются встречающиеся в различных вопросах конечномерные линейные преобразования над полями действительных и комплексных чисел (и над конечными полями) и оцениваются сложность их вычисления с помощью различных наборов элементарных арифметических операций в этих полях. Эти множества элементарных операций называются *базисами* (путаницы с понятием базиса в линейном пространстве обычно не возникает). *Сложность вычисления* – это число выполненных операций (далее будет дано формальное определение).

В комбинаторике [1], [2] известно *биномиальное преобразование* $\mathbb{R}^n \rightarrow \mathbb{R}^n$ и обратное к нему, определяемые соответственно формулами

$$y_k = \sum_{m=0}^k \binom{k}{m} x_m, \quad x_k = \sum_{m=0}^k (-1)^{k-m} \binom{k}{m} y_m, \quad k = 0, \dots, n-1,$$

где $\binom{k}{m} = k!/(m!(k-m)!)$ – биномиальные коэффициенты. Матрица этого преобразования треугольная, ее ненулевые элементы образуют *треугольник Паскаля порядка n* . Используя тождество Паскаля, легко вычислить все числа, образующие треугольник Паскаля, с помощью $(n-1)(n-2)/2$ операций сложения¹. Этот алгоритм

¹ Работа выполнена при поддержке Российского фонда фундаментальных исследований (гранты №№ 14-01-00598, 14-01-00671а).

оптимален в случае *аддитивного базиса* $B_+ = \{x + y, 1\}$, и в более широком базисе он также оптимален².

Используемая модель вычислений в случае базиса B_+ известна под названием аддитивные цепочки [3]. *Аддитивной цепочкой длины l* называется последовательность натуральных чисел $a_0, \dots, a_l$, в которой $a_0 = 1$ и каждое число a_i равно сумме каких-то двух предшествующих чисел $a_j, a_k, j < i, k < i$ (не обязательно $j \neq k$; в случае $j = k$ соответствующий шаг цепочки называется *удвоением*). Аддитивная цепочка может начинаться не с единицы, а с произвольной переменной x . Тогда она вычисляет функцию nx . Аналогично определяются мультипликативные цепочки, вычисляющие степени x^n (хотя такой термин не используется по очевидным причинам). Согласно [3] задачи, в которых речь шла об аддитивных цепочках, появились в одном французском журнале в конце 19-го века. Точная формула для функции $l(n)$, равной длине кратчайшей аддитивной цепочки, заканчивающейся числом n , неизвестна. Альфред Брауэр в 30-е годы доказал, что $l(n)$ асимптотически равна $\log_2 n$ (с тех пор этот результат многократно переоткрывался). Совсем легко получить оценку $l(n) = O(\log n)$. Для ее доказательства достаточно построить цепочку по следующему правилу (цепочка строится с конца): если n четно, то вычисляем n как удвоение $n/2$, а если n нечетно, то вычисляем n путем прибавления единицы: $n = (n - 1) + 1$.

Есть обобщение этой модели, называемое *векторными аддитивными цепочками* (см., например, [3], [4]). Эти цепочки состоят из векторов заданной длины m и начинаются с m единичных векторов вида $(0, \dots, 1, 0, \dots, 0)$. Их можно рассматривать как *схемы с входами* $x_1, \dots, x_m$ в базисе B_+ . Такими схемами можно вычислить любые системы линейных многочленов с натуральными коэффициентами. Подобные схемы для вычисления произвольных многочленов с целыми коэффициентами рассматривались, например, в [5].

Приведем общее определение схемы (неветвящейся программы) для произвольного базиса B , состоящего из операций вида $\omega_i(x_1, \dots, x_{n_i}): E^{n_i} \rightarrow E$, где E – заданное множество, например, множество действительных чисел³. *Схемой с входами* $x_1, \dots, x_n$ называется последовательность функций⁴

$$f_i(x_1, \dots, x_n): E^n \rightarrow E, \quad i = 1, \dots, l,$$

начинающаяся с селекторных функций $e_i(x_1, \dots, x_n) = x_i, i = 1, \dots, n$ (т.е. попросту с переменных x_i), в которой каждая функция $f_i(x_1, \dots, x_n)$ вычисляется с помощью некоторой базисной операции⁵ $\omega_j(y_i, \dots, y_{n_j})$ и каких-то предыдущих функций $f_{k_r}, k_r < i, r = 1, \dots, n_j$:

$$f_i(x_1, \dots, x_n) = \omega_j(f_{k_1}(x_1, \dots, x_n), \dots, f_{k_{n_j}}(x_1, \dots, x_n)).$$

Сложностью схемы называется число $l - n$ функций в ней (кроме селекторных функций, которые рассматриваются как *входы схемы*). Схема *реализует (вычисляет)* функцию $g(x_1, \dots, x_n)$ (или вектор-функцию $g_1, \dots, g_m$), если эта функция

¹В силу его симметрии фактическое число сложений почти в два раза меньше.

²Потому что число операций в вычислении не может быть меньше количества вычисляемых чисел.

³Для некоторых базисных операций может быть $n_i = 0$, т.е. операция вычисляет константу.

⁴Некоторые переменные у них могут быть фиктивными, т.е. значение функции от них не зависит.

⁵Если эта операция – константа, то и вычисляемая ей функция тоже константа.

встречается в последовательности $f_i(x_1, \dots, x_n)$, $i = 1, \dots, l$ (обычно на последнем месте). Схема вычисляет вектор функцию $g_1, \dots, g_m$, если все функции g_i встречаются в последовательности f_i , $i = 1, \dots, l$. Если в схеме каждая функция (кроме входов) используется только один раз при вычислении следующих за ней функций, то такая схема называется *формулой*. *Сложностью вычисления* функции g (или вектор-функции $g_1, \dots, g_m$) схемами (или формулами) в данном базисе B называется минимальная сложность схемы (формулы) в этом базисе, реализующей данную функцию (вектор-функцию)⁶.

Далее рассматривается сложность схемной реализации некоторых линейных преобразований, использующихся в комбинаторике (и других областях), например преобразований Стирлинга обоих родов, преобразований Лаха и Гаусса. В качестве базисов, кроме упомянутого аддитивного базиса B_+ , используются конечный арифметический базис $B_{+,*./} = \{x + y, x - y, xy, 1/x, 1\}$, конечный полиномиальный базис $B_{+,*} = \{x + y, xy, -1\}$, континуальный линейный базис $B_l = \{ax + by : a, b \in \mathbb{R}\}$ и его подмножества: базис с вычитанием $B_{+,-}$, счетный линейный базис $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$, линейный базис с ограниченными константами $B_{l,C} = \{x + y\} \cup \{ax : |a| \leq C\}$ и монотонный линейный базис $B_{m,l} = \{ax + by : a, b \in \mathbb{R}_+\}$. Для вычисления p -ичного преобразования Серпинского применяется базис $\{x + y \bmod p\}$, операция которого выполняется в поле простой характеристики p , а для вычисления преобразования Сильвестра – базис $B_{\oplus} = \{x \oplus y\}$, где операция есть сложение по модулю два. Определения всех упомянутых линейных преобразований даются в соответствующих пунктах статьи.

Рассмотрены также несколько задач о сложности вычисления не самих линейных преобразований, а их коэффициентов. Для этого используются базисы B_+ , $B_{+,*}$, $B_{+,*./}$.

Полученные результаты сведены в таблицу. В ней b_n , C_n , s_n , S_n , L_n , G_n соответственно обозначают преобразования n -го порядка биномиальное, Серпинского, Стирлинга 1-го и 2-го рода, Лаха и Гаусса, а $B_{l,C}$, B_l , $B_{+,*}$, $B_{+,*./}$ – определенные выше базисы операций. Через $Tb_n, \dots, TG_n$ обозначены матрицы коэффициентов упомянутых преобразований, т.е. треугольники Паскаля, Стирлинга, Лаха, Гаусса, а через $T_nb_n, \dots, T_nG_n$ – нижние строки этих матриц. Для них в таблице приводятся оценки сложности вычисления указанных множеств коэффициентов. В преобразовании Гаусса параметр q предполагается нечетным и малым в сравнении с n , поэтому в оценках он не появляется. Все оценки приведены с точностью до порядка, хотя в некоторых случаях они получены в более точном виде. Базисы B_+ и $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$ в таблицу не включены, так как оценки для них совпадают с оценками для базисов $B_{l,C}$ и $B_{+,*./}$ соответственно. Также не включен базис $B_{l,m}$, потому что для него получены только нижние оценки вида $\Omega(n \log n)$ и только для преобразований b_n , C_n , L_n , G_n . Не включены в таблицу оценки для преобразования Адамара–Сильвестра и p -ичного преобразования Серпинского. Они все имеют вид $O(n \log n)$. Некоторые из оценок данной таблицы тривиальны или непосредственно следуют из оценок для других базисов (так как $B_{l,C}$ содержится в B_l , а $B_{+,*}$ содержится в $B_{+,*./}$).

⁶Очевидно, что сложность формульной реализации не меньше (а, как правило, больше) сложности схемной реализации. Формульная сложность далее не рассматривается.

ТАБЛИЦА

	$B_{l,C}$	B_l	$B_{+,*}$	$B_{+,*,/}$
b_n	$\Theta(n^2)$	$O(n \log n)$	$O(n^2)$	$O(n \log n \log \log n)$
C_n	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$	$O(n \log n)$
S_n	$O(n^2 \log n)$	$O(n^2)$	$O(n^2)$	$O(n^{3/2} \log^{3/2} n \log \log n)$
s_n	$\Theta(n^2 \log n)$	$O(n^2)$	$O(n^2)$	$O(n^2)$
L_n	$\Theta(n^2 \log n)$	$O(n \log n)$	$O(n^2)$	$O(n \log n \log \log n)$
G_n	$\Theta(n^3)$	$O(n \log n)$	$O(n^2)$	$O(n \log n \log \log n)$
Tb_n	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$
TS_n	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$
TS_n	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$
TL_n	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$
TG_n	$O(n^3)$	$\Theta(n^2)$	$\Theta(n^2)$	$\Theta(n^2)$
T_nb_n	$O(n^2/\log n)$	$\Theta(n)$	$O(n \log n \log \log n)$	$\Theta(n)$
T_nS_n	$O(n^2)$	$\Theta(n)$	$O(n \log^2 n \log \log n)$	$O(n \log n \log \log n)$
T_ns_n	$O(n^2)$	$\Theta(n)$	$O(n \log^2 n \log \log n)$	$O(n \log^2 n \log \log n)$
T_nL_n	$O(n^2/\log n)$	$\Theta(n)$	$O(n \log n \log \log n)$	$\Theta(n)$
T_nG_n	$O(n^3/\log n)$	$\Theta(n)$	$O(n \log^2 n \log \log n)$	$\Theta(n)$

2. Сложность биномиального преобразования. Используя аналог треугольника Паскаля, можно вычислить биномиальное преобразование в аддитивном базисе B_+ со сложностью $n(n-1)/2$.

