

# Дискретная математика

УДК 512.14

## КОМБИНАТОРНОЕ ПРЕДСТАВЛЕНИЕ СУММЫ ВЗВЕШЕННЫХ ОДИНАКОВЫХ СТЕПЕНЕЙ ЧЛЕНОВ АРИФМЕТИЧЕСКОЙ ПРОГРЕССИИ

*А. И. Никонов*

Самарский государственный технический университет,  
Россия, 443100, Самара, ул. Молодогвардейская, 244.

E-mail: nikonovai@mail.ru

*Устанавливается справедливость равенства, которое даёт выражение для суммы взвешенных одинаковых степеней членов арифметической прогрессии в комбинаторном виде. Этот вид предусматривает использование двойного суммирования определённых алгебраических комбинаций со свободными и весовыми компонентами данной суммы. Указанные алгебраические комбинации включают в себя также биномиальные коэффициенты. Определение искомого равенства выполнялось с использованием сравнения истинных и гипотетических величин.*

**Ключевые слова:** *сумма взвешенных одинаковых степеней, истинное представление, гипотетическое представление, биномиальные коэффициенты.*

Исходным выражением для суммы взвешенных одинаковых степеней (СВОС) членов арифметической прогрессии будем считать равенство

$$\Phi^\xi(p, \nu) = \sum_{\iota=1}^p b_\iota (\iota+d)^\nu = \sum_{\iota=1}^p b_\iota ((\iota-1)+\xi)^\nu; \quad p, \nu, \iota \in \mathbb{N}, \quad b_\iota = b_\iota^0, \quad d, \xi \in \mathbb{R}. \quad (1)$$

Первый член, разность, количество членов арифметической прогрессии составляют здесь соответственно  $\xi$ , 1,  $p$ .

Применительно к сфере шифрования достоинство использования СВОС членов арифметической прогрессии заключается в наличии дополнительно вводимого параметра  $\xi$ , который может принимать любые значения из множества  $\mathbb{R}$ , что создает соответственно дополнительное препятствие в раскрытие шифра, формируемого на основе данной СВОС.

Ниже устанавливается справедливость равенства, позволяющего выразить сумму (1), используя свободные, вида  $\alpha$ , и весовые, вида  $H$ , компоненты СВОС:

$$\Phi^\xi(p, \nu) = \sum_{l=1}^{\max l} \sum_{j(i)=1}^{\nu(i)} \left( \xi^{j(i)} H_i(p) + H_l(p) \right) \alpha_{j(i)}^c, \quad (2)$$

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

где  $l = 1, \dots, \max l$ ,  $\max l = \min(p, \nu)$ ,  $i = l - 1$ ;  $j(i) = 1, \dots, \max j(i)$ ,  $\max j(i) = \nu - i$ ;  $H_i(p) = b_0^l = \sum_{k=0}^{p-l} b_{p-i-k}^i$ ,  $i \geq 0$ ;  $H_l(p) = \sum_{\tau=0}^{p-l} b_{p-l-\tau}^l$ , причём [1, 2]

$$\alpha_{j(i)}^i = \sum_{j(i-1)=j(i)+1}^{\max j(i-1)} \alpha_{j(i-1)}^{i-1} C_{j(i-1)}^{j(i)}, \quad i \geq 1; \tag{3}$$

$$\alpha_{j(0)}^0 = \begin{cases} 0: & j(0) < \nu, \\ 1: & j(0) = \nu. \end{cases} \tag{4}$$

Равенство (1) назовем истинным представлением рассматриваемой СВОС членов арифметической прогрессии, а равенство (2) — её гипотетическим представлением. Далее будем снабжать истинные величины индексами «и» и «l», а гипотетические величины — индексами «г» и  $r = t + 1$ . Индекс  $r$  выполняет здесь ту же роль, что и аналогичный ему индекс  $l$  в известном представлении СВОС [1, 2].

Положим сначала, что  $\nu \leq p$ , то есть  $\max l = \nu$ . Проводя при этом доказательство гипотетического равенства (2), будем сравнивать между собой соответствующие друг другу фрагменты из (1) и (2). Такие действия должны привести нас к благоприятным результатам выполнения указанных сравнений для случаев принятия степенями величины  $\xi$  значения  $j = 0$  (случай с индексом 0) и совокупности значений  $j = 1, \dots, \nu$  (случай с индексом  $1/\nu$ ).

