# Тема 1. Аддитивные цепочки

*С. Б. Гашков, И. С. Сергеев*

Рассмотрим следующую задачу. Пусть задано число $x$, которое требуется возвести в некоторую натуральную степень $n$. Как обойтись при этом наименьшим числом умножений? Первым шагом очевидно станет получение $x^2$. Далее, мы можем получить $x^3$, перемножив $x$ и $x^2$, либо $x^4$ возведением в квадрат $x^2$. И т.д. В итоге выписывается последовательность

$$x,\, x^{a_1},\, x^{a_2}, \ldots,\, x^n,$$

из степеней $x$, которая оканчивается на $x^n$. Можно не переписывать все время $x$, и оставить в записи только показатели степени — они образуют аддитивную цепочку.

*Аддитивной цепочкой* для числа $n$ называется любая начинающаяся с 1 последовательность натуральных чисел $a_0 = 1,\ a_1,\ \ldots,\ a_m = n$, в которой каждое число является суммой каких-то двух предыдущих чисел (возможно совпадающих), т.е. для всех $i \geq 1$ выполнено $a_i = a_j + a_k,\ j,k < i$. Под *длиной* цепочки $a_0,\ a_1,\ \ldots,\ a_m$ понимается число $m$. Через $l(n)$ обозначим длину *кратчайшей* аддитивной цепочки для $n$.

Таким образом, возведение в степень интерпретируется как построение аддитивной цепочки для показателя степени. *Удвоения* в аддитивной цепочке соответствуют возведениям в квадрат, а прочие сложения — умножениям.

Аддитивная цепочка называется *линейной*, если каждый ее элемент равен сумме предыдущего элемента и какого-то еще, т.е. для всех $i \geq 1$ выполнено $a_i = a_{i-1} + a_j,\ j < i$. Длина кратчайшей линейной цепочки обозначается через $l^*(n)$.

Очевидно следующее соотношение:

$$l^*(n) \geq l(n) \geq \lambda(n),$$

где $\lambda(n) = \lfloor \log_2 n \rfloor$, поскольку $2^k$ — это максимальное число, которое можно получить при помощи аддитивной цепочки длины $k$.

# 1 Бинарный метод

Пусть $n = [n_{k-1}, n_{k-2}, \ldots, n_0]$. Используя схему Горнера, можно записать формулу

$$n = (\ldots(2n_{k-1} + n_{k-2})2 + \ldots + n_1)2 + n_0,$$

по которой выписывается универсальная аддитивная цепочка для числа $n$ (вычисления производятся слева направо)

$$a_0 = n_{k-1} = 1,\ a_1 = 2a_0 = 2,\ a_2 = a_1 + n_{k-2},\ a_3 = 2a_2,\ \ldots\ ,$$
$$a_{2k-4} = a_{2k-5} + n_1,\ a_{2k-3} = 2a_{2k-4},\ a_{2k-2} = a_{2k-3} + n_0.$$

Удалив из построенной цепочки повторяющиеся элементы, получим окончательно цепочку, соответствующую так называемому бинарному (перебирающему разряды слева направо) алгоритму.

Например, для числа $n = 19 = [10011]$ выписывается цепочка

$$1,\ 2,\ 2,\ 4,\ 4,\ 8,\ 9,\ 18,\ 19.$$

Удаляя из нее повторяющиеся элементы, получаем цепочку

$$1,\ 2,\ 4,\ 8,\ 9,\ 18,\ 19.$$

Чтобы сразу построить цепочку без повторений, можно воспользоваться следующим правилом. Удалим из двоичной записи числа $n$ единицу в старшем разряде, перед остальными единицами вставим двойки, а все нули заменим на двойки. В итоге получится слово из символов 1 и 2, в котором единицы означают прибавление 1, а двойки — удвоение. Например, для числа $n = 19 = [10011]$ получается слово 222121, которому соответствует приведенная выше аддитивная цепочка.

Пусть $\nu(n)$ обозначает вес числа $n$, т.е. количество единиц в двоичной записи.

**Лемма 1.** *Длина бинарной аддитивной цепочки для числа $n$ равна*

$$\lambda(n) + \nu(n) - 1.$$

*Доказательство.* Заметим, что в описанном выше бинарном методе используется $k-1 = \lambda(n)$ удвоений и столько прибавлений единицы, сколько ненулевых разрядов в двоичной записи числа $n$, не считая старшего, а именно $\nu(n) - 1$. Лемма доказана.