Действительно, вычислим сначала с помощью $n-1$ операций сложения все суммы вида $x_0 + x_1, x_1 + x_2, \dots, x_{n-2} + x_{n-1}$, потом вычислим с помощью $n-2$ операций сложения все суммы вида

$$\begin{aligned}
 (x_0 + x_1) + (x_1 + x_2) &= x_0 + 2x_1 + x_2, (x_1 + x_2) + (x_2 + x_3) \\
 &= x_1 + 2x_2 + x_3, \dots, (x_{n-3} + x_{n-2}) + (x_{n-2} + x_{n-1}) \\
 &= x_{n-3} + 2x_{n-2} + x_{n-1},
 \end{aligned}$$

и так далее, «на $(n-2)$ -м ярусе» схемы вычислим две суммы

$$\sum_{i=0}^{n-2} \binom{n-1}{i} x_i, \quad \sum_{i=1}^{n-1} \binom{n-1}{i-1} x_i,$$

а на последнем « $n - 1$ -м ярусе» с помощью одного сложения вычисляем

$$\begin{aligned} & \sum_{i=0}^{n-2} \binom{n-1}{i} x_i + \sum_{i=1}^{n-1} \binom{n-1}{i-1} x_i \\ &= x_0 + x_{n-1} + \sum_{i=1}^{n-2} \left(\binom{n-1}{i-1} + \binom{n-1}{i} \right) x_i = \sum_{i=0}^{n-1} \binom{n}{i} x_i. \end{aligned}$$

Для обоснования указанных тождеств применяется тождество Паскаля. Общее число использованных сложений равно

$$(n-1) + (n-2) + \dots + 1 = \frac{n(n-1)}{2}.$$

Среди вычисленных сумм встречаются все суммы из биномиального преобразования n -го порядка.

Если в рассмотренной схеме заменить операции сложения на операции сложения по модулю p , то получится схема той же сложности для вычисления биномиального преобразования по модулю p . Его коэффициенты образуют треугольник Паскаля по модулю p . Последнее замечание далее будет использовано.

Очевидная нижняя оценка сложности биномиального преобразования n -го порядка равна $n - 1$. Получим нетривиальную нижнюю оценку для более широкого *линейного базиса с ограниченными константами* $B_{l,C} = \{x + y\} \cup \{ax : |a| \leq C\}$ (который можно рассматривать и в поле комплексных чисел). Далее везде $a(n) = \Theta(b(n))$ означает равенство по порядку $a(n) \leq Cb(n)$, $b(n) \leq Ca(n)$, C не зависит от n .

ТЕОРЕМА 1. *Сложность вычисления биномиального преобразования порядка n в линейном базисе с ограниченными константами $B_{l,C}$ равна $\Theta(n^2)$.*

ДОКАЗАТЕЛЬСТВО. Для доказательства нижней оценки используется следующая

ЛЕММА 1 [5]. *Для любой последовательности линейных форм $l_i(x_1, \dots, x_n)$ такой, что $l_i = x_i$, $i = 1, \dots, n$, и для всякого $j > i$ либо $l_j = al_m$, $|a| \leq C$, $m < j$, либо $l_j = l_s + l_m$, $s, m < j$, рассмотрим $(L \times n)$ -матрицу A , строки которой образованы коэффициентами рассматриваемой последовательности линейных форм l_j , $j = 1, \dots, L$. Для любого $k \leq n$ обозначим Δ_k максимум модулей миноров порядка k (т.е. определителей подматриц порядка k) этой матрицы. Тогда*

$$\Delta_k \leq \max(C, 2)^{L-n}.$$

ДОКАЗАТЕЛЬСТВО. Лемма доказывается индукцией по L . База ($L = n$) очевидна.

Шаг индукции. Достаточно рассмотреть только миноры, содержащие $(L + 1)$ -ю строку матрицы A . Пусть M – такой минор. Для простоты обозначений будем считать, что $k = n$. Его нижняя строка либо равна al_i , либо равна $l_i + l_j$, где $i, j \leq L$ (строки матрицы также обозначаем l_i). Во втором случае рассмотрим миноры M_i, M_j , полученные из M заменой нижней строки на l_i или l_j соответственно, тогда согласно свойству определителей $M = M_i + M_j$. В первом случае, умножив в M_i нижнюю строку на a , получим, очевидно, минор $M_{i,a}$, равный рассматриваемому. Если полученные подматрицы содержат равные строки, то соответствующие миноры равны нулю. В противном случае по предположению индукции $M_i, M_j \leq \max(C, 2)^{L-k}$. Поэтому во всех рассматриваемых случаях $M \leq \max(C, 2)^{L+1-k}$.

Пусть биномиальное преобразование порядка n вычисляется схемой сложности L . Очевидно, матрица этого преобразования является подматрицей определенной в лемме матрицы A (она образована n строками матрицы A , не обязательно соседними, для наглядности можно считать, что нижняя часть матрицы A совпадает с матрицей рассматриваемого биномиального преобразования). При $r = \lfloor n/3 \rfloor$ эта матрица, а значит, и матрица A , содержит минор $(r+1)$ -го порядка⁷

$$\begin{vmatrix} \binom{2r}{r} & \binom{2r}{r+1} & \cdots & \binom{2r}{2r} \\ \binom{2r+1}{r} & \binom{2r+1}{r+1} & \cdots & \binom{2r+1}{2r} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{3r}{r} & \binom{3r}{r+1} & \cdots & \binom{3r}{2r} \end{vmatrix}.$$

Согласно задаче 317 из [6] этот минор равен

$$\frac{\binom{3r}{r+1}}{\binom{2r}{r+1}} \cdots \frac{\binom{2r+1}{r+1}}{\binom{r+1}{r+1}} = \frac{3r!(r-1)!}{2r!(2r-1)!} \cdots \frac{(2r+1)!}{r!(r+1)!}$$

(далее это будет доказано). Используя предыдущее равенство, оценим снизу первую дробь

$$\frac{3r!(r-1)!}{2r!(2r-1)!} = 2 \frac{3r!r!}{(2r!)^2}.$$

Применяя формулу Стирлинга и выполняя сокращения дробей, получим

$$\frac{3r!r!}{(2r!)^2} \geq \Omega\left(\left(\frac{27}{16}\right)^r\right).$$

Следующие дроби по величине больше ее, так как, деля друг на друга соседние дроби, имеем $(2r-a)(2r-1-a) > (3r-a)(r-1-a)$, так как $2r(2r-1) > 3r(r-1)$. Поэтому произведение всех дробей

$$\frac{\binom{3r}{r+1}}{\binom{2r}{r+1}} \cdots \frac{\binom{2r+1}{r+1}}{\binom{r+1}{r+1}} \geq \left(\frac{27}{16}\right)^{r^2 - \Omega(r)},$$

значит, $\Delta_{r+1} \geq 2^{\Omega(n^2)}$. Применяя лемму, имеем $L \geq \Omega(\log \Delta_{r+1}) \geq \Omega(n^2)$, что доказывает теорему.

Для полноты докажем равенство из задачи 317 [6], следуя указаниям этого задачника:

$$\det \begin{vmatrix} \binom{m}{k} & \binom{m}{k+1} & \cdots & \binom{m}{k+n} \\ \binom{m+1}{k} & \binom{m+1}{k+1} & \cdots & \binom{m+1}{k+n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n}{k} & \binom{m+n}{k+1} & \cdots & \binom{m+n}{k+n} \end{vmatrix} = \frac{\binom{m+n}{n+1} \binom{m+n-1}{n+1} \cdots \binom{m+n-k+1}{n+1}}{\binom{k+n}{n+1} \binom{k+n-1}{n+1} \cdots \binom{n+1}{n+1}}.$$

⁷Вероятно, это наибольший из миноров матрицы рассматриваемого биномиального преобразования, но этот факт не будет использоваться.

Записывая биномиальные коэффициенты как

$$\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k(k-1)\cdots 1}$$

и пользуясь однородным свойством определителя, выносим из первой строки множитель m , из второй – множитель $m+1$ и т.д., из последней – множитель $m+n$. Аналогично выносим из первого столбца множитель $1/k$, из второго – множитель $1/(k+1)$ и т.д., из последнего – множитель $1/(k+n)$. Заменяя каждый элемент оставшегося определителя $\frac{i}{j}\binom{j}{i}$ на $\binom{j-1}{i-1}$ и замечая, что

$$\frac{m(m+1)\cdots(m+n)}{k(k+1)\cdots(k+n)} = \frac{\binom{m+n}{n+1}}{\binom{k+n}{n+1}},$$

получаем тождество

$$\det \begin{vmatrix} \binom{m}{k} & \binom{m}{k+1} & \cdots & \binom{m}{k+n} \\ \binom{m+1}{k} & \binom{m+1}{k+1} & \cdots & \binom{m+1}{k+n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n}{k} & \binom{m+n}{k+1} & \cdots & \binom{m+n}{k+n} \end{vmatrix} = \frac{\binom{m+n}{n+1}}{\binom{k+n}{n+1}} \det \begin{vmatrix} \binom{m-1}{k-1} & \binom{m-1}{k} & \cdots & \binom{m-1}{k+n-1} \\ \binom{m}{k-1} & \binom{m}{k} & \cdots & \binom{m}{k+n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n-1}{k-1} & \binom{m+n-1}{k} & \cdots & \binom{m+n-1}{k+n-1} \end{vmatrix}.$$

Повторяя эту процедуру еще $k-1$ раз, имеем

$$\begin{aligned} \det \begin{vmatrix} \binom{m}{k} & \binom{m}{k+1} & \cdots & \binom{m}{k+n} \\ \binom{m+1}{k} & \binom{m+1}{k+1} & \cdots & \binom{m+1}{k+n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n}{k} & \binom{m+n}{k+1} & \cdots & \binom{m+n}{k+n} \end{vmatrix} \\ = \frac{\binom{m+n}{n+1}\binom{m+n-1}{n+1}\cdots\binom{m+n-k+1}{n+1}}{\binom{k+n}{n+1}\binom{k+n-1}{n+1}\cdots\binom{n+1}{n+1}} \det \begin{vmatrix} \binom{m-k}{0} & \binom{m-k}{1} & \cdots & \binom{m-k}{n} \\ \binom{m+1-k}{0} & \binom{m+1-k}{1} & \cdots & \binom{m+1-k}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n-k}{0} & \binom{m+n-k}{1} & \cdots & \binom{m+n-k}{n} \end{vmatrix}. \end{aligned}$$

Остается доказать, что

$$\det \begin{vmatrix} \binom{m}{0} & \binom{m}{1} & \cdots & \binom{m}{n} \\ \binom{m+1}{0} & \binom{m+1}{1} & \cdots & \binom{m+1}{n} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n}{0} & \binom{m+n}{1} & \cdots & \binom{m+n}{n} \end{vmatrix} = 1.$$

Вычитая из n -й строки $(n-1)$ -ю, из $(n-1)$ -й – $(n-2)$ -ю и т.д., пользуясь тождеством Паскаля и разлагая полученный определитель по первому столбцу, находим,

что предыдущий определитель равен

$$\det \begin{vmatrix} 1 & \binom{m}{1} & \cdots & \binom{m}{n} \\ 0 & \binom{m}{0} & \cdots & \binom{m}{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \binom{m+n-1}{0} & \cdots & \binom{m+n-1}{n-1} \end{vmatrix} = \det \begin{vmatrix} \binom{m}{0} & \binom{m}{1} & \cdots & \binom{m}{n-1} \\ \binom{m+1}{0} & \binom{m+1}{1} & \cdots & \binom{m+1}{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n-1}{0} & \binom{m+n-1}{1} & \cdots & \binom{m+n-1}{n-1} \end{vmatrix}.$$

Повторяя эту процедуру понижения порядка еще $n - 1$ раз, доходим до единичной матрицы порядка один.

