КОМП'ЮТЕРНІ ЗАСОБИ, МЕРЕЖІ ТА СИСТЕМИ

УДК 512(075)

А.В. ПАЛАГИН, М.В. СЕМОТЮК

ОБОБЩЕНИЕ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ

Рассмотрено обобщение известных теоретико-числовых преобразований на основе некоторой фундаментальной теоремы связывающей базис преобразования s с модулем M кольца вычетов, на котором задано это преобразование. Показано, что все известные преобразования такого рода являются частным случаем преобразования, полученного на основании этой теоремы.

Алгоритмы обработки сигналов в конечных математических структурах, аналогично спектральной обработке, составляют интересную область исследований, полезную для представления систем счисления, кодовых последовательностей, операций над полиномами, а также для решения ряда задач, где требуются точные значения результатов вычислений. Несмотря на большое количество публикаций по этому вопросу [1, 2, 3], в литературе нет обобщающих работ по теоретико-числовым преобразованиям (ТЧП), как, скажем, для Фурье-преобразований (ПФ). В работе [3] показано существование ТЧП и его основных теорем на базе теории представлений конечных абелевых групп, где удалось получить удовлетворительные результаты, однако, ряд его теорем попрежнему остается не доказанными. Это объясняется следующим.

Во-первых, ПФ рассматриваются как представления конечных абелевых групп, заданных на конечных множествах. ТЧП же задаются на множествах, которые называются структурами или решетками. Для этих множеств, кроме условия целостности, еще заданы точная верхняя грань $\sup\mathbf{Z}$ и точная нижняя грань $\inf\mathbf{Z}$, а операции, которые заданы на этих множествах, представляют собой операции по некоторому модулю.

Во-вторых, для представления реальных сигналов требуется, по крайней мере, хотя бы такая алгебра, как кольцо, ибо одной бинарной операции, которая задана группой, явно недостаточно. Расширение же группы до кольца, если в качестве носителя алгебры

выступает конечное множество, не представляет существенных затруднений, и, стало быть, ПФ достаточно полно согласуются с представлениями групп. В ТЧП, в качестве кольца, используется кольцо вычетов по модулю Z_m, носителем которого, естественно, является структура (решетка), а расширение группы вычетов до кольца вычетов по модулю в свою очередь имеет ряд особенностей, связанных с двойственностью операций в кольце вычетов. Поэтому прямые аналогии с теорией ПФ для ТЧП не всегда могут быть корректны. Отсюда возникает необходимость в создании некоторой обобщенной теории, специально построенной для ТЧП, которая систематизировала бы ряд полученных за последнее время результатов. Основу этой теории может составлять некоторая фундаментальная теорема для обобщения ТЧП. Сформулируем эту теорему.

Пусть алгебра вида $Z_m =< \mathbf{S},+,\cdot,\mathbf{0},\mathbf{1} >$ и $\mathbf{0} \neq \mathbf{1}$, где $\mathbf{S} \in \mathbf{Z}$ – структура (решетка), имеющая $\sup \mathbf{S} = S^p - 1$, $\inf \mathbf{S} = \mathbf{0}$ при $\forall p \in \mathbf{N}$, представляет собой кольцо вычетов Z_m с единицей, в котором своими аргументами задана степенная зависимость $y = s^x$. Тогда для $\forall s \in \mathbf{S}$, $\forall p \in \mathbf{N}$, $\forall x = \overline{0, N}$ и $\forall p << N$ существует такое число $M < \sup \mathbf{S}$, при котором имеет место следующее равенство (сравнение) в кольце вычетов Z_m.

$$S^{(x) \bmod p} \underline{\underline{Z_m}} (s^x) \bmod M, \qquad (1)$$

где $\underline{\underline{Z_m}}$ - обозначение равенства в кольце вычетов (в общем случае не всегда совпадающее с известным понятием "сравнение по модулю" в силу разных значений модуля в левой и правой частях выражения (1). При этом M есть функция от p - $M = f(p)$. Другими словами, если в левой или правой частях равенства есть операция по модулю, то независимо от нее результат еще раз ограничивается, как слева, так и справа равенства, модулем кольца Z_m. Доказательство этого утверждения в виде теоремы приведено в [4].Отметим некоторые следствия, вытекающие из этой теоремы.

