Math-Net.Ru

Общероссийский математический портал

А. И. Никонов, Преобразование суммы взвешенных степеней натуральных чисел с одинаковыми показателями, *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010, выпуск 1(), 258–262

DOI: <https://doi.org/10.14498/vsgtu751>

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: 54.89.56.158

26 апреля 2023 г., 17:46:01

Информатика

УДК 512.14

ПРЕОБРАЗОВАНИЕ СУММЫ ВЗВЕШЕННЫХ СТЕПЕНЕЙ
НАТУРАЛЬНЫХ ЧИСЕЛ С ОДИНАКОВЫМИ ПОКАЗАТЕЛЯМИ**А. И. Никонов**Самарский государственный технический университет,
443100, Самара, ул. Молодогвардейская, 244.

E-mail: nikonovai@mail.ru

Рассмотрено преобразование конечной суммы взвешенных одинаковых степеней натуральных чисел к виду, использующему биномиальные коэффициенты. Такое преобразование обеспечивается последовательным снижением степеней нумерованных величин, которые относятся к промежуточным и завершающим операциям указанного снижения.

Ключевые слова: конечная сумма взвешенных степеней натуральных чисел, индекс состояния, операция степенного снижения, биномиальное разложение, соответствие, последовательность.

В настоящей работе рассматривается способ, позволяющий представить конечную сумму взвешенных степеней натуральных чисел с одинаковыми натуральными показателями, используя при этом как биномиальные коэффициенты, так и действительные весовые коэффициенты самих степеней. Данный способ может быть использован в рамках осуществления криптографической информационной защиты, которая не требует относительно высоких трудозатрат на дешифрование принимаемых сообщений.

Исходная конечная сумма, задаваемая для преобразования и содержащая не менее двух степенных компонентов, имеет вид

$$\Phi(\rho, \nu) = \sum_{\pi=1}^{\rho} b_{\pi} \pi^{\nu}; \quad \rho, \nu, \pi \in \mathbb{N}, b_{\pi} \in \mathbb{R}. \quad (1)$$

Несколько вариантов представления исходной конечной суммы на основе использования биномиальных коэффициентов для частного случая (1), когда $b_{\pi} = 1$, хорошо известны [1, 2]. Настоящая работа позволяет выражать зависимости исходной величины $\Phi(\rho, \nu)$ от сумм того же вида с последовательно снижаемыми максимумами оснований и показателей степеней натуральных чисел, а также изменения значений весовых коэффициентов на каждом шаге такого степенного снижения. Важную роль в описании операций данного снижения играет порядок индексирования получаемых при этом промежуточных и результирующих конечных сумм.

Индекс состояния, в котором находится конечная сумма взвешенных степеней натуральных чисел до проведения очередной операции степенного снижения, а также индекс убывания номеров позиций весовых коэффициентов при степенях конечной суммы обозначим соответственно через i и τ , причём $i, \tau \in \mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Придавая числу π значение $(\rho - i - \tau)$, можно ввести обозначение $b_{\pi}^i = b_{\rho-i-\tau}^i$, где

Александр Иванович Никонов (д.т.н., проф.), профессор, каф. электронных систем и информационной безопасности.

верхний индекс специально указывает на состояние конечной суммы и номер предстоящей операции степенного снижения. В частном случае $i = 0$ действительны равенства $b_\pi = b_\pi^0 = b_{\rho-\tau}$.

Проведение операции степенного снижения подразумевает изначальное выделение единицы в основании каждой степени, относящейся к сумме (1):

$$\pi^\nu = ((\pi - 1) + 1)^\nu,$$

а затем биномиальное разложение данной степени. Первая по счёту операция в процессе общего порядкового преобразования исходной суммы (1) достигает соответствующего единичного снижения как оснований, так и максимального показателя получаемых в ходе нее взвешенных степеней:

$$\Phi(\rho\nu) = \sum_{\tau=0}^{\rho-1} b_{\rho-\tau}^0 (\rho - \tau)^\nu = \Phi_{\rho-1 \ j(1)}|_{j(1)=0} + \sum_{j(1)}^{i-1} C_\nu^{j(1)} \Phi_{\rho-1 \ j(1)}, \quad (2)$$