Другой вариант доказательства можно найти в [7]. Там формула для рассматриваемого определителя получена в виде (используем наши обозначения)

$$\prod_{i=1}^k \prod_{j=1}^{n+1} \frac{m - k + i + j - 1}{i + j - 1}$$

и доказано, что она выражает число трехмерных диаграмм Юнга, лежащих в параллелипипеде размера $(m - k) \times k \times (n + 1)$. Ссылки на задачник [6] в [7] нет, возможно потому, что упомянутая формула для числа диаграмм Юнга, а также, по-видимому, и формула для рассматриваемого определителя была известна еще в начале 20-го века майору Макмагону⁸.

Если расширить базис до *линейного базиса* $B_l = \{x + y\} \cup \{ax : a \in \mathbb{R}\}$, включив в него так называемые *скалярные умножения*⁹, то справедлива следующая теорема.

ТЕОРЕМА 2. *Сложность вычисления биномиального преобразования порядка n в линейном базисе B_l равна $O(n \log n)$, в конечном арифметическом базисе $B_{+,*}/ = \{x \pm y, xy, 1/x, 1\}$ – равна $O(n \log n \log \log n)$. Такая же оценка справедлива и для базиса $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$. Сложность вычисления биномиального преобразования порядка n в поле характеристики p в базисе $\{x + y \bmod p\}$ не больше $((p - 1)/2)n \log_p n$.*

ДОКАЗАТЕЛЬСТВО. Биномиальное преобразование порядка n можно представить в виде *свертки*

$$\frac{y_k}{k!} = \sum_{m=0}^k \frac{1}{(k - m)!} \frac{x_m}{m!}, \quad k = 0, \dots, n - 1,$$

векторов $(1/0!, \dots, 1/(n - 1)!)$, $(x_0/0!, \dots, x_{n-1}/(n - 1)!)$, значит, для вычисления $y_k/k!$, $k = 0, \dots, n - 1$, достаточно найти младшие n коэффициентов произведения многочленов

$$\left(1 + t + \frac{t^2}{2!} + \cdots + \frac{t^{n-1}}{(n - 1)!}\right) \left(x_0 + x_1 t + \frac{x_2}{2!} t^2 + \cdots + \frac{x_{n-1}}{(n - 1)!} t^{n-1}\right).$$

Если обозначить через $M(n)$ сложность умножения двух многочленов степени $n - 1$ в *полиномиальном базисе* $B_{+,*} = \{x + y, xy, -1\}$, то в арифметическом базисе $B_{+,*}/$

⁸Преподавателю королевской военной академии и автору монографии по комбинаторному анализу, так и не переведенной на русский язык.
⁹Унарные операции, являющиеся умножениями на фиксированные константы.

сложность вычисления $y_k/k!$, $k = 0, \dots, n-1$, оценивается сверху как $M(n) + 4n$. Действительно, в указанном базисе прогрессию $\{1, 2, \dots, n-1\}$ можно вычислить со сложностью $n-2$, а потом систему факториалов $\{1!, 2!, \dots, (n-1)!\}$ с помощью операций $k! = k \cdot (k-1)!$ можно вычислить со сложностью $n-2$, потом векторы $(1/0!, \dots, 1/(n-1)!)$, $(x_0/0!, \dots, x_{n-1}/(n-1)!)$ вычисляются с помощью $2(n-2)$ операций деления на вычисленные факториалы. Значит, сложность вычисления биномиального преобразования порядка n в арифметическом базисе оценивается как $M(n) + 5n$. Метод умножения Кантора–Калтофена [8] дает оценку $M(n) = O(n \log n \log \log n)$ даже в полиномиальном базисе. Так как один из сомножителей состоит из констант, а алгоритмы Кантора–Калтофена и Шёнхаге [8]–[10] *билинейные*, то ту же оценку можно получить и в счетном линейном базисе $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$ (в этом базисе указанные выше векторы вычисляются со сложностью $2(n-2)$).

В базисе B_l в обоих полях $\mathbb{R}, \mathbb{C}$ справедлива оценка $O(n \log n)$. Действительно, умножение многочленов сводится к трехкратному применению *быстрого преобразования Фурье* [10]–[12]. Сложность вычисления БПФ равна $O(n \log n)$ уже в базисе $B_{l,1}$. Так как первый сомножитель имеет фиксированные коэффициенты, то одно из БПФ фактически можно не выполнять. Кроме БПФ нужно еще $O(n)$ операций скалярного умножения на произвольные константы (для покомпонентного перемножения n -мерных векторов, получившихся в результате БПФ; так как один из этих векторов состоит из констант, то умножения будут скалярными). Поэтому в базисе B_l биномиальное преобразование порядка n можно вычислить со сложностью $O(n \log n)$, причем скалярных умножений на большие по модулю константы нужно только $O(n)$.

Остается доказать последнее утверждение теоремы 2. При этом можно ограничиться конечным полем $GF(p)$, а треугольник Паскаля определять с помощью тождества Паскаля по модулю p .

Пусть $p^{k-1} < n \leq p^k$. Достаточно доказать, что при $n = p^k$ сложность вычисления преобразования F_n :

$$y_k = \sum_{m=0}^k \binom{k}{m} x_m, \quad k = 0, \dots, n-1,$$

оценивается как $(p(p-1)/2)n \log_p n$. Матрица P_n этого преобразования согласно теореме Люка (см., например, [13]) состоит из чисел

$$\begin{aligned} \binom{i}{j} \bmod p &= \binom{i_0}{j_0} \cdots \binom{i_{k-1}}{j_{k-1}} \bmod p, & \binom{i}{j} &= 0, \quad i < j, & \binom{0}{0} &= 1, \\ i &= i_0 + i_1 p + \cdots + i_{k-1} p^{k-1}, & j &= j_0 + j_1 p + \cdots + j_{k-1} p^{k-1}, \\ 0 &\leq i_s, j_s < p, & s &= 0, \dots, k-1, \end{aligned}$$

поэтому представима в виде *кронекерова произведения* $P_n = P_p \otimes P_{n/p}$, т.е. состоит из p^2 подматриц $A_{i,j} = \left(\binom{i}{j} \bmod p \right) P_{n/p}$ размера $n/p \times n/p$ (это известная «фрактальная» структура p -ичного треугольника Паскаля), значит, преобразование $y = F_n(x)$ можно вычислить, применив вначале p раз преобразование $F_{n/p}$ к векторам

$$(x_0, \dots, x_{n/p-1}), \quad \dots, \quad (x_{(p-1)n/p}, \dots, x_{n-1}),$$

и вычислив p (n/p) -мерных векторов $z_0, \dots, z_{p-1}$, а потом применить к этим векторам покомпонентно n/p раз преобразование F_p . Отсюда вытекает рекуррентная оценка сложности $L(n) \leq pL(n/p) + L(p)n/p$. Так как согласно замечанию перед теоремой 1 $L(p) \leq p(p-1)/2$, то $L(n) \leq pL(n/p) + n(p-1)/2$, откуда по индукции имеем

$$L(n) \leq \frac{(k-1)n(p-1)}{2} + p^{k-1}L(p) = \frac{kn(p-1)}{2} = \frac{(p-1)}{2} n \log_p n.$$

ЗАМЕЧАНИЕ 1. Для базиса $B_{+,*,/}$ в любом поле характеристики большей n (или нулевой) справедлива верхняя оценка $M(n) + O(n)$. В поле нулевой характеристики то же самое верно и для базиса $B_l = \{x + y\} \cup \{ax : a \in \mathbb{Q}\}$. Если в этом базисе использовать для умножения многочленов алгоритм Шёнхаге [9], [10], то число скалярных умножений на константы равно $O(n \log n)$.

3. Монотонный линейный базис. Задачу о вычислении преобразования F_n , матрица которого состоит из чисел $\binom{i}{j} \bmod p$, можно рассмотреть и в поле характеристики нуль и аддитивном базисе $\{x + y\}$. Очевидно, что в этом случае $L(p) = O(p^2 \log p)$, потому что каждый из p^2 коэффициентов преобразования $L(p)$ меньше, чем p , поэтому согласно приведенной во введении оценке для длины аддитивных цепочек имеем $L(p) \leq p^2 + p^2 l(p) = O(p^2 \log p)$, откуда, как и в доказательстве теоремы 2, выводится, что $L(n) = O(np(\log p) \log_2 n)$.

В случае $p = 2$ рекуррентное правило построения матрицы $M_k = P_{2^k}$ выглядит особенно просто:

$$M_{k+1} = \begin{vmatrix} M_k & 0 \\ M_k & M_k \end{vmatrix}, \quad M_0 = 1.$$

Матрица M_k размера $n \times n$, $n = 2^k$, в [14] называется *матрицей Серпинского*¹⁰, и для соответствующего преобразования там доказана нижняя оценка $(n/2) \log_2 n$ сложности в базисе B_+ . На самом деле там доказано точное равенство, но в базисе $\{x \oplus y\}$, так как рассматривались линейные преобразования над полем $GF(2)$ и нижняя оценка была получена для схем с некоторыми ограничениями. Доказательство [14] можно перенести на случай произвольных схем в базисе B_+ и преобразований над $\mathbb{R}$ с матрицей $a_{i,j} = \binom{i}{j} \bmod 2$ (при $n = 2^k$ это матрица Серпинского M_k).

Определим индуктивно последовательность

$$f(n) = f(2^k) + f(n - 2^k) + n - 2^k, \quad 2^k < n \leq 2^{k+1}, \quad f(0) = f(1) = 0.$$

По индукции можно вывести явное выражение $f(n)$ по данной двоичной записи $n = \sum_{i=1}^m 2^{k_i}$, $k_1 < \dots < k_m$,

$$f(n) = \sum_{i=1}^m 2^{k_i-1} k_i + \sum_{i=1}^{m-1} 2^{k_i} (m-i) > \frac{n}{4} \log_2 n, \quad f(2^k) = 2^{k-1} k.$$

ТЕОРЕМА 3. Сложность вычисления биномиального преобразования порядка n в монотонном линейном базисе $B_{m,l} = \{ax + by : a, b \in \mathbb{R}_+\}$ не меньше $f(n)$, сложность r -ичного биномиального преобразования порядка n с коэффициентами $a_{i,j} =$

¹⁰Потому, что она подобна «салфетке Серпинского», но, видимо, правильнее ее назвать матрицей Паскаля–Серпинского.

$\binom{i}{j} \bmod p$, $a_{i,j} = 0$, $i < j$, в базисе $B_{m,l}$ не меньше $((p-1)/p^2)n \log_p n$, а в случае $p = 2$ сложность преобразования Серпинского порядка n с матрицей $(a_{i,j}) = (\binom{i}{j} \bmod 2)$ в базисах $B_{m,l}$ и B_+ равна $f(n)$.

ДОКАЗАТЕЛЬСТВО. Докажем нижнюю оценку для преобразования Серпинского C_n индукцией по n . Для этого используем метод [14], но получим при этом результат для любого n . База ($n = 1, 2$) очевидна.