Следствие 1. Числа s и $\sum_{m=0}^{p-1} s^m$ взаимно простые при $\forall s > 2$.

Действительно

$$\sum_{m=0}^{p-1} s^m = s^0 + \sum_{m=1}^{p-1} s^m = s^0 + \sum_{m=0}^{p-2} s^m .$$

Поскольку $s < \sum_{m=0}^{p-1} s^m$, то, учитывая последнее, имеем

$$\frac{\sum_{m=0}^{p-1} s^m}{s} = \frac{s^0}{s} + \sum_{m=0}^{p-2} s^m , \quad \text{здесь} \quad \sum_{m=0}^{p-2} s^m = \operatorname{int} \frac{\sum_{m=0}^{p-1} s^m}{s}, \quad \text{а} \quad \frac{s^0}{s} = \frac{1}{s} < 1 .$$

Тогда $\forall s > 2$ не является делителем для $\sum_{m=0}^{p-1} s^m$ и эти числа являются взаимно простыми.

Следствие 2. Две числовые последовательности вида нуля для $\sum_{m=0}^{p-1} s^m$ и, следовательно, эти числа $s^{(x) \bmod p}$ и $(\mathrm{s}^{\mathrm{X}}) \bmod (\sum_{\mathrm{m}=0}^{\mathrm{p}-1} \mathrm{s}^{\mathrm{m}})$ полученные, из s^x путем изменения $x = \overline{0, N}$ в кольце вычетов Z_m, конгруэнтные вплоть до каждого члена при одном и том же значении x.

Следствие 3. Две числовые последовательности вида $s^{(x) \bmod p}$ и $(s^x) \bmod (\sum_{m=0}^{p-1} s^m)$ при $x = \overline{0, N}$ периодичны в кольце вычетов Z_m, имеют одинаковый период p и одно и то же главное значение, находящееся в интервале $[0, p-1]$.

Отметим еще одно важное свойство теоремы (1), заключающееся в том, что она позволяет заменять операции по модулю над степенными выражениями в целом, операциями по модулю над показателями степеней степенных зависимостей, входящих в эти выражения. Но тогда в пределах изменения показателя степени степенной зависимости вычеты этой зависимости в кольце Z_m являются кусочно-аналитическими периодическими функциями и, следовательно, к ним применим математический аппарат аналитических функций. Для теоретико-числовых преобразований последнее является как раз тем фундаментальным свойством, столь необходимым для доказательства условий существования таких преобразований , а также их основных теорем**.**

Полагая, что главное значение числовой степенной последовательности находится на закрытом интервале $[0, p-1] = [0, N-1]$, при этом $\sup \mathbf{S} = M$, где $M = \sum_{m=0}^{N-1} s^m$ - модуль кольца Z_m, определим формально следующее преобразование, заданное на структуре **S**

$$X(k) \overset{Z_m}{=\!=} \sum_{i=0}^{N-1} x(i) s^{-(ki) \bmod N}, \tag{2}$$

$$x(i) \overset{Z_m}{=\!=} \frac{1}{N} \sum_{k=0}^{N-1} X(k) s^{(ki) \bmod N}, \tag{3}$$

$$M = \sum_{m=0}^{N-1} s^m,$$

где Z_m – кольцо вычетов по модулю M, N – некоторое число из множества $\mathbf{N}$, $\overset{Z_m}{=\!=}$ – означает равенство (сравнение) в кольце вычетов Z_m, $x(i), X(k)$ – числовые последовательности, представляющие оригинал и изображение соответственно, s – некоторое число (базис преобразования), в общем случае комплексное, i, k – номера (индексы) компонент последовательностей.