где $\Phi_{\rho-1 \ j(1)}|_{j(1)=0} = \Phi_{\rho-1 \ 0} = \sum_{\tau=0}^{\rho-1} b_{\rho-1-\tau}^1$;

$$\Phi_{\rho-1 \ j(1)} = \Phi(\rho - 1, j(1)) = \sum_{\tau=0}^{p-2} b_{\rho-1-\tau}^1 (\rho - 1 - \tau)^{j(1)}; \quad (3)$$

$$b_{\rho-1-\tau}^1 = b_{\rho-\tau}^0 + b_{\rho-\tau}^1, \quad b_\rho^1 = 0. \quad (4)$$

Используя (4), по индукции несложно прийти к равенству

$$b_{\rho-1-\tau}^1 = \sum_{k=0}^{\tau} b_{\rho-k}^0. \quad (5)$$

В самом деле, при $\tau = 0$ имеем частный случай данного равенства: $b_{\rho-1}^1 = b_\rho^0 + b_\rho^1 = b_\rho^0$.

Полагая, что (5) соблюдается для произвольного $\tau < \rho - 1$ и увеличивая затем это произвольное значение на единицу, получаем

$$b_{\rho-1-(\tau+1)}^1 = b_{\rho-(\tau+1)}^0 + b_{\rho-(\tau+1)}^1 = b_{\rho-1-\tau}^0 + \sum_{k=0}^{\tau} b_{\rho-k}^0 = \sum_{k=0}^{\tau+1} b_{\rho-k}^0.$$

Выведенное соотношение подтверждает справедливость равенства (5).

Из выражений (2), (5) видно, что индексы типов j, k относятся к множествам соответственно

$$J_0(1) = \{0, 1, \dots, \nu - 1\}, \quad \{0, \dots, \tau\}.$$

Число, занимающее позицию в скобках возле индекса j , указывает, в свою очередь, на индекс первой операции степенного снижения (здесь он, естественно, равен единице). Используем далее следующие соотношения, которые являются простым обобщением выражений (3), (4):

$$\Phi_{\rho-i \ j(i)} = \begin{cases} \Phi(\rho - i, j(i)) = \sum_{\tau=0}^{\rho-i-1} b_{\rho-i-\tau} (\rho - i - \tau)^{j(i)} & : j(i) \geq 1, \\ \Phi(\rho - i, 0) = \sum_{\tau=0}^{\rho-i} b_{\rho-i-\tau}^i & : j(i) = 0; \end{cases} \quad (6)$$

$$b_{\rho-i-\tau}^i = \begin{cases} b_{\rho-(i-1)-\tau}^{i-1} + b_{\rho-i-(\tau-1)}^i, & b_{\rho-i+1}^i = 0 & : i \geq 1, \\ b_{\rho-\tau}^0 = b_{\rho-\tau}, & b_0^0 = 0 & : i = 0; \end{cases} \quad (7)$$

$$\begin{aligned} i \in I_0 = \{0, 1, \dots, \max i\}, \quad \max i &= \begin{cases} \rho - 1 & : \rho \leq \nu, \\ \nu - 1 & : \nu \leq \rho; \end{cases} \\ \tau \in T_0 = \{0, 1, \dots, \max \tau\}, \quad \max \tau &= \rho - i; \\ j(i) \in J_0(i) = \{0, 1, \dots, \max j(i)\}, \quad \max j(i) &= \nu - i. \end{aligned}$$

Легко также убедиться (аналогично тому, как это было сделано применительно к выражению (5)) в справедливости равенства

$$b_{\rho-i-\tau}^i = \sum_{k=0}^{\tau} b_{\rho-(i-1)-k}^{i-1}, \quad i \geq 1. \quad (8)$$

Индексы типа i (в том числе верхние), используемые выражениями (6)–(8), и здесь соответствуют состояниям конечных сумм в процессе выполнения последовательности операций степенного снижения.

Обобщая теперь равенство (2) на случай степенного снижения, операция которого отмечается произвольным индексом $(i+1)$, получаем

$$\Phi_{\rho-i \ j(i)} = \Phi_{\rho-(i+1) \ 0} + \sum_{j(i+1)} C_{j(i)}^{j(i+1)} \Phi_{\rho-(i+1) \ j(i+1)}; \quad (9)$$

$$j(i+1) \in \{1, 2, \dots, \max j(i+1)\}.$$

Соответствие конечных сумм из левой и правой частей (9) может быть представлено как

$$(\Phi_{\rho-i \ j(i)}, j(i) \in J_1(i)) \xrightarrow{i+1} (\Phi_{\rho-(i+1) \ j(i+1)}, j(i+1) = P_{J_0}(i+1)), \quad (10)$$

где $J_1(i) = J_0(i) \setminus \{0\}$; $P_{J_0}(i+1)$ — конечная последовательность, построенная из возрастающих по значениям элементов множества $J_0(i+1)$; индекс $(i+1)$, помещённый над знаком соответствия ($\longrightarrow$), задаёт его номер, а также номер соответствующей операции степенного снижения; $j(i+1) = 0$: $C_{j(i)}^{j(i+1)} = 1$.