Шаг индукции. Пусть дана схема S с входами $x_1, \dots, x_n$, вычисляющая преобразование C_n . Выделим в ней подсхему S_1 , состоящую из элементов, связанных только с входами $x_1, \dots, x_{2^k}$, $2^k < n \leq 2^{k+1}$.¹¹ Очевидно, что если оба «предка» элемента схемы S принадлежат подсхеме S_1 , то он и сам ей принадлежит. Эта подсхема содержит выходы $y_1, \dots, y_{2^k}$ и вычисляет преобразование C_{2^k} (элементы, связанные с входами x_m , $m > 2^k$, не используются для вычисления y_t , $t \leq 2^k$, в противном случае в силу монотонности y_t , $t \leq 2^k$, зависело бы от x_m , $m > 2^k$, что невозможно в силу треугольности матрицы C_n). Поэтому сложность S_1 согласно предположению индукции не меньше $f(2^k)$.

Рассмотрим подсхему S_2 , состоящую из всех элементов, не входящих в S_1 . Подставим нули вместо входов x_i , $i \leq 2^k$. На выходах y_j , $j > 2^k$, тогда будет вычисляться преобразование $C_{n-2^k}(x_{2^k+1}, \dots, x_n)$. На выходах всех элементов из S_1 появятся нули. Обозначим S_3 множество элементов из S_2 , которые после указанной подстановки превратятся в одноходовые элементы ax . При $a = 1$ такой элемент «исчезает», а при $a \neq 1$ его можно удалить, умножив на a «коэффициенты» элемента, соединенного с его входом x . Число оставшихся элементов S_2 согласно предположению индукции не меньше $f(n - 2^k)$.

Оценим снизу число элементов S_3 . Пусть их m , и $z_1, \dots, z_m$ — линейные функции от $x_1, \dots, x_n$, реализуемые на выходах этих элементов. Так как элементы из S_3 не принадлежат S_1 , то они имеют «предков» из S_2 , поэтому в силу монотонности все z_i должны зависеть от каких-то x_j , $j > 2^k$. Подадим на входы x_i , $i > 2^k$, нули. Функции z_i превратятся в функции $z'_i(x_1, \dots, x_{2^k})$, а функции $y_{2^k+1}, \dots, y_n$ — в функции $y'_j(x_1, \dots, x_{2^k})$, $j = 1, \dots, n - 2^k$. Обозначим все ненулевые функции, которые реализуются на выходах элементов из S_2 при указанной подстановке нулей, через u_l . Среди них будут содержаться все z'_i и все y'_j . Для произвольного элемента, реализующего u_l , рассмотрим подсхему, образованную им самим и всеми его «предками». На каждой цепи, соединяющей этот элемент с входами x_i , либо найдется элемент, реализующий нуль при указанной подстановке, либо найдется элемент из S_1 . Его предшественник на этой цепи будет по определению принадлежать S_3 и, значит, реализовывать на своем выходе некоторую функцию z'_i . Выберем на каждой цепи по одному такому элементу¹². Функция u_l является линейной комбинацией функций, реализуемых на выходах выбранных элементов. Значит, она является линейной комбинацией функций z'_i . В частности, все функции y'_j , $j = 1, \dots, n - 2^k$, линейно выражаются через z'_i , $i = 1, \dots, m$.

Заметим, что функции y'_j , $j = 1, \dots, n - 2^k$, линейно независимы. Действительно, они совпадают с функциями y_j , $j = 1, \dots, n - 2^k$, преобразования C_n (это следует из рекуррентного построения матрицы $M_{k+1} = C_{2^{k+1}}$ и того факта, что матрица

¹¹То есть из тех элементов, которые не соединяются цепью элементов с входом x_m , $m > 2^k$.

¹²Реализующему на своем выходе или нуль или одну из функций z'_i .

C_n лежит в верхнем левом углу матрицы $C_{2^{k+1}}$, а все функции преобразования C_n линейно независимы, так как его матрица треугольная с единицами на диагонали. Поэтому $m \geq n - 2^k$ согласно известной лемме линейной алгебры. Из доказанного имеем, что сложность схемы S не меньше

$$f(2^k) + f(n - 2^k) + n - 2^k = f(n).$$

Докажем по индукции, что можно построить схему S сложности $f(n)$, реализующую преобразование C_n . База ($n = 1, 2$) очевидна.

Шаг индукции. Пусть построены схемы S_1, S_2 , реализующие $C_{2^k}(x_1, \dots, x_{2^k})$ и $C_{n-2^k}(x_{2^k+1}, \dots, x_n)$ со сложностью $f(2^k) = 2^{k-1}k$ и $f(n - 2^k)$ соответственно. Функции $y_i(x_1, \dots, x_i)$, $i \leq 2^k$, преобразования C_n совпадают с функциями преобразования C_{2^k} , и поэтому они реализованы подсхемой S_1 . Подсхема S_2 реализует функции $y'_i(x_{2^k+1}, \dots, x_n)$, $i < n - 2^k$. Подавая ее выходы на входы $n - 2^k$ элементов $x + y$, а на другие их входы подавая выходы элементов подсхемы S_1 , реализующие функции $y_i(x_1, \dots, x_i)$, $i \leq n - 2^k \leq 2^k$, получаем (согласно рекуррентной конструкции матрицы $C_{2^{k+1}}$) на выходах добавленных $n - 2^k$ сумматоров функции $y_i(x_1, \dots, x_i)$, $i = 2^k + 1, \dots, n$. Построенная схема имеет сложность

$$f(2^k) + f(n - 2^k) + n - 2^k = f(n).$$

Для биномиального преобразования нижняя оценка доказывается аналогично. Нужно лишь проверить, что любой минор, расположенный ниже диагонали матрицы биномиального преобразования, отличен от нуля, что гарантирует линейную независимость функций y'_j , $j = 1, \dots, n - 2^k$, из доказательства нижней оценки. Неравенство нулю указанных миноров следует, например, из формул для них, данных в доказательстве теоремы 1¹³.

Для p -ичного обобщения преобразования C_n данное доказательство не проходит, но его можно видоизменить, получив при $n = p^k$ нижние оценки $L(n) \geq (1 - 1/p) \times n \log_p n$. Для этого индуктивно доказывается оценка

$$L(mp^k) \geq L((m-1)p^k) + L(p^k) + p^k \geq mL(p^k) + (m-1)p^k,$$

откуда следует, что $L(p^{k+1}) \geq pL(p^k) + p^{k+1}(1 - 1/p)$, и далее по индукции получаем, что $L(p^k) \geq (1 - 1/p)p^k k$. Для обоснования линейной независимости возникающих в доказательстве функций достаточно установить, что определители матриц порядков p^i , примыкающие к левой стороне матрицы биномиального преобразования, отличны от нуля. Так как эти определители в матрице P_{p^k} , полученной из матрицы биномиального преобразования приведением по модулю p , также примыкают к ее левой стороне¹⁴, то для их вычисления можно применить прием из доказательства теоремы 1 и убедиться, что эти определители отличны от нуля.

ЗАМЕЧАНИЕ 2. Верхняя оценка сложности биномиального преобразования в базисе $B_{m,l}$ равна $O(n^2)$. Как ее улучшить, неясно. В базисе B_+ это сделать нельзя согласно теореме 1. А в базисе B_l можно согласно теореме 2. Если рассматривать биномиальное преобразование в поле характеристики p , то для базиса $\{x + y \bmod p\}$

¹³Отличие от нуля тех миноров, которые нужны для доказательства, следует также из того, что те же миноры, взятые по модулю два, равны единице в матрице C_n .

¹⁴См. доказательство теоремы 2.

можно аналогичным образом получить такие же оценки, если наложить на схемы ограничение, такое же как в [14], а именно, рассматривать только схемы, в которых при сложении линейных функций никогда не возникают нулевые коэффициенты при сложении по модулю p ненулевых коэффициентов, т.е. фактически векторные аддитивные цепочки – схемы над базисом B_+ . Доказательство нижней оценки указанного вида проходит для любого треугольного линейного преобразования, в котором подходящие миноры отличны от нуля.

В [15], [16] для схем в линейном базисе с определенными ограничениями (так называемых направленных вычислений) и линейных преобразований с треугольными матрицами вида

$$M_{k+1} = \begin{vmatrix} M_k & 0 \\ Q_k & T_k \end{vmatrix},$$

получены рекуррентные нижние оценки вида $L(M_{k+1}) \geq L(M_k) + L(T_k) + \text{rank } Q_k$. Аналогичные оценки можно получить и в базисе $B_{m,l}$.

В случае, когда $Q_k = E_k$ – единичная матрица, $M_k = T_k$, в [15], [16] получено равенство

$$L(M_k) = \frac{n}{2} \log_2 n, \quad n = 2^k.$$

Очевидно, что сумма модулей элементов матрицы M_k , обозначаемая $|M_k|$, равна $O(n \log_2 n)$. В случае, когда Q_k – матрица, состоящая из единиц, кроме диагонали, на которой стоят нули, и $T_k = M_k$, справедливы равенства по порядку $|M_k| = \Theta(n^2)$ для суммы модулей элементов матрицы M_k и $L_{B_{m,l}}(M_k) = O(n \log_2 n)$ для сложности соответствующего линейного преобразования. Для доказательства нижних оценок достаточно заметить, что определитель матрицы Q_k не равен нулю (см. задачу 324 [6]). Для доказательства верхних оценок заметим, что сложность реализации преобразования с матрицей Q_k в базисе $\{x + y\}$ не больше $3n - 4$ (на самом деле она равна $3n - 4$ согласно [17]), и применим рекуррентные верхние оценки $L_{B_{m,l}}(M_{k+1}) \geq 2L_{B_{m,l}}(M_k) + 4n - 2$. В случае, когда $Q_k = I_k$ – матрица, состоящая из одних единиц, M_{k+1} есть треугольная матрица с единицами на диагонали и ниже ее, и тогда $L_{B_{m,l}}(M_k) = n - 1$.

4. Сложность преобразования Сильвестра. Если заменить указанное выше рекуррентное правило на следующее:

$$A_{k+1} = \begin{vmatrix} A_k & \neg A_k \\ A_k & A_k \end{vmatrix}, \quad A_0 = 1,$$

где $\neg A_k$ обозначает *булеву матрицу*, состоящую из отрицаний элементов булевой матрицы A_k , то получим булеву матрицу Сильвестра¹⁵. Для нее в базисе $B_{\oplus} = \{x \oplus y\}$, где операция сложения есть сложение по модулю два, сложность реализации соответствующего линейного преобразования не больше $(n/2) \log_2 n$, $n = 2^k$, что доказывается аналогично теореме 2.

¹⁵Или Адамара–Сильвестра.

Обычная матрица Сильвестра получается из булевой заменой нулей на минус единицы и вычисляется по рекуррентному правилу

$$S_{k+1} = \begin{vmatrix} S_k & -S_k \\ S_k & S_k \end{vmatrix}, \quad S_0 = 1.$$

ТЕОРЕМА 4. В базисе $B_{l,C}$ сложность преобразования с матрицей Сильвестра S_k , $n = 2^k$, равна $\Theta(n \log_2 n)$. То же самое верно и для матрицы A_k .

ДОКАЗАТЕЛЬСТВО. Верхние оценки доказываются аналогично теореме 2. Они справедливы для $B_- = \{x - y\}$. Аналогично теореме 1 для преобразования с матрицей S_k получим нижнюю оценку $\Omega(n \log n)$. Для этого заметим, что $\det S_{k+1} = 2^{2^k} (\det S_k)^2$, $\det S_0 = 1$, откуда по индукции имеем, что $\log_2 \det S_k = (n/2) \log_2 n$. Докажем указанную рекуррентную формулу для $\det S_{k+1}$. Для этого используем известные свойства определителей и заметим, что

$$\det \begin{vmatrix} S_k & -S_k \\ S_k & S_k \end{vmatrix} = \det \begin{vmatrix} 2S_k & 0 \\ S_k & S_k \end{vmatrix},$$

откуда следует то, что нужно.