Следовательно, доказано

$$l(n) \leq \lambda(n) + \nu(n) - 1.$$

Бинарный метод не является оптимальным, что видно из следующего примера. Пусть $n = s\,t$, и построены аддитивные цепочки для $s$ и $t$

$$1,\ a_1,\ \ldots,\ a_i = s; \qquad 1,\ b_1,\ \ldots,\ b_j = t.$$

Тогда для $n$ выписывается следующая аддитивная цепочка

$$1,\ a_1,\ \ldots,\ a_i = s,\ sb_1,\ sb_2, \ldots,\ sb_j = n.$$

Длина ее равна сумме длин аддитивных цепочек для сомножителей, т.е.

$$l(st) \leq l(s) + l(t).$$

Если для вычисления $s$ и $t$ используются бинарные цепочки, то длина цепочки для $n$ составит $\lambda(s) + \lambda(t) + \nu(s) + \nu(t) - 2$. При $n = 15$ этим способом впервые улучшается результат бинарного метода (с 6 до 5).

Можно однако доказать, что при $n \leq 14$ и вообще для всех $n$ с весом $\nu(n) \leq 3$ бинарный метод все же дает кратчайшую цепочку.

## 2 Асимптотически наилучший метод

Следующий метод еще называется $2^k$-арным методом Брауэра.

**Теорема 1** (Брауэр, 1939)**.**

$$l(n) \leq \lambda(n) + (1 + o(1))\frac{\lambda(n)}{\lambda(\lambda(n))}.$$

*Доказательство.* Пусть $k \in \mathbb{N}$, $t = \lfloor \log_{2^k} n \rfloor$. Запишем число $n$ в системе счисления с основанием $2^k$:

$$n = n_{t-1}2^{k(t-1)} + n_{t-2}2^{k(t-2)} + \ldots + n_0.$$

Перепишем, используя схему Горнера:

$$n = (\ldots(2^k n_{t-1} + n_{t-2})2^k + \ldots)2^k + n_0.$$

Рассмотрим следующую аддитивную цепочку:

$$1,\ 2,\ 3,\ \ldots,\ 2^k-1,\ 2n_{t-1},\ 4n_{t-1},\ \ldots,\ 2^k n_{t-1},\ 2^k n_{t-1}+n_{t-2},\ \ldots\ldots,\ n.$$

Эта цепочка имеет длину $2^k - 2 + (k+1)(t-1)$. При $k = \lambda(\lambda(n)) - 2\lambda(\lambda(\lambda(n)))$ (полагая, что $n \geq 4$) имеем:

$$2^k - 2 + (k+1)(t-1) \leq c_1 \frac{\lambda(n)}{\lambda^2(\lambda(n))} + (k+1)\left(\frac{\lambda(n)}{k} + c_2\right) \leq$$
$$\leq \lambda(n) + \frac{\lambda(n)}{k} + c_3 \frac{\lambda(n)}{\lambda^2(\lambda(n))} = \lambda(n) + (1+o(1))\frac{\lambda(n)}{\lambda(\lambda(n))}.$$

Теорема доказана.

Метод Брауэра является асимптотически наилучшим в силу доказанной П. Эрдошем нижней оценки длины аддитивной цепочки

$$l(n) \geq \lambda(n) + (1 - o(1))\frac{\lambda(n)}{\lambda(\lambda(n))},$$

справедливой для почти всех $n$ при $n \to \infty$.

В отношении абсолютной нижней границы длины аддитивной цепочки известна гипотеза

$$l(n) \geq \lambda(n) + \lceil \log_2 \nu(n) \rceil.$$

В 1975 г. А. Шёнхаге доказал лишь чуть-чуть более слабую оценку

$$l(n) \geq \log_2 n + \log_2 \nu(n) - 2,13.$$

# 3 Аддитивные цепочки для чисел вида $2^n - 1$

Представляет интерес построение аддитивных цепочек для чисел специального вида. Известная недоказанная гипотеза Шольца—Брауэра гласит:

$$l(2^n - 1) \leq n - 1 + l(n).$$

Задача построения коротких аддитивных цепочек для чисел вида $2^n - 1$ является актуальной в наше время — к ней, например, сводится задача инвертирования в конечном поле характеристики 2. Гипотеза Брауэра сравнительно просто доказывается для линейных цепочек.