Часть истинного комбинаторного представления СВОС [1, 2], соответствующая нулевой степени величины  $\xi$ , может быть выражена как

$$\Phi_{\text{и}0}^{\xi}(\nu \leq p) = \sum_{l=1}^p b_l(l-1)^\nu = \xi^0 \sum_{l=1}^{\nu} \Phi_{p-1-l0} \alpha_0^l; \tag{5}$$

$$\Phi_{p-1-l0} = \sum_{\tau=0}^{p-1-l} b_{p-1-l-\tau}^l.$$

Часть же гипотетического представления СВОС членов арифметической прогрессии, также соответствующая нулевой степени  $\xi$ , имеет вид

$$\Phi_{\text{г}0}^{\xi}(\nu \leq p) = \sum_{r=1}^{\nu} \sum_{j(t)=1}^{\nu-t} H_r(p) \alpha_{j(t)}^t. \tag{6}$$

Зададимся следующими равенствами, в которых отразим соотношения индексов истинного и гипотетического представлений:

$$r = l = l(j) = t + 1.$$

Тогда, преобразуя (6), получим

$$\Phi_{\text{г}0}^{\xi}(\nu \leq p) = \sum_{l=1}^{\nu} H_l(p) \left( \sum_{j(t)=1}^{\nu-t} \alpha_{j(t)}^t \right). \tag{7}$$

Согласно выражению (3), второй сомножитель, находящийся под знаком суммы из (7), имеет тот же вид, что и соответствующий сомножитель  $\alpha_0^l$  из (5).

Располагая известным комбинаторным представлением [3]

$$\Phi_{p-l0} = \sum_{k=0}^{p-l} C_{p-k}^l b_{p-k}^0,$$

нетрудно получить следующие соотношения:

$$H_l(p) = \sum_{k=0}^{p-l-1} C_{p-1-k}^l b_{p-k}^0,$$

$$H_{l-1}(p) = \sum_{k=0}^{p-l-1} C_{p-1-k}^{l-1} b_{p-k}^0,$$

$$\Phi_{p-1-l0} = \sum_{k=0}^{p-1-l} C_{p-1-k}^l b_{p-k}^0.$$

В последней из данных сумм, где сравнительно с величиной  $\Phi_{p-l0}$  взята аналогичная величина со сниженным индексным значением  $(p-1-l)$ , в качестве сомножителей биномиальных коэффициентов оставлены именно весовые коэффициенты с большими индексами. Итак, в рамках случая  $j=0$  имеет место равенство

$$H_l(p) = \Phi_{p-1-l0},$$

а вместе с ним и равенство друг другу величин (5) и (7):

$$\Phi_{r0}^\xi(\nu \leq p) = \Phi_{n0}^\xi(\nu \leq p). \quad (8)$$

Далее исследуем случай  $j=1, \dots, \nu$  с индексом  $1/\nu$ . Части истинного комбинаторного [1, 2] и гипотетического представлений суммы (1) в данном случае выражаются таким образом:

$$\begin{aligned} \Phi_{n1/\nu}^\xi &= \Phi_{n1/\nu}^{\xi 1}(\nu \leq p) + \Phi_{n1/\nu}^{\xi 2}(\nu \leq p) = \\ &= \sum_{j=1}^{\nu-1} \xi^j C_\nu^j \sum_{l=1}^{\nu-j} \Phi_{p-1-l0} \alpha_0^l(\nu-j) + \xi^\nu \sum_{\iota=1}^p b_\iota^0; \quad (9) \end{aligned}$$

$$\sum_{\iota=1}^p b_\iota^0 = \Phi_{p-1-l0} \Big|_{l=0} = \Phi_{p-10}; \quad \Phi_{r1/\nu}^\xi = \sum_{r=1}^{\nu} \sum_{j(t)=1}^{\nu-t} \xi^j H_t(p) \alpha_{j(t)}^t. \quad (10)$$

Здесь в рамках рассматриваемого случая приняты индексные соотношения

$$r-1 = t = l = l(j).$$

Поскольку  $\min r = 1$ , наименьшее значение  $l(j)$  должно принимать в данном случае нулевое значение.