Выражение (2) представляет собой прямое преобразование, а (3) – обратное. Покажем теперь, что эта пара выражений действительно представляет собой теоретико-числовое преобразование. Для чего, во избежание путаницы индексов, в выражении (2) заменим i на n, а затем подставим его в (3). В результате будем иметь

$$x(n) \overset{Z_m}{=\!=} \frac{1}{N}\sum_{k=0}^{N-1}\Big(\sum_{i=0}^{N-1} x(i)\, s^{-(ki) \bmod N}\Big) s^{(kn) \bmod N}.$$

Изменив порядок суммирования, получаем

$$x(n) \overset{Z_m}{=\!=} \frac{1}{N}\sum_{k=0}^{N-1} x(i)\Big(\sum_{i=0}^{N-1} x(i)\, s^{(kn-ki) \bmod N}\Big).$$

Далее

$$x(n) \overset{Z_m}{=\!=} \frac{1}{N}\sum_{i=0}^{N-1} x(i)\Big(\frac{1}{N}\sum_{k=0}^{N-1} s^{|(n-i)k| \bmod N}\Big). \qquad (4)$$

Рассмотрим теперь внутреннюю сумму

$$\sum_{k=0}^{N-1} s^{|(n-i)k| \bmod N}. \qquad (5)$$

Очевидно, что при $i = n$ значение этой суммы будет равно N. Для $i \neq n$ внутренняя сумма (5) не равна N и не равна нулю, что необходимо для преобразования. Однако, может существовать сравнение вида

$$\sum_{k=0}^{N-1} s^{|(n-i)k| \bmod N} = 0 \mid \bmod M, \qquad (6)$$

которого достаточно для преобразования, поскольку вычисления будут выполняться в кольце вычетов Z_m. Положим, что $M = \sum_{m=0}^{N-1} s^m$. Тогда на основании свойств геометрической прогрессии имеем

$$\sum_{k=0}^{N-1} s^{|(n-i)k| \bmod N} \overset{Z_m}{=\!=} \frac{s^{(n-i)N}-1}{s^{n-i}-1} = 0 \mid \bmod M,$$

что на основании теоремы (1) равно

$$(s^{(n-i)N}) \bmod M \overset{Z_m}{=\!=} s^{[(n-i)N] \bmod N} \overset{Z_m}{=\!=} s^0 = 1,$$

$$(\frac{s^{(n-i)N}-1}{s^{n-i}-1}) \bmod M \overset{Z_m}{=\!=} (\frac{1-1}{s^{n-i}-1}) \bmod M \overset{Z_m}{=\!=} 0.$$

Сравнение (6) действительно выполняется. Последнее, с учетом вышесказанного, а также порядком выполнения операций в кольце вычетов будет иметь вид следующей системы уравнений:

$$\begin{cases} \sum\limits_{m=0}^{N-1} s^{[(n-i)k] \bmod N} \overset{Z_m}{=\!=} N, \quad i = n \ , \\ \sum\limits_{m=0}^{N-1} s^{[(n-i)k] \bmod N} \overset{Z_m}{=\!=} \mathbf{0}, \quad i \neq n \ . \end{cases} \tag{7}$$

Отсюда следует, что и правая часть выражения (4) будет состоять из единственного, не равного нулю в кольце вычетов Z_m, члена $x(i)$ только в том случае, если $i = n$. Тогда в (4) последовательность $x(n)$ совпадает с последовательностью $x(i)$ при $i = n$, следовательно, выражения (2) и (3) представляют собой теоретико-числовое преобразование (S-преобразование, т.е. преобразование, заданное на структуре). Последнее легко иллюстрируется в матричном виде.

Пусть $N = 3$, $M = \sum\limits_{m=0}^{2} s^m$. Для этого случая имеем две матрицы , одну – для прямого, другую – для обратного преобразований.