**Теорема 2** (Брауэр, 1939)**.**

$$l^*(2^n - 1) \le n - 1 + l^*(n).$$

*Доказательство.* По произвольной линейной цепочке

$$1,\ a_1,\ \ldots,\ a_m = n$$

строится аддитивная цепочка для $2^n - 1$ следующим образом. Выписывается последовательность

$$1 = 2^1 - 1,\ 2^{a_1} - 1,\ \ldots,\ 2^{a_m} - 1 = 2^n - 1,$$

затем в промежутки между числами вставляются последовательности удвоений. Так, между соседними числами $2^{a_k} - 1$ и $2^{a_{k+1}} - 1$, где $a_{k+1} = a_k + a_j$, помещается последовательность из $a_j$ элементов

$$2(2^{a_k} - 1),\ 2^2(2^{a_k} - 1),\ \ldots,\ 2^{a_{k+1} - a_k}(2^{a_k} - 1) = 2^{a_{k+1}} - 2^{a_j}.$$

Поскольку $2^{a_{k+1}} - 1 = (2^{a_{k+1}} - 2^{a_j}) + (2^{a_j} - 1)$, то итоговая последовательность является линейной аддитивной цепочкой.

Покажем, что суммарное количество элементов во всех вставках составляет $n - 1$. Для этого докажем по индукции, что число вставленных перед $2^{a_i} - 1$ элементов равно $a_i - 1$.

Для $i = 0$ проверяемое утверждение очевидно выполнено: перед элементом $2^{a_0} - 1 = 1$ мы ничего не вставляем. Предположим, что оно выполнено для всех $i \le k$ и пусть $a_{k+1} = a_k + a_j$. Тогда число вставленных перед $2^{a_k} - 1$ элементов равно $a_k - 1$. Складывая это число с числом $a_j$ вставляемых между $2^{a_k} - 1$ и $2^{a_{k+1}} - 1$ элементов, получаем, что всего $a_k - 1 + a_j = a_{k+1} - 1$ элементов вставляется перед числом $2^{a_{k+1}} - 1$.

Таким образом, построенная цепочка для $2^n - 1$ имеет длину $n + m - 1$. Выбирая $m = l^*(n)$, приходим к утверждению теоремы.

Анализируя доказательство, можно заметить, что оно проходит для цепочек более общего вида, чем линейные. Такие цепочки называются цепочками Ханзена.

Известно, что существуют $n$ такие, что $l(n) < l^*(n)$ (наименьшее такое число — 12509), т.е. не всегда удается найти среди кратчайших цепочек линейную. Этот факт доказан Ханзеном, причем в доказательстве используются цепочки Ханзена. В 2005 г. было обнаружено число $n = 5784689$, для которого среди кратчайших цепочек нет даже цепочки Ханзена.

## 4 Векторные аддитивные цепочки

Рассмотрим два многомерных обобщения задачи о возведении в степень за минимальное число умножений.

1) Требуется вычислить $x_1^{n_1} x_2^{n_2} \cdot \ldots \cdot x_k^{n_k}$, исходя из $x_1, \ldots, x_k$.

2) Требуется вычислить $x^{n_1}, x^{n_2}, \ldots, x^{n_k}$, зная $x$.

(В обоих случаях предполагается, что все $n_i \neq 0$.)

Для работы с первой задачей вводится концепция *векторной $k$-мерной аддитивной цепочки*, состоящей из векторов, в которых $i$-я компонента соответствует показателю степени при $x_i$. Такая цепочка определяется по аналогии с обычной: она начинается с $k$ базисных единичных векторов, а каждый следующий вектор равен сумме каких-либо двух предыдущих. Длина кратчайшей цепочки для вектора $(n_1, \ldots, n_k)$ обозначается через $l([n_1, \ldots, n_k])$, базисные вектора при подсчете длины не учитываются.

**Теорема 3** (Страус)**.** *Пусть* $n = \max n_i$. *Тогда*

$$l([n_1, \ldots, n_k]) \leq \lambda(n) + (1 + o(1)) \frac{k\lambda(n)}{\lambda(\lambda(n))}.$$

*Доказательство.* Для доказательства воспользуемся обобщением $2^k$-арного метода на многомерный случай.