Учёт выражения (10), указывающего на факт перехода от суммы $\Phi_{\rho-i \ j(i)}$ к конечной последовательности

$$\Phi_{\rho-(i+1) \ 0}, \Phi_{\rho-(i+1) \ 1}, \dots, \Phi_{\rho-(i+1) \ \max j(i+1)},$$

а также введение множителя $\alpha_{j(i+1)}^{i+1}$ для любой используемой суммы $\Phi_{\rho-(i+1) \ j(i+1)}$ дают возможность сформировать соответствие следующих конечных последовательностей:

$$(\alpha_{j(i)}^i \Phi_{\rho-i \ j(i)}, j(i) = P_{J_1}(i)) \longrightarrow (\alpha_{j(i+1)}^{i+1} \Phi_{\rho-(i+1) \ j(i+1)}, j(i+1) = P_{J_0}(i+1)), \quad (11)$$

$$\alpha_{j(i+1)}^{i+1} = \sum_{j(i)=j(i+1)+1}^{\max j(i)} \alpha_{j(i)}^i \beta_{j(i) \ j(i+1)}, \quad \beta_{j(i) \ j(i+1)} = C_{j(i)}^{j(i+1)}, \quad (12)$$

где $P_{J_1}(i)$ — конечная последовательность, построенная из упорядоченных по возрастанию элементов множества $J_1(i)$.

Наличие в правой части (11) множителей вида $\alpha_{j(i+1)}^{i+1}$ при нахождении множителей вида $\alpha_{j(i)}^i$ в левой части данного соответствия объясняется тем, что при построении указанной правой части в её составе образуются алгебраические комбинации вида $\sum_{j(i)} \alpha_{j(i)}^i C_{j(i)}^{j(i+1)}$. Такое образование происходит путём суммирования конечных последовательностей, получаемых за счёт разложения компонентов левой

части (11) согласно описанию операции (9), к которому здесь прилагается условие принятия индексом $j(i)$ последовательно возрастающих значений $1, 2, \dots, \max j(i)$.

В свою очередь, множители вида $\alpha_{j(i)}^i$ появляются в левой части (11) благодаря соответствующему (предшествующему данному) алгебраическому комбинированию, производимому с участием компонентов вида

$$\alpha_{j(i-1)}^{i-1} \Phi_{\rho-(i-1) j(i-1)},$$

которые используются в предшествующей (i -той) операции степенного снижения. Множители вида α , соответствующие начальным звеньям формируемой цепи последовательно возрастающих индексов i , имеют следующие значения:

$$\alpha_{j(0)}^0 = \begin{cases} 0 & : j(0) < \nu, \\ 1 & : j(0) = \nu; \end{cases} \quad (13)$$

$$\alpha_{j(1)}^1 = C_\nu^j(1), \quad j(1) \in \{0, 1, \dots, \max j(1)\}, \quad \max j(1) = \nu - 1. \quad (14)$$

Как нетрудно заметить, соотношение (10) является частным случаем соответствия (11); в рамках (10) задаётся единственное значение $j(i) \in J_1(i)$. Поскольку имеет место равенство

$$\max j(i) = \max j(i+1) + 1,$$

то общее количество конечных сумм, входящих в правую часть (11) и имеющих ненулевые индексы вида j , оказывается сниженным по сравнению с количеством конечных сумм, которые входят в левую часть (11). Таким образом, с последовательным ростом значения индекса самого соответствия (11) происходит и последовательное сокращение числа промежуточных конечных сумм $\Phi_{\rho-(i+1) j(i+1)}, j(i+1) \in J_1(i+1)$.