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & s^1 & s^2 \\ 1 & s^2 & s^1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1/s^1 & 1/s^2 \\ 1 & 1/s^2 & 1/s^1 \end{bmatrix}.$$

Найдем обратные элементы для $1/s^1$ и $1/s^2$. Ими будут соответственно s^2 и s^1 в силу того, что $s^2 \cdot s^1 = 1 \,|\, \bmod M$. Тогда матрицы примут вид

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & s^1 & s^2 \\ 1 & s^2 & s^1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 & 1 \\ 1 & s^2 & s^1 \\ 1 & s^1 & s^2 \end{bmatrix},$$

а их произведение в кольце вычетов Z_m будет равно

$$\left[\begin{bmatrix} 1 & 1 & 1 \\ 1 & s^1 & s^2 \\ 1 & s^2 & s^1 \end{bmatrix} \times \begin{bmatrix} 1 & 1 & 1 \\ 1 & s^2 & s^1 \\ 1 & s^1 & s^2 \end{bmatrix}\right] \bmod (\sum_{m=0}^{2} s^m) = \begin{bmatrix} 3 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{bmatrix}$$

в чем нетрудно убедиться, выполнив соответственно вычисления, принимая во внимание при этом, что матрица, находящаяся в произведении слева, соответствует матрице обратного теоретико-числового преобразования, т.е. выражению

(3), а матрица, находящаяся справа от знака произведения, представляет прямое преобразование (2).

В выражениях (2) и (3) было декларировано, что N - простое число. Это связано с тем, что при простом N в кольце вычетов Z_m всегда существует обратный элемент N^{-1}, так как в этом случае образуется тройка взаимно простых чисел s, N, M (N - простое по определению, а взаимная простота s и M следует из следствия 1 теоремы (1)). Если же N не является простым числом, то возникают проблемы не только с обратным элементом N^{-1}, но и со значением выражения (5), для которого должны обязательно выполняться условия (7), определяющие существование преобразований (2) и (3). С другой стороны произвольный выбор N весьма желателен, так как он, в конечном счете, определяет размерность преобразования.

Пусть N - составное число $N = p_1 p_2$, составленное из двух простых чисел p_1 и p_2. Тогда система весовых функций преобразования будет содержать степенные последовательности с периодами $N, p_1 и p_2$. Нетрудно убедиться в том, что средние значения этих функций при $i = \overline{0, N-1}$ будут равны или кратны соответственно

$$S_1 = M = \sum_{m=0}^{N-1} s^m \ - \text{период равен } N, \quad S_2 = M = \sum_{m=0}^{p_2-1} s^{p_1 m} \ - \text{период равен } p_2,$$

$$S_3 = M = \sum_{m=0}^{p_1-1} s^{p_2 m} \ - \text{период равен } p_1.$$

Если между p_1 и p_2 выполняется соотношение $p_1 < p_2$, тогда между этими суммами существует соотношение

$$S_3 < S_2 < S_1. \tag{8}$$

Для выполнения условия существования теоретико-числовых преобразований (7) необходимо, чтобы

$$S_1 = 0 \,|\, \mathrm{mod}\, M, \quad S_2 = 0 \,|\, \mathrm{mod}\, M, S_3 = 0 \,|\, \mathrm{mod}\, M, \quad \forall S_i > N.$$

Из соотношения (8) следует, что $M = S_3$, так как S_3 наименьшая сумма. Однако, теперь необходимо, чтобы S_1 и S_2 делились на S_3 без остатка. Действительно, на основании свойств геометрической прогрессии имеем

$$S_1 = \frac{s^N - 1}{s - 1}, \quad S_2 = \frac{(s^{p_1})^{p_2} - 1}{s^{p_1} - 1} = \frac{s^N - 1}{s^{p_1} - 1}, \quad S_3 = \frac{(s^{p_2})^{p_1} - 1}{s^{p_2} - 1} = \frac{s^N - 1}{s^{p_2} - 1}.$$