Обозначим $\vec{n} = (n_1, \ldots, n_k)$, и запишем этот вектор в системе счисления с основанием $2^s$:

$$\vec{n} = \vec{d}_{t-1} 2^{s(t-1)} + \vec{d}_{t-2} 2^{s(t-2)} + \ldots + \vec{d}_0 = (\ldots(2^s \vec{d}_{t-1} + \vec{d}_{t-2})2^s + \ldots)2^s + \vec{d}_0,$$

где $t = \lfloor \log_{2^s} n \rfloor$, а компоненты всех векторов $\vec{d}_i$ не превосходят $2^s - 1$.

Аддитивная цепочка для $\vec{n}$ начинается с выписывания всевозможных векторов $d\vec{e}_i$, где $\vec{e}_i$ — базисные вектора, а $2 \leq d \leq 2^s - 1$ (всего $k(2^s - 2)$ штук). Затем из них образуются вектора $\vec{d}_i$ (для чего требуется не более $t(k-1)$ шагов). Еще $(s+1)(t-1)$ шагов требуется, чтобы завершить вычисление $\vec{n}$ по схеме Горнера. Итого, построенная цепочка имеет длину не более

$$t(k + s) + 2^s k - (2k + s + 1) \leq \lambda(n) + \frac{\lambda(n)}{s} k + 2^s k.$$

Утверждение теоремы получается при выборе $s = \lambda(\lambda(n)) - 2\lambda(\lambda(\lambda(n)))$.

*Замечание.* Остаточный член в формулировке теоремы является не лучшим из возможных. Неулучшаемый остаточный член выглядит как $O(k)+(1+o(1))\frac{R}{\log_2 R}$, где $R=\log_2(n_1\cdot\ldots\cdot n_k)$.

Рассмотрим вторую задачу, которая сводится к построению (одномерной) аддитивной цепочки, содержащей числа $n_1,\ldots,n_k$. Длину кратчайшей из таких аддитивных цепочек обозначим через $l(n_1,\ldots,n_k)$.

Задачи 1 и 2 являются двойственными друг другу в смысле, который будет разъяснен ниже, а величины $l([n_1,\ldots,n_k])$ и $l(n_1,\ldots,n_k)$ связаны следующим соотношением.

**Теорема 4** (Пиппенджер, Оливос)**.**

$$l([n_1,\ldots,n_k]) = l(n_1,\ldots,n_k)+k-1.$$

Для доказательства нам удобно рассмотреть задачу 3, обобщающую задачи 1 и 2:

3) Требуется вычислить набор мономов $x_1^{a_{i,1}}x_2^{a_{i,2}}\cdot\ldots\cdot x_p^{a_{i,p}}$, $i=1,\ldots,q$, исходя из $x_1,\ldots,x_p$.

О решении этой задачи будем говорить как о реализации матрицы $A=(a_{i,j})$ векторными аддитивными цепочками.

## 4.1 Лемма о сложности транспонированного отображения

Предварительно напомним определение схемы из функциональных элементов (СФЭ). Пусть задано множество функций $B$, аргументы и значения которых принадлежат множеству $M$. СФЭ над базисом $B$ — это ориентированный граф без ориентированных циклов с вершинами-входами, которым приписаны символы переменных или константы, и функциональными элементами в других вершинах; некоторые вершины отмечены как выходы. Входы и выходы элементов схемы принимают значения в $M$, а сами функциональные элементы реализуют функции из базиса $B$. Более подробное определение и доказательство корректности приводится в соответствующих курсах. *Сложностью* схемы $S$ называется число функциональных элементов в ней и обозначается $L(S)$, а *глубиной* — максимальное число элементов в цепочке, ведущей от входа к выходу схемы, которое обозначается $D(S)$. Сложность (глубина) функции $f$ определяется как минимальная сложность (глубина) схемы, реализующей данную функцию. Обозначения: $L(f)$ и $D(f)$.

Рассмотрим оператор $AX$ линейного отображения с целочисленной матрицей $A$ размера $p \times q$ ($p$ столбцов, $q$ строк) над базисом $\{+\}$ (здесь $"+"$ — ассоциативная и коммутативная операция).

**Лемма 2** (Митягин, Садовский, 1965)**.** $L(AX) = L(A^T X) + p - q$.

*Доказательство.* Пусть схема $S$ реализует $AX$, где $X = (x_1, \ldots, x_p)$ — вектор входов схемы. Через $Y = (y_1, \ldots, y_q)$ обозначим выходы схемы.