Сопоставляя (9) и (10), выделяем компоненты, первая пара которых относится к истинным, а вторая пара — к гипотетическим величинам:

$$\xi^j C_\nu^j \Phi_{p-1-l} \alpha_0^l (\nu - j), \quad 1 \leq j \leq \nu - 1; \quad (11)$$

$$\xi^\nu \sum_{l=1}^p b_l^0, \quad j = \nu; \quad (12)$$

$$\begin{aligned} \xi^j H_t(p) \alpha_{j(t)}^t &= \xi^j \sum_{k=0}^{p-t-1} C_{p-1-k}^t b_{p-k}^0 \times \\ &\times \left( C_\nu^{j(t)} \sum_{\chi=1}^t (-1)^{t+\chi} C_t^\chi \chi^{\nu-j(t)} \right), \quad 1 \leq j = j(t) \leq \nu - 1; \end{aligned} \quad (13)$$

$$\xi^\nu H_t(p) \alpha_{j(t)}^t \Big|_{t=0, j(t)=\nu} = \xi^\nu \sum_{k=0}^{p-1} b_{p-k}^0, \quad j = \nu. \quad (14)$$

При выполненном таким образом выделении компонентов, относящихся к гипотетическим величинам, с учётом принятых выше индексных соотношений нами использовалось равенство вида

$$\alpha_{j(l)}^l = \left( \sum_{\chi=1}^l (-1)^{1+\chi} C_l^\chi \chi^{\nu-j(l)} \right) C_\nu^{j(l)}, \quad (15)$$

которое обобщает ранее полученное соотношение [3]. Продолжим здесь изложение общих результатов производимого анализа случая с индексом  $1/\nu$ , а к строгому доказательству (15) в рамках настоящей мы вернемся позже.

Рассматривая пределы суммирования в выражениях (9), (10), можно установить, что количество попарно сравниваемых там объектов суммирования  $O_{\text{н}1/\nu}(\nu \leq p)$ ,  $O_{\text{г}1/\nu}(\nu \leq p)$  составляет как для  $\Phi_{\text{н}1/\nu}^\xi(\nu \leq p)$ , так и для  $\Phi_{\text{г}1/\nu}^\xi(\nu \leq p)$  одну и ту же величину

$$O_{\text{н}1/\nu}(\nu \leq p) = O_{\text{г}1/\nu}(\nu \leq p) = 0,5\nu(\nu - 1) + 1.$$

При этом из величины  $O_{\text{г}1/\nu}$  вычитается число объектов (равное  $\nu - 1$ ), которым, согласно выражению (4), исходно ставятся в соответствие нулевые значения; наличие или отсутствие таких компонентов никак не сказывается на результате количественного определения рассматриваемой СВОС.

Итак, поскольку наблюдается попарное совпадение друг с другом выражений (11) и (13), (12) и (14) при наличии баланса объектов суммирования, относящихся к истинным и гипотетическим величинам, действительными оказываются также следующие равенства:

$$\sum_{j=1}^{\nu-1} \xi^j H_t(p) \sum_{j(t)=1}^{\nu-t} \alpha_{j(t)}^t = \Phi_{\text{н}1/\nu}(\nu \leq p), \quad j = 1, \dots, \nu - 1;$$

$$\xi^\nu \sum_{\iota=1}^p H_0(p) \alpha_\nu^0 = \Phi_{\text{и}1/\nu}^{\xi 2}(\nu \leq p), \quad j = \nu;$$

$$\Phi_{\text{г}1/\nu}^\xi(\nu \leq p) = \Phi_{\text{и}1/\nu}^\xi(\nu \leq p).$$

В целом же с учётом выражения (8), наконец, имеем

$$\Phi_{\text{г}0}^\xi(\nu \leq p) + \Phi_{\text{г}1/\nu}^\xi(\nu \leq p) = \Phi_{\text{и}0}^\xi(\nu \leq p) + \Phi_{\text{и}1/\nu}^\xi(\nu \leq p).$$

Перейдём к рассмотрению случая  $p \leq \nu$ , в рамках которого число  $l$  ограничивается сверху значением  $p$ , а число  $i$  — значением  $(p - 1)$ . Здесь сохраняется прежняя справедливость равенства друг другу истинной  $\Phi_{\text{и}0}^\xi$  и гипотетической  $\Phi_{\text{г}0}^\xi$  сумм взвешенных степеней, определяемых как модификации выражений (5) и (7), где вводятся соответствующие поправки на обозначения верхних пределов суммирования, учитывающие особенность рассматриваемого случая. Таким образом, нетрудно убедиться, что  $\Phi_{\text{и}0}^\xi(p \leq \nu) = \Phi_{\text{г}0}^\xi(p \leq \nu)$ . Остаются в силе также и вышеприведённые соотношения, связанные с парными сравнениями друг с другом выражений вида (11) и (13), (12) и (14). Уточнения требует лишь количество сравниваемых объектов суммирования.