Нижняя оценка для преобразования с матрицей A_k теперь выводится из оценки для матрицы S_k . Действительно, пусть преобразование $A_k(X)$ реализуется в базисе $B_{l,C}$ со сложностью $L(n)$. Умножая выходы схемы на 2 (это можно сделать n элементами $x + x$) и вычитая из них $x_1 + \dots + x_n$ (сложность вычитания не больше $2n - 1$), можно реализовать преобразование $S_k(X)$ со сложностью не больше $L(n) + 3n$. Из полученной выше нижней оценки для $S_k(X)$ следует неравенство $L(n) > \Omega(n \log_2 n)$ для $A_k(X)$.

ЗАМЕЧАНИЕ 3. Для базиса $B_{\oplus} = \{x \oplus y\}$, где операция сложения есть сложение по модулю два, в [18] было доказано, что $L_{B_{\oplus}}(A_k) = O(n)$, $n = 2^k$ (на самом деле $L_{B_{\oplus}}(A_k) < 3n$).

Для базиса $B_{+,-} = \{x + y, x - y\}$ можно доказать равенства

$$L_{B_{+,-}}(A_k) = \frac{n}{2} \log_2 n + O(n), \quad L_{B_{+,-}}(S_k) = \frac{n}{2} \log_2 n + O(n).$$

5. Сложность строки треугольника Паскаля. В силу тождества

$$\binom{n}{k} = \frac{n - k + 1}{k} \binom{n}{k-1}$$

очевидно, что для базиса $B_{+,*}/$ сложность вычисления $\binom{n}{k}$, $k = 0, \dots, n$, равна по порядку n . Для базиса B_+ Цыганков в дипломной работе¹⁶ показал, используя результат из [4], что сложность вычисления $\binom{n}{k}$, $k = 0, \dots, n$, асимптотически не больше $(n^2/4) \ln n$.

ТЕОРЕМА 5. В полиномиальном базисе $B_{+,*} = \{x + y, xy, -1\}$ сложность вычисления n -й строки треугольника Паскаля равна $O(n \log n \log \log n)$.

¹⁶Выполненной в 2012 г. под руководством автора данной статьи на кафедре дискретной математики мехмата МГУ.

ДОКАЗАТЕЛЬСТВО. Вычисление $\binom{n}{k}$, $k = 0, \dots, n$, равносильно вычислению коэффициентов многочлена $p_n(x) = (1+x)^n$. Поскольку $p_n(x) = p_{n/2}^2(x)$ или $p_n(x) = p_{(n-1)/2}^2(x)(1+x)$ в зависимости от четности n , сложность $L(n)$ коэффициентов многочлена p_n рекуррентно оценивается как

$$L(n) \leq L\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + M\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + O(n),$$

где $M(n)$ – сложность умножения двух многочленов степени $n-1$ в базисе $B_{+,*} = \{x+y, xy, -1\}$.

Очевидно, что $M(n)$ монотонна. Можно считать¹⁷, что $M(n) \geq 2M(n/2)$. По индукции имеем

$$L(n) \leq M\left(\frac{n}{2}\right) + M\left(\frac{n}{4}\right) + \dots + M(1) + O\left(n + \frac{n}{2} + \dots + 1\right) \leq M(n) + O(n).$$

Для оценки $M(n)$ в базисе $B_{+,*}$ можно применить алгоритм Кантора–Калтофена.

6. Числа и преобразования Стирлинга и Лаха. Рассмотрим преобразования Стирлинга 1-го рода $y = s(x)$ и 2-го рода $x = S(y)$, взаимно обратные друг к другу:

$$y_k = \sum_{m=0}^k s_m^k x_m, \quad x_k = \sum_{m=0}^k S_m^k y_m, \quad k = 0, \dots, n-1,$$

где s_m^k, S_m^k – числа Стирлинга 1-го и 2-го рода соответственно.

Матрицы этих преобразований являются треугольными матрицами, ненулевые элементы которых образуют *треугольники Стирлинга* порядка n 1-го и 2-го рода соответственно. Эти треугольники (подобно треугольнику Паскаля) определяются *тождествами Стирлинга*:

$$s_k^n = s_{k-1}^{n-1} - (n-1)s_k^{n-1}, \quad S_k^n = kS_k^{n-1} + S_{k-1}^{n-1}, \quad S_0^n = s_0^n = 0, \quad n > 0, \quad S_0^0 = s_0^0 = 1.$$

Эти числа встречаются и в других тождествах, например,

$$x^n = \sum_{k=0}^n S_k^n (x)_k, \quad (x)_k = x(x-1) \cdots (x-k+1), \quad (x)_0 = 1, \quad (x)_n = \sum_{k=0}^n s_k^n x^k, \\ (x)^n = x(x+1) \cdots (x+n-1) = \sum_{k=0}^n |s_k^n| x^k, \quad k! S_k^n = \sum_{m=0}^k \binom{k}{m} m^n (-1)^{k-m},$$

и имеют комбинаторные интерпретации [1], [2]: S_k^n равно числу разбиений n -элементного множества на k непустых подмножеств, а $|s_k^n|$ равно числу подстановок n -го порядка, разлагающихся в произведение k непересекающихся циклов.

Монотонное преобразование Стирлинга 1-го рода определяется равенством

$$y_k = \sum_{m=1}^k |s_m^k| x_m, \quad k = 1, \dots, n.$$

¹⁷Такое естественное предположение обычно делают в подобных оценках битовой сложности вычислений, см., например, [10], [11].

Число $\mathbb{B}_n$ всех разбиений n -элементного множества на непустые подмножества называется *числом Белла*:

$$\mathbb{B}_n = \sum_{k=1}^n S_k^n.$$

Композиция преобразований

$$y_k = \sum_{m=0}^k |s_m^k| z_m, \quad z_k = \sum_{m=0}^k S_m^k x_m, \quad k = 0, \dots, n-1,$$

есть *преобразование Лаха* $y = L(x)$.

Его коэффициенты встречаются в тождествах [1], [2]:

$$(x)^n = \sum_{k=0}^n L_k^n(x)_k, \quad L_k^n = \binom{n}{k} (n-1)_{n-k} = \binom{n-1}{k-1} (n)_{n-k} = \binom{n-1}{k-1} \frac{n!}{k!},$$

$$L_k^n = (n-1+k) L_k^{n-1} + L_{k-1}^{n-1}, \quad n, k > 0, \quad L_0^0 = 1, \quad L_0^n = 0.$$

Для доказательства

$$(m)^n = \sum_{k=0}^n \binom{n-1}{k-1} \frac{n!}{k!} (m)_k$$

достаточно заметить, что число нестрого монотонно возрастающих отображений $\{1, \dots, n\} \rightarrow \{1, \dots, m\}$ с одной стороны равно $(m)^n/n!$ – числу сочетаний с повторениями из m элементов по n , а с другой стороны, равно $\sum_{k=0}^n a_k$, где

$$a_k = \binom{n-1}{k-1} \frac{1}{k!} (m)_k = \binom{n-1}{k-1} \binom{m}{k}$$

равно числу монотонных отображений, образ которых состоит ровно из k чисел.

Обратное преобразование к преобразованию Лаха отличается от прямого только знаками коэффициентов. Из указанных тождеств следует, что сложность вычисления всех чисел в треугольниках Стирлинга 1-го и 2-го рода и в треугольнике Лаха n -го порядка в базисе $B_{+,*}$ равна $\Theta(n^2)$. Для базиса B_+ получается оценка $O(n^2 \log n)$. Вычисление n -й строки треугольника Лаха в базисе $B_{+,*}$ сводится к вычислению n -й строки треугольника Паскаля и $O(n)$ дополнительным операциям, поэтому сложность этого вычисления равна $O(n \log n \log \log n)$. В силу тождеств

$$L_k^n = L_k^{n-1} \frac{(n-k+1)}{k(k-1)}, \quad L_1^n = n!$$

сложность n -й строки треугольника Лаха в базисе $B_{+,*}/$ равна $\Theta(n)$. Для базиса B_+ можно показать, используя [4], что эта сложность асимптотически не больше $(n^2/2) \ln n$.

ТЕОРЕМА 6. *Сложность вычисления n -й строки треугольника Стирлинга 2-го рода в базисе $B_{+,*}/$ есть $O(n \log n \log \log n)$. Сложность вычисления n -й строки треугольников Стирлинга 1-го и 2-го рода в базисе $B_{+,*}$ равна $O(n \log^2 n \log \log n)$. Для сложности преобразования Стирлинга 1-го рода (и монотонного преобразования Стирлинга) в базисах $B_{l,C}$, $B_{+,-}$, B_+ справедлива асимптотика $\Theta(n^2 \log_2 n)$.*

ДОКАЗАТЕЛЬСТВО. Для доказательства первого равенства используем теорему 2 и тождество

$$(-1)^k k! S_k^n = \sum_{m=0}^k \binom{k}{m} m^n (-1)^m.$$

Остается заметить, что сложность вычисления $1^n, 2^n, \dots, n^n$ в базисе $B_{+,*}$ равна $O(n \log n)$. Действительно, сложность вычисления прогрессии $1, 2, \dots, n$ в базисе B_+ равна $n - 1$, а сложность возведения каждого из ее членов в n -ю степень равна $l(n) = O(\log n)$ (в базисе B_* из одной операции умножения), как было объяснено во введении.

Докажем второе равенство. Для вычисления n -й строки треугольника Стирлинга 1-го рода в базисе $B_{+,*}$ согласно тождествам

$$(x)_n = \sum_{k=0}^n s_k^n x^k, \quad (x)^n = x(x+1) \cdots (x+n-1) = \sum_{k=0}^n |s_k^n| x^k,$$

достаточно вычислить коэффициенты многочлена

$$(x)^n = x(x+1) \cdots (x+n-1).$$

Для этого применим метод «деления пополам» (см. [10], [11]), в котором это вычисление рекуррентно сводится к вычислению коэффициентов многочленов $(x)^{\lfloor n/2 \rfloor}$, $(x + \lfloor n/2 \rfloor)^{\lfloor n/2 \rfloor}$ и их последующему умножению со сложностью $M(\lfloor n/2 \rfloor)$. Рекуррентная оценка сложности всего вычисления есть

$$L(n) \leq 2L\left(\left\lceil \frac{n}{2} \right\rceil\right) + M\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + O(n),$$

и из нее по индукции с помощью неравенства $2M(n/2) \leq M(n)$ следует, что $L(n) = \log n M(n) + O(n)$. Используя алгоритм Кантора–Калтофена, окончательно имеем оценку $O(n \log^2 n \log \log n)$.

Для треугольника Стирлинга 2-рода вычисление n -й строки сводится к вычислению коэффициентов разложения многочлена x^n в виде

$$x^n = \sum_{k=0}^n S_k^n(x)_k.$$

Это можно сделать так же, как в доказательстве теоремы 8.