Можно проверить, что число (ориентированных) путей в схеме, соединяющих вход $x_i$ с выходом $y_j$, равно соответствующему элементу $a_{i,j}$ матрицы $A$. Для этого достаточно доказать по индукции, что $i$-я компонента вектора $f(e)$, вычисляемого в произвольной вершине $e$ схемы, равна числу путей $\rho(e, x_i)$, соединяющих эту вершину с $i$-м входом. Если $e = x_j$ (основание индукции), то утверждение очевидно. Если утверждение верно для вершин $e_1$ и $e_2$, которые являются входами для вершины $e$, то оно верно и для $e$, т.к. $f(e) = f(e_1) + f(e_2)$ и $\rho(e) = \rho(e_1) + \rho(e_2)$.

Пусть $r$ и $v$ — соответственно число ребер и вершин в схеме $S$. Тогда $L(S) = r - v + p$ (поскольку $r = 2L(S)$ и $L(S) = v - p$). Преобразуем схему $S$ к схеме $S'$, вычисляющей $A^T Y$.

Сначала устраним случаи использования выходов схемы в качестве входов для других ее элементов. Для этого выпустим из таких выходов висячие ребра, и перенесем выходы на свободные концы этих ребер.

После этого обратим ориентацию ребер схемы. Вершины $Y$ становятся входами, а $X$ — выходами в новой схеме. В этой схеме могут оказаться вершины, в которые входит только одно ребро. Удалим такие ребра, совместив концы каждого из них (если одним из концов ребра был вход (выход), то входом (выходом) становится совмещенная вершина). Также в схеме могут оказаться вершины, в которые входит пучок из более чем двух ребер. Такие пучки заменим эквивалентными бинарными деревьями на тех же входах. Окончательно получим схему $S'$, в которой в каждую вершину кроме входов ведут по два ребра.

Обратим внимание, что во-первых, число путей, соединяющих вершины $x_i$ и $y_j$, не изменяется при всех преобразованиях. Следовательно, схема $S'$ реализует матрицу $A^T$. Во-вторых, разница между числом ребер и вершин остается постоянной (по существу, достаточно убедиться, что при замене пучка с $t$ входами бинарным деревом мы добавляем в схему $t - 2$ новых ребра и столько же новых вершин). Как следствие, $L(S') = r - v + q = L(S) + q - p$. Лемма доказана.

## 4.2 Схемная интерпретация аддитивной цепочки

Рассмотрим $k$-мерную аддитивную цепочку с $q$ выходами. Она вычисляет некоторую матрицу $A$ размера $q \times k$. Цепочку можно изобразить графически в виде ориентированного графа, вершинам которого для удобства приписаны символы элементов цепочки $a_i$. В вершину, которой приписан символ $a_i$, идут ребра от вершин с символами $a_j$, $a_k$, где $a_i = a_j + a_k$ (в случае неоднозначности разложения выбирается произвольное из возможных представлений).

Построенный граф можно интерпретировать как схему. Для этого тем вершинам графа, которым приписаны символы базисных единичных векторов, припишем символы переменных $x_i$. Вершины графа интерпретируются как функциональные элементы, реализующие операцию сложения.

Таким образом, построена схема над базисом $\{+\}$, реализующая линейное целочисленное преобразование $AX$, причем сложность схемы совпадает с длиной цепочки.

Обращая проведенное рассуждение, замечаем обратное: некоторой схеме, вычисляющей преобразование $AX$, соответствует цепочка, вычисляющая матрицу $A$, и имеющая длину, равную сложности схемы.

В силу установленной выше двойственности задач реализации матриц $A$ и $A^T$ линейными схемами, двойственность имеет место и для аддитивных цепочек. Таким образом, получаем

**Следствие 1.** *Пусть $A$ — матрица размера $p \times q$. Тогда*

$$l(A) = l(A^T) + p - q.$$

Из этого следствия вытекает теорема 4.

# Дополнительные вопросы

1. Дать конструктивное определение аддитивной цепочке Ханзена.
2. Доказать теорему 1 для линейных цепочек.
3. Доказать, что предполагаемая нижняя граница длины аддитивной цепочки $\lambda(n) + \lceil \log_2 \nu(n) \rceil$ не может быть повышена. Для любого $v \in \mathbb{N}$ предъявить число $n$ веса $v$ и аддитивную цепочку для $n$ длины $\lambda(n) + \lceil \log_2 v \rceil$.