Подсчёт объектов суммирования в истинной величине  $\Phi_{\text{и}1/\nu}^\xi(p \leq \nu)$ , аналогичной (9), применительно к настоящему условию  $p \leq \nu$  даёт значение

$$O_{\text{и}1/\nu}(p \leq \nu) = 0,5(2\nu - p)(p - 1) + 1,$$

а подсчёт объектов суммирования в величине гипотетического характера  $\Phi_{\text{г}1/\nu}^\xi(p \leq \nu)$ , аналогичной (10), с учётом указанного условия приводит нас к равенству, сходному с прежним:

$$O_{\text{г}1/\nu}(p \leq \nu) = O_{\text{и}1/\nu}(p \leq \nu).$$

Как и для прежнего случая  $\nu \leq p$ , из данного результата изъяты  $(\nu - 1)$  объектов суммирования, которые соответствуют нулевым свободным компонентам, указываемым выражением (4). Следовательно, и в данном случае  $p \leq \nu$  сохраняется общий баланс объектов суммирования истинного и гипотетического представления СВОС членов арифметической прогрессии.

Теперь, чтобы окончательно убедиться в истинности общей гипотезы (2), остаётся доказать справедливость равенства (15) для используемых диапазонов чисел  $l$ ,  $j(l)$ , что будет выполнено ниже с использованием метода математической индукции.

Сперва рассмотрим случай  $\nu \leq p$  и в рамках базы индукции определим параметр  $\alpha_{j(1)}^l = \alpha_{j(1)}^1$ . Согласно истинному соотношению (3), с учётом исходной системы равенств (4) данный параметр может быть представлен как [1]

$$\alpha_{j(1)}^1 = \sum_{j(0)=1}^{\nu} C_{j(0)}^{j(1)} \alpha_{j(0)}^0.$$

Отсюда видно, что членам конечной последовательности  $(j(1)) = 0, \dots, \nu - 1$  соответствует совокупность чисел  $(\alpha_{j(1)}^1) = (C_{\nu}^{j(1)})$ .

Согласно же заявленному — пока гипотетическому — утверждению (15) имеем для  $l = 1$

$$\alpha_{j(1)}^1 = \sum_{\chi=1}^1 ((-1)^{1+1} C_l^1 1^\nu) C_{\nu}^{j(1)}.$$

То есть для конечной последовательности  $(j(1))$  получена та же конечная последовательность, что и при использовании истинного соотношения (3). Следовательно, для  $l = 1$  наше гипотетическое утверждение (15) следует обоснованно считать истинным, а при  $\max l = 1$  ( $\nu = 1$  или  $p = 1$ ) — ещё и окончательным. Далее будем рассматривать случай  $\nu \leq p$ ,  $\nu > 1$ .

Предваряя осуществление индукционного шага, найдём отношение величин  $\alpha_{j(l)}^{l+1}$  и  $\alpha_{j(l)}^l$ , первоначально представляемых в заявленном гипотетическом виде:

$$\frac{\alpha_{j(l+1)=j(l)}^{l+1}(\nu)}{\alpha_{j(l)}^l(\nu)} = \frac{\sum_{\chi=1}^l (-1)^{l+1+\chi} C_{l+1}^{\chi} \chi^{\nu-j(l)}}{\sum_{\chi=1}^l (-1)^{l+\chi} C_l^{\chi} \chi^{\nu-j(l)}};$$

$$0 \leq j(l) = j(l+1) \leq \nu - l - 1 \Rightarrow l \leq \nu - 1, \quad l + 1 \leq \nu.$$

Как видим, число  $(l + 1)$  остаётся здесь в интервале индексов определяемых параметров вида  $\alpha_{j(l)}^l, \alpha_{j(l)}^{l+1}$ .

Доказанное ранее [3] позволяет утверждать, что

$$\sum_{\chi=1}^{\psi} (-1)^{\psi+\chi} C_{\psi}^{\chi} \alpha^{\nu-j(l)} = \alpha_0^{\psi}(\nu - j(l)), \quad \psi \in \{l, l + 1\}.$$

Но тогда

$$\frac{\alpha_{j(l)}^{l+1}(\nu)}{\alpha_{j(l)}^l(\nu)} = \frac{\alpha_0^l(\nu - j(l))}{\alpha_0^l(\nu - j(l))}. \tag{16}$$

Выявление отношения истинных значений параметров из правой части (16) оказалось возможным исходя из отношения параметров гипотетического характера из левой части (16), т.е. гипотетическое отношение определилось истинными величинами. Это позволяет облегчить завершение производимого доказательства.