Докажем третье утверждение. Верхняя оценка справедлива для базиса $B_{+,-}$, а в случае монотонного преобразования – и для базиса B_+ . Действительно, пусть, например,

$$y_k = \sum_{m=1}^k |s_m^k| x_m, \quad k = 1, \dots, n.$$

Так как $|s_k^n| = |s_{k-1}^{n-1}| + (n-1)|s_k^{n-1}|$, то

$$y_n = (n-1)y_{n-1} + y_{n-1,1}, \quad y_{n-1,1} = \sum_{m=2}^n |s_{m-1}^{n-1}| x_m,$$

$$y_{n-1} = (n-2)y_{n-2} + y_{n-2,1}, \quad y_{n-1,1} = (n-1)y_{n-2,1} + y_{n-2,2}, y_{n-2,2}$$

$$= \sum_{m=3}^{n-1} |s_{m-2}^{n-2}| x_m$$

и т.д. Вычисление на первом ярусе $y_n = (n-1)y_{n-1} + y_{n-1,1}$ требует асимптотически $\log_2 n$ операций сложения (для вычисления $(n-1)y_{n-1}$ применяем аддитивные цепочки, как было объяснено во введении), на втором ярусе вычисление

$$y_{n-1} = (n-2)y_{n-2} + y_{n-2,1}, \quad y_{n-1,1} = (n-1)y_{n-2,1} + y_{n-2,2}$$

требует асимптотически $2 \log_2 n$ операций сложения, и т.д. На произвольном k -м ярусе сложность вычисления асимптотически равна $k(1 + \log_2(n-k))$, и поэтому общая верхняя оценка сложности всего вычисления по порядку равна $n^2 \log n$. Более точная оценка асимптотически равна $(n^2/2) \log_2 n$.

Доказательство нижней оценки проводим подобно теореме 1.

Для этого достаточно вычислить определитель из модулей чисел Стирлинга 1-го рода

$$\det \begin{vmatrix} |s_1^n| & |s_2^n| & \dots & |s_n^n| \\ |s_1^{n+1}| & |s_2^{n+1}| & \dots & |s_n^{n+1}| \\ \vdots & \vdots & \ddots & \vdots \\ |s_1^{2n-1}| & |s_2^{2n-1}| & \dots & |s_n^{2n-1}| \end{vmatrix}.$$

Это можно сделать подобно тому, как вычислялся определитель в теореме 1. Вычитая из n -й строки $(n-1)$ -ю, умноженную на $2n-2$, получим равный ему

$$\det \begin{vmatrix} |s_1^n| & |s_2^n| & \dots & |s_n^n| \\ |s_1^{n+1}| & |s_2^{n+1}| & \dots & |s_n^{n+1}| \\ \vdots & \vdots & \ddots & \vdots \\ |s_1^{2n-2}| & |s_2^{2n-2}| & \dots & |s_n^{2n-2}| \\ |s_0^{2n-2}| & |s_1^{2n-2}| & \dots & |s_{n-1}^{2n-2}| \end{vmatrix}.$$

Повторяя эту процедуру последовательно для остальных строк, начиная с $(n-1)$ -й и заканчивая второй, а также учитывая, что $s_0^k = 0$, получаем

$$\det \begin{vmatrix} |s_1^n| & |s_2^n| & \dots & |s_n^n| \\ 0 & |s_1^n| & \dots & |s_{n-1}^n| \\ \vdots & \vdots & \ddots & \vdots \\ 0 & |s_1^{2n-2}| & \dots & |s_{n-1}^{2n-2}| \end{vmatrix}.$$

Повторяя тот же прием для минора порядка $n - 1$ в правом нижнем углу

$$\det \begin{vmatrix} |s_1^n| & \dots & |s_{n-1}^n| \\ \vdots & \ddots & \vdots \\ |s_1^{2n-2}| & \dots & |s_{n-1}^{2n-2}| \end{vmatrix},$$

получим определитель с нулевой $(2 \times (n - 2))$ -подматрицей в левом нижнем углу

$$\det \begin{vmatrix} |s_1^n| & |s_2^n| & |s_3^n| & \dots & |s_n^n| \\ 0 & |s_1^n| & |s_2^n| & \dots & |s_{n-1}^n| \\ 0 & 0 & |s_1^{n+1}| & \dots & |s_{n-2}^{n+1}| \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & |s_1^{2n-2}| & \dots & |s_{n-2}^{2n-2}| \end{vmatrix},$$

и т.д., пока не получим треугольный определитель

$$\det \begin{vmatrix} |s_1^n| & |s_2^n| & |s_3^n| & \dots & |s_n^n| \\ 0 & |s_1^n| & |s_2^n| & \dots & |s_{n-1}^n| \\ 0 & 0 & |s_1^n| & \dots & |s_{n-2}^n| \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & |s_1^n| \end{vmatrix},$$

который равен произведению диагональных элементов $\Delta_n = (s_1^n)^n = ((n - 1)!)^n$. Применяя лемму 1, имеем нижнюю оценку $\log \Delta_n = \Omega(n^2 \log n)$. Более точная нижняя оценка асимптотически равна $(n^2/4) \log_2 n$ в случае базиса $B_{l,1}$. Для преобразования

$$y_k = \sum_{m=1}^k s_m^k x_m, \quad k = 1, \dots, n,$$

доказательство аналогично.

ЗАМЕЧАНИЕ 4. Используя [4], можно показать, что в базисе B_+ сложность вычисления треугольника Стирлинга 2-го рода есть $O(n^2)$. В базисе B_+ сложность n -й строки треугольника Стирлинга 2-го рода тоже равна $O(n^2)$. То же самое верно и для треугольника из модулей чисел Стирлинга 1-го рода. Используя тождество $s_k^n = s_{k-1}^{n-1} - (n-1)s_k^{n-1}$, можно показать, что в базисе $B_{+,*}$ сложность преобразования Стирлинга 1-го рода n -го порядка равна $O(n^2)$. То же самое верно и для монотонного преобразования Стирлинга 1-го рода. Для преобразования Стирлинга 2-го рода n -го порядка в [19] показано, что сложность его вычисления в базисе $B_{+,*}/$ равна $O(n^{3/2}) \log^{3/2} n \log \log n$. Там же показано, что в том же базисе сложность последовательности чисел Белла $B_1, \dots, B_n$ есть $O(n \log n \log \log n)$.

ЗАМЕЧАНИЕ 5. Числа Стирлинга применяются в теории интерполяции [20]. В ней используются и аналогичные числам Стирлинга коэффициенты разложений

$$x^{[n]} = \sum_{k=0}^n t_{n,k} x^k, \quad x^n = \sum_{k=0}^n T_{n,k} x^{[k]},$$

$$x^{[n]} = x \left(x + \frac{n}{2} - 1 \right)_{n-1} = \left(x^2 - \left(\frac{n}{2} - 1 \right)^2 \right) x^{[n-2]},$$

которые в комбинаторике называются *центральными факториальными числами* (см. [21]). Для этих чисел справедливо тождество [21]

$$k!T(n, k) = \sum_{j=0}^k \binom{k}{j} (-1)^j \left(\frac{k}{2} - j \right)^n.$$

Используя данные тождества, можно доказать для этих чисел аналогии теоремы 6.

ТЕОРЕМА 7. Сложность вычисления преобразования Лаха порядка n в базисе B_l равна $O(n \log n)$, а в базисе $B_{+,*./}$ равна $O(n \log n \log \log n)$. Последняя оценка справедлива и для базиса $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$. Для сложности преобразования Лаха в базисе $B_{m,l}$ нижняя оценка равна $f(n)$. Для базиса $B_{l,C}$ справедлива асимптотика $\Theta(n^2 \log_2 n)$.

ДОКАЗАТЕЛЬСТВО. Преобразование Лаха

$$y_m = \sum_{k=1}^m L_k^m x_k, \quad L_k^m = \binom{m-1}{k-1} \frac{m!}{k!}, \quad m = 1, \dots, n,$$

можно записать в виде композиции «растяжения» $y_m = m!Y_m$, $m = 1, \dots, n$, биномиального отображения $Y_m = \sum_{k=1}^m \binom{m-1}{k-1} X_k$, $m = 1, \dots, n$, и «сжатия» $X_k = x_k/k!$, $k = 1, \dots, n$. Обратно, биномиальное преобразование можно записать в виде композиции «сжатия» $Y_m = y_m/m!$, $m = 1, \dots, n$, преобразования Лаха $y_m = \sum_{k=1}^m L_k^m x_k$, $m = 1, \dots, n$, и «растяжения» $x_k = k!X_k$, $k = 1, \dots, n$. Преобразования «сжатия» и «растяжения» в любом из базисов B_l , $B_{+,*./}$, $B_{m,l}$, $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$ вычисляются со сложностью $O(n)$, так как сложность вычисления системы факториалов $1!, 2!, \dots, n!$ в базисе $B_{+,*./}$ равна $O(n)$, как было показано в доказательстве теоремы 2 (для остальных базисов утверждение очевидно).

Если обозначить сложности преобразования Лаха и биномиального преобразования $L_1(n)$, $L_2(n)$, то отсюда вытекает равенство $|L_1(n) - L_2(n)| = O(n)$ для любого из базисов B_l , $B_{+,*./}$, $B_{m,l}$, $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$.

Из этого равенства и теорем 2, 3 следуют верхние оценки для этих базисов и нижняя оценка $f(n) - O(n) = \Omega(n \log_2 n)$ для базиса $B_{m,l}$.

Для базиса $B_{l,C}$ аналогичным образом получается верхняя оценка

$$L_1(n) \leq L_2(n) + O(n^2 \log_2 n) = O(n^2 \log_2 n)$$

(для оценки сложности вычисления «растяжения» применяются аддитивные цепочки и получается уже для базиса B_+ оценка

$$nl(n) = O(\log n!)n = O(n^2 \log n),$$

«сжатие» в базисе $B_{l,C}$ выполняется, очевидно, со сложностью n).

Оценку $f(n) - O(n)$ можно усилить до $f(n)$, если применить для доказательства тот же прием, что и для доказательства нижней оценки сложности биномиально-го преобразования в теореме 3. Доказательство нижней оценки указанного вида проходит для любого треугольного линейного преобразования, в матрице которого прилегающие к левому краю этой матрицы миноры отличны от нуля.