Тогда

$$\frac{S_1}{S_3} = \frac{s^N - 1}{s - 1} = \sum_{i=0}^{p_2-1} s^i, \tag{9}$$

$$\frac{S_2}{S_3} = \frac{s^{p_2} - 1}{s^{p_1} - 1} = \sum_{i=0}^{p_2 - 1} s^i \,, \tag{10}$$

говорит о том, что N не может быть составным числом, так как не будут удовлетворяться условия (7). Исключение составляет случай, вытекающий из (9), при котором

$$N = p \cdot p \,. \tag{11}$$

По индукции можно показать, что $N = p^n$. Тогда условие, связующее p, s и M будет следующее:

$$M = \sum_{m=0}^{p-1} s^{pm} > p^n \,.$$

На основании свойств геометрической прогрессии $\dfrac{s^p - 1}{s - 1} > p^n$ или

$$p < \sqrt[n]{\frac{s^p - 1}{s - 1}} \,. \tag{12}$$

Таким образом, получено еще одно выражение для N, при котором существует ТЧП. Далее уточним величину модуля M. На основании (11) имеем

$$N = p^n = p \cdot p^{n-1} \,.$$

Тогда

$$s - 1 = (s^{p^{n-1}})^p - 1 \,, \tag{13}$$

или в силу (11)

$$s^N - 1 = (s^{p^{n-1}} - 1) \cdot \sum_{m=0}^{p-1} (s^{p^{n-1}})^m \,.$$

Подставляя в (13), получаем

$$s^N - 1 = (s - 1) \cdot \sum_{k=0}^{p^{n-1}} s^k \cdot \sum_{m=0}^{p-1} (s^{p^{n-1}})^m \,.$$

Поделив обе части полученного выражения на $(s - 1)$, имеем

$$M = \sum_{m=0}^{n-1} s^m = \sum_{k=0}^{p^{n-1}} s^k \cdot \sum_{m=0}^{p-1} (s^{p^{n-1}})^m \,. \tag{14}$$

Таким образом, при $N = p^n$ модуль M является составным числом и в связи с последним в качестве модуля преобразования может быть выбрано одно из этих составных чисел. Вместе с тем условия преобразования удовлетворит только M, равное

$$M = \sum_{m=0}^{p-1} (s^{p^{n-1}})^m \,. \tag{15}$$

Этот факт объясняется тем, что в силу теоремы (1) модуль преобразования

$$M = \sum_{k=0}^{p^{n-1}} s^k \ , \tag{16}$$

дает последовательность s^k размерностью p^{n-1}, следовательно, такую же размерность преобразования, что значительно меньше требуемого N. Далее, на основании (15) ясно, что последовательность s^k при $i = \overline{0, N-1}$ и

$$s^i < M = \sum_{m=0}^{p-1} (s^{p^{n-1}})^m \tag{17}$$

имеют обычную явную степенную зависимость. Определим теперь какую зависимость будет представлять s^i при $s^i > M$. Действительно, последний член в (15) имеет вид

$$(s^{p^{n-1}})^{p-1} = s^{p^n - p^{n-1}}.$$

Стало быть, элементы последовательности $s^i > M$ будут иметь выражение вида $s^i = (s^{p^n - p^{n-1}}) \cdot s^k = s^{p^n - p^{n-1} + k}$, где $k = \overline{1, N - p^n + p^{n-1} - 1}$, полученное из условия замены переменной

$$i = p^n - p^{n-1} + k > p^n - p^{n-1} \ . \tag{18}$$

Тогда

$$s^{p^n - p^{n-1} + k} = s^{p^n} \cdot s^{-p^{n-1} + k}$$

на основании теоремы (1) дает

$$s^{p^n - p^{n-1} + k} \underline{\underline{Z_m}} \ s^{-p^{n-1} + k}.$$

Заменив обратно k на i, из (18) получаем

$$s^{p^n - p^{n-1} + k} \underline{\underline{Z_m}} \ s^{-p^{n-1} - p^n + p^{n-1} + i} \underline{\underline{Z_m}} \ s^{-p^n + i}$$