Общее выражение разработанной системы соответствий (сопровождаемых степенными порядковыми снижениями) с компонентами вида (11) начиная с исходной взвешенной суммы (1) может быть представлено следующим образом:

$$\begin{aligned} \Phi(\rho, \nu) = \Phi_{\rho-0 \nu-0} &\xrightarrow{1} \begin{cases} \alpha_0^1 \Phi_{\rho-1 \ 0}, \\ (\alpha_{j(1)}^1 \Phi_{\rho-1 j(1)}, j(1) = P_{J_1}(1)) \end{cases} \xrightarrow{2} \dots \\ &\dots \xrightarrow{i} \begin{cases} \alpha_0^i \Phi_{\rho-i \ 0}, \\ (\alpha_{j(i)}^i \Phi_{\rho-i j(i)}, j(i) = P_{J_1}(i)) \end{cases} \xrightarrow{i+1} \\ &\xrightarrow{i+1} \begin{cases} \alpha_0^{i+1} \Phi_{\rho-(i+1) \ 0}, \\ (\alpha_{j(i+1)}^{i+1} \Phi_{\rho-(i+1) j(i+1)}, j(i+1) = P_{J_1}(i+1)) \end{cases} \xrightarrow{i+2} \dots \\ &\dots \xrightarrow{\max i} \begin{cases} \alpha_0^{\max i} \Phi_{\rho-\max i \ 0}, \\ (\alpha_{j(\max i)}^{\max i} \Phi_{\rho-(\max i) j(\max i)}, j(\max i) = P_{J_1}(\max i)) \end{cases} \xrightarrow{\max i+1} \\ &\xrightarrow{\max i+1} (\alpha_0^{\max i+1} \Phi_{\rho-(\max i+1) \ 0}). \end{aligned} \quad (15)$$

Система (15) оставляет в итоге не участвующей в процессе формирования последующих соответствий совокупность величин типа $\alpha_0^i \Phi_{\rho-i \ 0}$, что даёт возможность получить следующий общий результат преобразования исходной суммы взвешенных степеней одинакового порядка:

$$\Phi(\rho, \nu) = \sum_{i=1}^{\max i+1} \alpha_0^i \Phi_{\rho-i \ 0}, \quad \max i+1 = \begin{cases} \rho & : \rho \leq \nu, \\ \nu & : \nu \leq \rho. \end{cases} \quad (16)$$

При этом

$$\Phi_{\rho-(\max i+1) \ 0} = \begin{cases} \Phi_{0 \ 0} = b_0^\rho & : \rho \leq \nu, \\ \Phi_{\rho-\nu \ 0} & : \nu \leq \rho. \end{cases}$$

Непосредственное нахождение числовых значений конкретно заданной конечной суммы (1) выполняется путём рекуррентных вычислений, во-первых, её компонентов вида $\Phi_{\rho-i} 0$ с применением соотношений (6)–(8) и, во-вторых, компонентов вида α_0^i с применением соотношений (12)–(14). Затем полученные числовые компоненты алгебраически комбинируются между собой согласно выражению (16).

Нетрудно видеть, что рассмотренному способу присуще такое важное положительное свойство, как наличие расширенных функциональных возможностей, обеспечивающее преобразование в общем случае именно взвешенных степеней натуральных чисел с одинаковыми показателями. Кроме того, особенностью предложенного способа является наличие двухкомпонентного результата его реализации, который может быть использован субъектами системы передачи шифрованных сообщений в интересах обеспечения её успешной работы.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Градштейн И. С., Рыжик И. М. Таблицы интегралов, сумм, рядов и произведений. — М.: Физматлит, 1963. — 1108 с.
2. Прудников А. П., Брычков Ю. А., Маричев О. И. Интегралы и ряды: В 3-х т. Т. 1: Элементарные функции. — М.: Физматлит, 2002. — 632 с.

Поступила в редакцию 09/I/2010;
в окончательном варианте — 15/III/2010.

MSC: 05A10

CONVERTING THE SUM OF WEIGHTED DEGREES OF NATURAL NUMBERS WITH THE SAME PARAMETERS

A. I. Nikonov

Samara State Technical University,
244, Molodogvardeyskaya str., Samara, 443100.
E-mail: nikonovai@mail.ru

Consider the transformation of a finite sum of weighted equal powers of natural numbers to a form that uses the binomial coefficients. This conversion enables the sequential reduction of enumerated values that belong to the intermediate and final operations of this reduction.

Key words: *finite sum of weighted degrees of natural numbers, condition's index, operation of power reduction, binomial expansion, compliance, consistency.*

Original article submitted 09/I/2010;
revision submitted 15/III/2010.

Alexander I. Nikonov (Dr. Sci. (Techn.)), Professor, Dept. of Electronic Systems & Information Security.