Теперь, непосредственно выполняя шаг индукции, положим, что утверждение (15) для случая  $\nu \leq p$  истинно. Тогда с учётом (16) параметр

$$\alpha_{j(l)}^{l+1} = \frac{\alpha_{j(l)}^l(\alpha_0^{l+1}(\nu - j(l)))}{\alpha_0^l(\nu - j(l))},$$

занимающий следующую за  $l$  позицию в последовательности  $(\alpha_{j(l)}^l(\nu))$  с фиксированным значением  $j(l)$ , должен полагаться истинным, а данный индукционный шаг — уже законченным.

Для случая  $p \leq \nu$  ( $\max l = p$ ) все вышеприведённые соотношения, касающиеся базы индукции, получения частного (16), выполнения шага индукции, остаются в силе.

Имеем также

$$0 \leq j(l) = j(l+1) \leq \nu - l - 1 \quad \Rightarrow \quad l \leq \nu - 1, \quad l+1 \leq \nu,$$

однако более сильные ограничения, накладываемые на  $l, l+1$ , могут быть представлены в виде

$$p \leq \nu: \quad l \leq p - 1, \quad l+1 \leq p.$$

Как и прежде, число  $(l+1)$  остаётся в интервале индексов определяемых величин. На этом доказательство справедливости равенства (15), а вместе с тем и доказательство истинности общей гипотезы (2) можно считать завершённым.

В заключение укажем на одну особенность набора величин  $\alpha_{j(l)}^l(\nu)$ ,  $l + j(l) = \nu$ , которые представляют собой, с одной стороны, согласно выражению (15), произведения сумм компонентов  $(-1)^{l+\chi} C_l^\chi \chi^l$  и  $C_\nu^{j(l)}$ , а с другой — размещения из  $\nu$  элементов по  $l$  [4], то есть

$$\alpha_{j(l)}^l(\nu) = A_\nu^l = \frac{\nu!}{(\nu-l)!}, \quad l + j(l) = \nu.$$

Итак, убывающий факториал  $A_\nu^l$  может быть представлен здесь именно как сумма компонентов, входящих в выражение (15).

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. А. И. Никонов, “Преобразование суммы взвешенных степеней натуральных чисел с одинаковыми показателями” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010. №1(20). С. 258–262. [А. И. Nikonov, “Converting the Sum of Weighted Degrees of Natural Numbers with the Same Parameters” // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2010. no. 1(20). Pp. 258–262].
2. А. И. Никонов, “Об одном свойстве взвешенных сумм одинаковых степеней как матричных произведений” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2010. №5(21). С. 313–317. [А. И. Nikonov, “On One Property of the Weighed Sums of Equal Powers as Matrix Products” // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2010. no. 5(21). Pp. 313–317].
3. А. И. Никонов, “Приведение суммы взвешенных одинаковых степеней к явному комбинаторному представлению” // *Вестн. Сам. гос. техн. ун-та. Сер. Физ.-мат. науки*, 2012. №3(28). С. 163–169. [А. И. Nikonov, “Reduction of the sum of the weight equal powers to explicit combinatorial representation” // *Vestn. Samar. Gos. Tekhn. Univ. Ser. Fiz.-Mat. Nauki*, 2012. no. 3(28). Pp. 163–169].
4. А. И. Никонов, *Дискретная математика*. Самара: СамГТУ, 2011. 106 с. [А. И. Nikonov, *Discrete Mathematics*. Samara: Samara State Technical Univ., 2011. 106 pp.]

Поступила в редакцию 10/X/2013;  
в окончательном варианте — 12/XI/2013.

MSC: 05A10

## COMBINATORIAL REPRESENTATION OF THE SUM OF THE WEIGHTED EQUAL POWERS OF MEMBERS OF AN ARITHMETICAL PROGRESSION

*A. I. Nikonov*

Samara State Technical University,  
244, Molodogvardeyskaya st., Samara, 443100, Russia.

E-mail: [nikonovai@mail.ru](mailto:nikonovai@mail.ru)

*The correctness of equality which gives the combinatorial expression for the sum of the weighted equal powers of members of an arithmetical progression is found out. Such aspect provides usage of double summation of certain algebraic combinations with free and weight components of the given sum. Thus specified algebraic combinations also include binomial coefficients. Determination of required equality was made with use of comparison of real and hypothetical values.*

**Keywords:** *sum of the weighted equal powers, real representation, hypothetical representation, binomial coefficients.*

Original article submitted 10/X/2013;  
revision submitted 12/XI/2013.

---

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