Для базиса $B_{l,C}$ можно получить нижнюю оценку $\Omega(n^2 \log_2 n)$ аналогично теореме 1. Действительно, в силу соотношения

$$L_k^m = \frac{m}{k} \frac{m-1}{k-1} L_{k-1}^{m-1}$$

определитель из чисел Лаха удовлетворяет тождеству

$$\det \begin{vmatrix} L_k^m & L_{k+1}^m & \cdots & L_{k+r}^m \\ L_k^{m+1} & L_{k+1}^{m+1} & \cdots & L_{k+r}^{m+1} \\ \vdots & \vdots & \ddots & \vdots \\ L_k^{m+r} & L_{k+1}^{m+r} & \cdots & L_{k+r}^{m+r} \end{vmatrix} = \frac{(m+r) \cdots (m+r-k+2)}{(r+1) \cdots (r+1)} \frac{(m+r-1) \cdots (m+r-k+1)}{(r+1) \cdots (r+1)} \times \det \begin{vmatrix} L_1^{m-k+1} & L_2^{m-k+1} & \cdots & L_{r+1}^{m-k+1} \\ L_1^{m-k+2} & L_2^{m-k+2} & \cdots & L_{r+1}^{m-k+2} \\ \vdots & \vdots & \ddots & \vdots \\ L_1^{m-k+r+1} & L_2^{m-k+r+1} & \cdots & L_{r+1}^{m-k+r+1} \end{vmatrix},$$

которое доказывается аналогично тождеству задачи 317 [6] (доказательство этого тождества см. теорему 1), а последний определитель в силу тождества

$$L_k^m = \binom{m-1}{k-1} \frac{m!}{k!}$$

вычисляется путем вынесения общих множителей из строк и столбцов (и применения определителя задачи 317 [6]):

$$\begin{aligned} \det \begin{vmatrix} L_1^{m-k+1} & L_2^{m-k+1} & \cdots & L_{r+1}^{m-k+1} \\ L_1^{m-k+2} & L_2^{m-k+2} & \cdots & L_{r+1}^{m-k+2} \\ \vdots & \vdots & \ddots & \vdots \\ L_1^{m-k+r+1} & L_2^{m-k+r+1} & \cdots & L_{r+1}^{m-k+r+1} \end{vmatrix} \\ = \frac{(m-k+1)! \cdots (m-k+r+1)!}{1! \cdots (r+1)!} \det \begin{vmatrix} \binom{m-k}{0} & \binom{m-k+1}{1} & \cdots & \binom{m-k+1}{r} \\ \binom{m-k+2}{0} & \binom{m-k+2}{1} & \cdots & \binom{m-k+2}{r} \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m-k+r+1}{0} & \binom{m-k+r+1}{1} & \cdots & \binom{m-k+r+1}{r} \end{vmatrix} \\ = \frac{(m-k+1)! \cdots (m-k+r+1)!}{1! \cdots (r+1)!}. \end{aligned}$$

Продолжая далее рассуждения, аналогичные доказательству теоремы 1, выбираем $m = 2r$, $k = r = \lfloor n/3 \rfloor$ и оцениваем снизу указанный определитель. Согласно приведенным выше формулам он равен произведению трех дробей

$$\frac{\binom{m+r}{r+1} \cdots \binom{m+r-k+2}{r+1}}{\binom{k+r}{r+1} \cdots \binom{r+2}{r+1}} \frac{\binom{m+r-1}{r+1} \cdots \binom{m+r-k+1}{r+1}}{\binom{k+r-1}{r+1} \cdots \binom{r+1}{r+1}} \frac{(m-k+1)! \cdots (m-k+r+1)!}{1! \cdots (r+1)!}.$$

Первые две дроби, очевидно, больше единицы в силу неравенства

$$\binom{m+1}{k+1} = \binom{m}{k+1} + \binom{m}{k} > \binom{m}{k},$$

из которого следует, что $\binom{m+1}{k+1} / \binom{m}{k} > 1$ при $m > k$. Третья дробь, очевидно, равна

$$\frac{(r+1)! \cdots (2r+1)!}{1!2! \cdots (r+1)!} = \frac{(r+2)! \cdots (2r+1)!}{1!2! \cdots r!}.$$

Очевидно, что

$$\frac{(r+i+1)!}{(i+1)!} = \frac{(r+i)!}{(i)!} \frac{r+i+1}{i+1} > \frac{(r+i)!}{(i)!},$$

поэтому

$$(2r+1)! \frac{(r+2)! \cdots (2r)!}{2! \cdots r!} > (2r+1)! ((r+1)!)^{r-1} > (2r+1)! \left(\frac{r+1}{3} \right)^{(r+1)(r-1)} > \left(\frac{r}{3} \right)^{r^2}$$

в силу элементарного неравенства $m! > (m/3)^m$. Поэтому рассматриваемый определитель больше $(r/3)^{r^2}$, а его двоичный логарифм по порядку не меньше $r^2 \log r = \Theta(n^2 \log n)$.

7. Сложность преобразования Гаусса. Аналогом биномиальных коэффициентов являются *коэффициенты Гаусса*

$$\binom{n}{k}_q = \frac{q^n - 1}{q^k - 1} \frac{q^{n-1} - 1}{q^{k-1} - 1} \cdots \frac{q^{n-k+1} - 1}{q - 1}.$$

Для них справедливы следующие тождества [2], аналогичные тождествам для биномиальных коэффициентов (последние получаются из коэффициентов Гаусса $q \rightarrow 1$):

$$\begin{aligned} \binom{n}{k}_q &= \frac{q^n - 1}{q^k - 1} \binom{n-1}{k-1}_q = \frac{q^{n-k} - 1}{q^k - 1} \binom{n}{k-1}_q, & \binom{n}{k}_q &= \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q, \\ x^n &= \sum_{k=0}^n \binom{n}{k}_q g_{k,q}(x), & g_{k,q}(x) &= (x-1)(x-q) \cdots (x-q^{k-1}) \quad (\text{тождество Коши}). \end{aligned}$$

Суммы коэффициентов в n -й строке треугольника Гаусса называются *числами Галуа*:

$$G_n(q) = \sum_{k=0}^n \binom{n}{k}_q.$$

При $q = p^m$, где p – простое число, коэффициент $\binom{n}{k}_q$ интерпретируется как число k -мерных подпространств в n -мерном пространстве над полем Галуа $GF(q)$. Число

$G_n(q)$ интерпретируется как число всех подпространств в этом пространстве. Есть и другие интерпретации упомянутых чисел. Тожества для q -аналогов классических комбинаторных чисел в последнее время иногда называют квантовой комбинаторикой. Для чисел Галуа известно тождество

$$G_{n+1}(q) = 2G_n(q) + (q^n - 1)G_{n-1}(q),$$

из которого следует, что сложность вычисления в базисе $B_{+,*}$ всех чисел Галуа $G_1, \dots, G_n$ равна $O(n + \log q)$.

Можно рассмотреть преобразование Гаусса и обратное к нему

$$y_k = \sum_{m=0}^k \binom{k}{m}_q x_m, \quad x_k = \sum_{m=0}^k (-1)^{k-m} q^{\binom{k-m}{2}} \binom{k}{m}_q y_m, \quad k = 0, \dots, n-1.$$

Из указанных тождеств следует, что в базисе $B_{+,*}/$ при фиксированном q сложность вычисления n -й строки треугольника Гаусса равна $\Theta(n)$, сложность вычисления всего треугольника Гаусса порядка n в базисе $B_{+,*}$ равна $\Theta(n^2)$, а в базисе B_{+} оценивается как $O(n^3)$. Используя результат [4], легко показать, что сложность вычисления n -й строки треугольника Гаусса оценивается как $O(n^3/\log n)$.

ТЕОРЕМА 8. *Сложность вычисления q -преобразования Гаусса порядка n и обратного к нему в базисе B_l равна $O(n \log n)$, в базисе $B_{l,C}$ при нечетном q равна $\Theta(n^3 \log q)$, а в базисе $B_{+,*}/ = \{x + y, xy, 1/x\}$ равна $O(n \log n \log \log n + \log q)$. Такая же оценка справедлива и для базиса $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$. Для базиса $B_{m,l}$ сложность q -преобразования Гаусса по порядку не меньше $n \log_2 n$. В базисе $B_{+,*}$ сложность вычисления n -й строки q -треугольника Гаусса равна $O(n \log^2 n \log n + \log q)$.*

ДОКАЗАТЕЛЬСТВО. Первое утверждение доказывается аналогично теореме 2. Достаточно представить преобразования Гаусса порядка n в виде свертки двух векторов:

$$\frac{y_k}{(q^k - 1) \cdots (q - 1)} = \sum_{m=0}^k \frac{1}{(q^{k-m} - 1) \cdots (q - 1)} \frac{x_m}{(q^m - 1) \cdots (q - 1)}, \quad k = 0, \dots, n-1.$$

Обратное преобразование представляется в виде свертки следующим образом:

$$\frac{x_k}{(q^k - 1) \cdots (q - 1)} = \sum_{m=0}^k \frac{(-1)^{k-m} q^{\binom{k-m}{2}}}{(q^{k-m} - 1) \cdots (q - 1)} \frac{y_m}{(q^m - 1) \cdots (q - 1)}, \quad k = 0, \dots, n-1.$$

Оценка в базисах $B_{+,*}/$ и $\{x \pm y\} \cup \{nx : n \in \mathbb{N}\} \cup \{x/n : n \in \mathbb{N}\}$ также доказывается аналогично теореме 2.

Доказательство нижней оценки в случае базиса $B_{l,C}$ аналогично теореме 1. Равенство определителей

$$\det \begin{vmatrix} \binom{m}{k}_q & \binom{m}{k+1}_q & \cdots & \binom{m}{k+n}_q \\ \binom{m+1}{k}_q & \binom{m+1}{k+1}_q & \cdots & \binom{m+1}{k+n}_q \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n}{k}_q & \binom{m+n}{k+1}_q & \cdots & \binom{m+n}{k+n}_q \end{vmatrix}$$

$$= \frac{\binom{m+n}{n+1}_q \binom{m+n-1}{n+1}_q \cdots \binom{m+n-k+1}{n+1}_q}{\binom{k+n}{n+1}_q \binom{k+n-1}{n+1}_q \cdots \binom{n+1}{n+1}_q} \det \begin{vmatrix} \binom{m-k}{0}_q & \binom{m-k}{1}_q & \cdots & \binom{m-k}{n}_q \\ \binom{m+1-k}{0}_q & \binom{m+1-k}{1}_q & \cdots & \binom{m+1-k}{n}_q \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n-k}{0}_q & \binom{m+n-k}{1}_q & \cdots & \binom{m+n-k}{n}_q \end{vmatrix}$$

доказывается, как и в теореме 1, аналогично задаче 317 [6]. Дальше непосредственная аналогия кончается, но можно заметить, что второй определитель по абсолютной величине не меньше единицы, так как при $m = 2^k$, $n = 2^l - 1$, $l \leq k$, он ненулевой. Действительно, по модулю два он равен единице, потому что тождество

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + q^k \binom{n-1}{k}_q$$

по модулю два превращается при нечетном q в тождество Паскаля

$$\binom{n}{k}_q = \binom{n-1}{k-1}_q + \binom{n-1}{k}_q,$$

значит, аналогично доказательству теоремы 1 можно проверить, что определитель

$$\det \begin{vmatrix} \binom{m-k}{0}_q & \binom{m-k}{1}_q & \cdots & \binom{m-k}{n}_q \\ \binom{m+1-k}{0}_q & \binom{m+1-k}{1}_q & \cdots & \binom{m+1-k}{n}_q \\ \vdots & \vdots & \ddots & \vdots \\ \binom{m+n-k}{0}_q & \binom{m+n-k}{1}_q & \cdots & \binom{m+n-k}{n}_q \end{vmatrix} = 1 \pmod{2}.$$

Применяя далее рассуждение из доказательства теоремы 1 к подобному же минору¹⁸

$$\begin{vmatrix} \binom{2r}{r+1}_q & \binom{2r}{r+2}_q & \cdots & \binom{2r}{2r}_q \\ \binom{2r+1}{r+1}_q & \binom{2r+1}{r+2}_q & \cdots & \binom{2r+1}{2r}_q \\ \vdots & \vdots & \ddots & \vdots \\ \binom{3r-1}{r+1}_q & \binom{3r-1}{r+2}_q & \cdots & \binom{3r-1}{2r}_q \end{vmatrix},$$

получим при $r = 2^k \leq \lfloor n/3 \rfloor < 2^{k+1}$ нижнюю оценку, равную по порядку

$$\log \left(\frac{\binom{3r-1}{r}_q}{\binom{2r}{r}_q} \cdots \frac{\binom{2r}{r}_q}{\binom{r+1}{r}_q} \right) = \Theta(\log(((q^r)^r)^r)) = \Theta(n^3 \log q).$$

Для обратного преобразования доказательство аналогично. Заметим, что после замен переменных $x_k = X_k(-1)^k$, $y_m = Y_m(-1)^m$ обратное преобразование имеет вид

$$x_k = \sum_{m=0}^k q^{\binom{k-m}{2}} \binom{k}{m}_q y_m, \quad k = 0, \dots, n-1,$$

сложность обоих вариантов преобразования отличается на $O(n)$, поэтому при доказательстве нижней оценки можно считать, что коэффициенты обратного преобразо-

¹⁸Или пользуясь фрактальной структурой матрицы Серпинского.