или окончательно

$$s^i \underline{\underline{Z_m}} \ (s^{p^n - i})^{-1} \underline{\underline{Z_m}} \ (s^{N-1})^{-1}, \text{ при } s^i > M \ . \tag{19}$$

Таким образом, элементы последовательности s^i при $s^i > M$ представляют собой обратные элементы по отношению к элементам $s^i > M$. Обратимость при этом существует только в кольце Z_m. В результате S-преобразование (2) ,(3) может рассматриваться, с учетом индексов по (18), как кососимметричное двустороннее преобразование вида

$$X(k) \underline{\underline{Z_m}} \sum_{i=(p^{n-1}-1)}^{p^n - p^{n-1}} x(i) s^{-(ki) \bmod [-p^n + 1, p^n - p^{n-i}]} \ , \tag{20}$$

$$x(i) \underline{\underline{Z_m}} \sum_{k=(p^{n-1}-1)}^{p^n - p^{n-1}} X(k) s^{(ki) \bmod [-p^n + 1, p^n - p^{n-i}]} \ , \tag{21}$$

$$M = \sum_{m=0}^{p-1} (s^{p^{n-1}})^m . \qquad (22)$$

При этом периодичность весовой функции преобразования определяется не величиной N (т.е. замкнутым интервалом $[0, N-1)$, а замкнутым интервалом $[-p^{n-1}+1, p^n - p^{n-1}]$, который к тому же и несимметричен, так как абсолютные значения его концов не равны между собой:

$$|-p^{n-1}+1| \neq | p^n - p^{n-1} |,$$

отчего и название преобразования – кососимметричное.

Вместе с тем существует еще один уникальный случай, представляющий исключение из условия (11). Речь идет о четном N

$$N = 2p, \qquad (23)$$

где p - любое целое число.

Стало быть,

$$s^N - 1 = s^{2p} - 1 = (s^p)^2 - 1 = (s^p - 1)*(s^p + 1).$$

Далее, в силу (11)

$$s^p - 1 = (s-1) \cdot \sum_{n=0}^{p-1} s^n .$$

Тогда

$$s^N - 1 = (s-1) \cdot \left(\sum_{n=0}^{p-1} s^n \right) \cdot (s^p + 1).$$

Разделив обе части на $(s-1)$, имеем

$$M = \sum_{m=0}^{p-1} (s^{p^{n-1}})^m = (s^p + 1) \cdot \sum_{n=0}^{p-1} s^n . \qquad (24)$$

Как и в случае (14), преобразованию удовлетворяет модуль

$$M = s^p + 1, \qquad (25)$$

дающий преобразование размерности N. При этом S-преобразование принимает вид

$$X(k) \overset{Z_m}{\Longleftarrow} \sum_{i=-(p-1)}^{p} x(i) s^{-(ki) \bmod [-p+1, p]}, \qquad (26)$$

$$x(i) \overset{Z_m}{\Longleftarrow} 1/N \sum_{k=-(p-1)}^{p} X(k) s^{(ki) \bmod [-p+1, p]}, \qquad (27)$$

$$M = s^p + 1. \qquad (28)$$

с интервалом существования

$$[-p+1, p], \qquad (29)$$

представляющий собой также разновидность теперь уже почти симметричного двустороннего преобразования, поскольку значения весовой функции s^{ki} при

$s^{ki} > M$, как и в случае (19), являются обратными элементами в кольце Z_m к значениям весовой функции s^{ki} при $s^{ki} > M$.

Однако может так оказаться, что $s^p + 1$ – также составное число, что следует из теоремы Ферма:

$$s^{N\,p} - 1 = 0 \bmod (N + 1). \tag{30}$$

Вместе с тем, все простые числа, за исключением числа 2, являются нечетными числами, а поскольку степенная функция не содержит членов, равных нулю, то ограниченная сверху модулем, равным $M = N + 1$, будет содержать на своем главном периоде всего N различных между собой значений, где N – четное число.

Таким образом, мы имеем дело с преобразованием, размерность которого представлена четным числом. Очевидно, что речь идет о преобразовании (26), (27), (28), в которых модуль преобразования может быть составным числом, которое содержит число $N+1$. Действительно, в силу (30), число $s^N - 1$ делится на $N+1$ без остатка, что означает, что один из сомножителей из (24) обязательно делится на $N+1$. Если же для (28) имеет место вышеизложенное, т.е. $M = s^p + 1$ – составное число, в которое входит $N+1$, то существует следующее преобразование:

$$X(k) \overset{Z_m}{=\!=} \sum_{i=0}^{N-1} x(i) s^{-(ki) \bmod N}, \tag{31}$$

$$x(i) \overset{Z_m}{=\!=} 1/N \sum_{k=0}^{N-1} X(k) s^{(ki) \bmod N}, \tag{32}$$

$$M = N + 1. \tag{33}$$

При этом, несмотря на малую величину модуля M, всегда существует обратный элемент для N

$$N^2 - 1 = (N-1) \cdot (N-1),$$

который дает сравнение по модулю $N+1$ следующего вида:

$$N^2 - 1 \equiv 0 \bmod (N + 1) \quad \text{или} \quad N^2 \equiv 1 \bmod (N + 1).$$

Отсюда надо полагать, что

$$N \cdot N^{-1} \overset{Z_m}{=\!=} 1,$$

тогда

$$N \cdot N^{-1} \overset{Z_m}{=\!=} N^2 \overset{Z_m}{=\!=} N \cdot N$$

и, стало быть, обратным элементом к N является само N.

Размерность преобразования равна N и весовая функция преобразования в этом случае будет содержать N различных значений, которые лежат в замкнутом интервале $[1, N]$ в силу модуля (33) и представляют целые числа от 1 до N.

Тогда матрицу как прямого, так и обратного преобразования можно упорядочить путем перестановки строк и столбцов таким образом, что элементы строки с индексом $k = 1 (i = 1)$ или столбца с индексом $i = 1 (k = 1)$, соответственно матриц прямого и обратного преобразований, будут представлять линейно возрастающую последовательность, в которой разность между соседними элементами постоянна и равна 1. В этом случае будет иметь место одна из разновидностей пилообразного преобразования (весовая функция при $k = 1$ – для прямого и $i = 1$ – для обратного преобразований представляет собой зависимость в виде отрезка прямой $y = x$, именуемой в технике пилой).

В заключение заметим, что часто используемые теоретико-числовые преобразования, такие как Мерсена и Ферма, являются частными случаями S-преобразования при $s = 2$. Так, преобразование Мерсена получается из (2) и (3) при $s = 2$ и модуле преобразования

$$M = 2^N - 1 = (2-1) \cdot \sum_{m=0}^{N-1} 2^m = \sum_{m=0}^{N-1} 2^m \ .$$

Преобразование же (26), (27), (28) дает преобразование Ферма при следующих условиях: $s = 2$ и $p = 2^n$, где n - целое число.

1. *Рабинер Л., Гоулд Б.* Теория и применение цифровой обработки сигналов // М.: Мир, 1978. – 848 с.
2. *Nussbauwer H.I.* Fast Fourier Transform fnd Convolution Algorithms // Berlin, Heedelberg, New York.: Springer-Verlad. – 1981. – 250 с.
3. *Вариченко Л.В., Лабунец В.Г., Раков М.А.* Абстрактные алгебраические системы и цифровая обработка сигналов // Киев: Наук. думка, 1986. – 247 с.
4. *Семотюк М.В.* Обобщенное теоретико-числовое преобразование. – Киев: 1994. – 30с. – (Препр. / Ин-т кибернетики им. В.М.Глушкова НАН Украины; 94-8).

Получено 01.07.2002