вания положительны и равны $q^{\binom{k-m}{2}} \binom{k}{m}_q$. Эти коэффициенты удовлетворяют тому же тождеству

$$c_{k,m} = \frac{q^k - 1}{q^m - 1} c_{k-1,m-1},$$

что и коэффициенты $\binom{k}{m}_q$ прямого преобразования, поэтому нижняя оценка указанного выше минора будет такой же, что и в случае прямого преобразования (так как при нечетном q коэффициенты обоих преобразований по модулю два совпадают).

Для доказательства верхней оценки в базисе $B_{l,1}$ представим

$$y_k = \sum_{m=0}^k \binom{k}{m}_q x_m = q^{n^2} \sum_{m=0}^k q^{-n^2} \binom{k}{m}_q x_m, \quad k = 1, \dots, n,$$

и заметим, что коэффициенты $q^{-n^2} \binom{k}{m}_q \in (0, 1)$, $k = 1, \dots, n$, а так как в базис входят умножения на любой скаляр по модулю меньший 1, то все суммы

$$\sum_{m=0}^k q^{-n^2} \binom{k}{m}_q x_m, \quad k = 1, \dots, n,$$

вычисляются со сложностью $n^2 - n$, поэтому y_k , $k = 1, \dots, n$, можно вычислить со сложностью $O(n^3 \log q)$. Для обратного преобразования Гаусса доказательство аналогично.

Нижняя оценка в базисе $B_{m,l}$ доказывается аналогично теореме 3 и равна введенной перед ней функции $f(n)$. Для доказательства достаточно заметить, что все миноры, равные 1 по модулю два в биномиальной матрице, будут равны 1 по модулю два и в матрице преобразования Гаусса.

Для доказательства последнего утверждения теоремы понадобится следующая лемма, которой мы предположим определение одного семейства многочленов. Пусть $f_n(x) = (x + a_1) \cdots (x + a_n)$ – последовательность многочленов, $f_0(x) = 1$. Для каждого $i < \log_2 n$ определим последовательность многочленов

$$\begin{aligned} f_{i,0}(x) &= \prod_{j=1}^{2^i} (x + a_j), & f_{i,1}(x) &= \prod_{j=1}^{2^i} (x + a_{2^i+j}), \\ & \dots, & f_{i,\lfloor n/2^i \rfloor}(x) &= \prod_{j=1}^{n-2^i \lfloor n/2^i \rfloor} (x + a_{2^i \lfloor n/2^i \rfloor + j}) \end{aligned}$$

(если n кратно 2^i , то последний многочлен равен 1). Очевидно, что

$$f_n = \prod_{j=1}^n f_{0,j} = \prod_{j=1}^{\lfloor n/2 \rfloor + 1} f_{1,j} = \prod_{j=1}^{\lfloor n/4 \rfloor + 1} f_{2,j}$$

и так далее.

ЛЕММА 2 (О коэффициентах в интерполяционной формуле Ньютона). Пусть

$$p(x) = b_0 + b_1x + \dots + b_nx^n$$

– многочлен u

$$p(x) = c_0 f_0(x) + \dots + c_n f_n(x)$$

– его разложение по линейно независимой системе определенных выше многочленов $\{f_0, \dots, f_n\}$. Для вычисления его коэффициентов c_k , $k = 0, \dots, n$, можно применить следующий рекуррентный алгоритм, в котором для простоты обозначений полагаем, что $n = 2^k$. Разделим $p(x)$ на $f_{n/2}(x)$ с остатком:

$$p(x) = p_0(x) + p_1(x)f_{n/2}(x), \quad \deg p_0 < \frac{n}{2} = 2^{k-1}, \quad \deg p_1 \leq 2^{k-1}.$$

Тогда коэффициенты c_i , $i < n/2 = 2^{k-1}$, можно найти, рекурсивно применив описываемый алгоритм к многочлену $p_0(x)$ и системе многочленов $\{f_0, \dots, f_{n/2-1}\}$, а остальные коэффициенты c_j , $j = n/2, \dots, n$, найти, рекурсивно применив описываемый алгоритм к многочлену $p_1(x)$ и системе

$$\{h_0 = 1, h_1 = x + a_{n/2+1}, \dots, h_{n/2} = (x + a_{n/2+1}) \dots (x + a_n)\}.$$

В процессе рекурсивного развертывания алгоритма вычисляются коэффициенты многочленов $f_{i,0}(x), \dots, f_{i,n/2^i-1}(x)$ и выполняются для каждого многочлена $f_{i,2j}$, $j = 0, \dots, n/2^{i+1} - 1$, деления с остатком на эти многочлены некоторых многочленов степени $2^{i+1} - 1$.

ДОКАЗАТЕЛЬСТВО. Лемма доказывается по индукции. Для обоснования шага индукции достаточно заметить, что если

$$p_0 = c_0 f_0 + \dots + c_{n/2-1} f_{n/2-1}, \quad p_1 = c_{n/2} h_0 + \dots + c_n h_{n/2},$$

то

$$\begin{aligned} p &= p_0 + p_1 f_{n/2} = c_0 f_0 + \dots + c_{n/2-1} f_{n/2-1} + f_{n/2}(c_{n/2} h_0 + \dots + c_n h_{n/2}) \\ &= c_0 f_0 + \dots + c_{n/2-1} f_{n/2-1} + c_{n/2} f_{n/2} h_0 + \dots + c_n f_{n/2} h_{n/2} \\ &= c_0 f_0 + \dots + c_n f_n. \end{aligned}$$

Оценим сложность вычислений в базисе $B_{+,*}$, выполняемых в приведенном алгоритме в случае $a_i = q^{i-1}$. Сложность вычисления констант a_i не больше $n + \log q$. Для вычисления каждого $f_{i,j}$ нужно перемножить $f_{i-1,2j}$ и $f_{i-1,2j+1}$. Это можно сделать со сложностью $M(2^{i-1})$. Полная сложность вычисления всех этих многочленов оценивается как

$$2^{k-1}M(1) + 2^{k-2}M(2) + \dots + 2M(2^{k-1}) \leq kM(2^k) = O(\log nM(n)).$$

Как известно [10], [11], [13] деление многочлена степени $2n - 1$ на многочлен степени n с остатком можно выполнить в базисе $B_{+,*}$ со сложностью $D(n) = O(M(n))$. Поэтому для сложности вычислений по указанному алгоритму можно получить следующую рекуррентную оценку: $L(n) \leq 2L(n/2) + D(n/2)$, из которой по индукции следует при $n = 2^k$ оценка

$$L(n) \leq D(2^{k-1}) + 2D(2^{k-2}) + \dots + 2^{k-1}D(1) = O(\log nM(n)).$$

В общем случае оценка остается такой же, так как при $2^{k-1} < n < 2^k$ справедливо неравенство

$$L(n) \leq L(2^k) = O(kM(2^k)) = O((1 + \log n)M(2n)) = O(\log nM(n)).$$

Используя указанное выше тождество Коши и предыдущую оценку вместе с алгоритмом Кантора–Калтофена, получаем, что сложность вычисления в базисе $B_{+,*}$ всех коэффициентов $\binom{n}{k}_q$, $k = 0, \dots, n$, равна

$$O(\log n M(n)) = O(n \log^2 n \log \log n + \log q).$$

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

- [1] Дж. Риордан, *Введение в комбинаторный анализ*, ИЛ, М., 1963.
- [2] Я. Гульден, Д. Джексон, *Перечислительная комбинаторика*, Наука, М., 1990.
- [3] Д. Кнут, *Искусство программирования*. Т. 2. *Получисленные алгоритмы*, Мир, М., 2000.
- [4] С. Б. Гашков, В. В. Кочергин, “Аддитивные цепочки векторов, вентильные схемы и сложность вычисления степеней”, *Методы дискрет. анализа*, **52** (1992), 22–40.
- [5] J. Morgenstern, “Note on lower bound of the linear complexity of the fast Fourier transform”, *J. Assoc. Comput. Mach.*, **20:2** (1973), 305–306.
- [6] Д. К. Фаддеев, И. С. Соминский, *Задачи по высшей алгебре*, Лань, СПб., 1999.
- [7] Е. Ю. Смирнов, *Диаграммы Юнга, плоские разбиения и знакопередающиеся матрицы*, МЦНМО, М., 2014.
- [8] D. G. Cantor, E. Kaltofen, “On fast multiplication of polynomials over arbitrary algebras”, *Acta Inform.*, **28:7** (1991), 693–701.
- [9] A. Schönhage, “Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2”, *Acta Inform.*, **7:4** (1977), 395–398.
- [10] J. von zur Gathen, J. Gerhard, *Modern Computer Algebra*, Cambridge Univ. Press, Cambridge, 1999.
- [11] А. Ахо, Дж. Хопкрофт, Дж. Ульман, *Построение и анализ вычислительных алгоритмов*, Мир, М., 1979.
- [12] J. W. Cooley, J. W. Tukey, “An algorithm for the machine calculation of complex Fourier series”, *Math. Comp.*, **19** (1965), 297–301.
- [13] С. Б. Гашков, В. Н. Чубариков, *Арифметика. Алгоритмы. Сложность вычислений*, Высшая школа, М., 2000.
- [14] J. Boyar, M. C. Find, *Cancellation-Free Circuits: An Approach for Proving Superlinear Lower Bounds for Linear Boolean Operators*, arXiv:1207.5321.
- [15] Д. Ю. Григорьев, “Нижние оценки в алгебраической сложности вычислений”, *Теория сложности вычислений. I*, Зап. научн. сем. ЛОМИ, **118**, Изд-во «Наука», Ленинград. отд., Л., 1982, 25–82.
- [16] D. Yu. Grigor’ev, “Additive complexity in directed computations”, *Theoret. Comput. Sci.*, **19:1** (1982), 39–67.
- [17] А. В. Чашкин, “О сложности булевых матриц, графов и соответствующих им булевых функций”, *Дискрет. матем.*, **6:2** (1994), 43–73.
- [18] N. Alon, M. Karchmer, A. Wigderson, “Linear circuits over GF(2)”, *SIAM J. Comput.*, **19:6** (1990), 1064–1067.
- [19] С. Б. Гашков, И. Б. Гашков, “О сложности вычисления дифференциалов и градиентов”, *Дискрет. матем.*, **17:3** (2005), 45–67.
- [20] И. П. Стефенсен, *Теория интерполяции*, ОНТИ, М., 1935.
- [21] Дж. Риордан, *Комбинаторные тождества*, Наука, М., 1982.

С. Б. Гашков

Московский государственный университет

им. М. В. Ломоносова

E-mail: sbgashkov@gmail.com

Поступило

01.09.2012

Исправленный вариант

05.09.2014