

ПАРАМЕТРИЧЕСКОЕ КОДИРОВАНИЕ ИНДЕКСОВ*

В. Н. Малозёмов
malv@gamma.math.spbu.ru

19 мая 2004 г.

1°. Пусть $N = n_1 n_2 \dots n_s$, где n_α — попарно взаимно простые натуральные числа, отличные от единицы. Обозначим $N_\alpha = N/n_\alpha$. При каждом $\alpha \in 1 : s$ возьмём натуральное число $p_\alpha \in 1 : n_\alpha - 1$, взаимно простое с n_α .

ПРЕДЛОЖЕНИЕ 1. *Формула*

$$j = \left\langle \sum_{\alpha=1}^s j_\alpha p_\alpha N_\alpha \right\rangle_N \quad (1)$$

устанавливает взаимно однозначное соответствие между наборами коэффициентов $(j_1, j_2, \dots, j_s)$ с $j_\alpha \in 0 : n_\alpha - 1$ и числами $j \in 0 : N - 1$.

Доказательство. Поскольку мощности множества векторов $(j_1, j_2, \dots, j_s)$ с $j_\alpha \in 0 : n_\alpha - 1$ и множества чисел $j \in 0 : N - 1$ равны, то достаточно проверить, что разные векторы $(j_1, j_2, \dots, j_s)$ порождают разные j . Допустив, что $(j_1, j_2, \dots, j_s) \rightarrow j$, $(j'_1, j'_2, \dots, j'_s) \rightarrow j$, получим

$$\sum_{\alpha=1}^s (j_\alpha - j'_\alpha) p_\alpha N_\alpha = r N$$

при некотором целом r . Отсюда следует, что при всех $\alpha \in 1 : s$

$$\langle (j_\alpha - j'_\alpha) p_\alpha N_\alpha \rangle_{n_\alpha} = 0.$$

Поскольку произведение $p_\alpha N_\alpha$ взаимно просто с n_α , то $j_\alpha - j'_\alpha$ делится на n_α , а так как $|j_\alpha - j'_\alpha| \leq n_\alpha - 1$, то необходимо $j_\alpha = j'_\alpha$ при всех $\alpha \in 1 : s$.

Теперь ясно, что разные наборы коэффициентов $(j_1, j_2, \dots, j_s)$ порождают разные j . Предложение доказано. $\square$

* Санкт-Петербургский городской семинар «Всплески (wavelets) и их приложения».
Секция «Дискретный гармонический анализ»: <http://www.math.spbu.ru/user/dmp/dha/>

2°. Перепишем (1) в виде

$$\sum_{\alpha=1}^s j_{\alpha} p_{\alpha} N_{\alpha} = r N + j.$$

Как следствие, получаем $\langle j_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}$ при всех $\alpha \in 1 : s$. Отсюда можно вывести явную формулу для j_{α} . Действительно, по условию числа $p_{\alpha} N_{\alpha}$ и n_{α} взаимно просты. Это гарантирует, что уравнение $\langle x p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$ имеет на множестве $1 : n_{\alpha} - 1$ единственное решение $x = q_{\alpha}$ [1]. Более того, q_{α} взаимно просто с n_{α} .

Покажем, что

$$j_{\alpha} = \langle j q_{\alpha} \rangle_{n_{\alpha}}, \quad \alpha \in 1 : s. \quad (2)$$

Для этого достаточно проверить, что правая часть (2) удовлетворяет уравнению $\langle x p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}$. Имеем

$$\langle \langle j q_{\alpha} \rangle_{n_{\alpha}} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = \langle j \langle q_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} \rangle_{n_{\alpha}} = \langle j \rangle_{n_{\alpha}}.$$

Формула (2) установлена.

Формулу (1) можно воспринимать как разложение индекса $j \in 0 : N - 1$ по базису $\{p_{\alpha} N_{\alpha}\}_{\alpha=1}^s$, в котором коэффициенты j_{α} вычисляются по формуле (2).

Обозначим $p = (p_1, p_2, \dots, p_s)$ и запишем (1) в компактном виде

$$j = (j_1, j_2, \dots, j_s)_p. \quad (3)$$

Правую часть (3) будем называть *p-кодом индекса j*.

3°. Как отмечалось, q_{α} взаимно просто с n_{α} при всех $\alpha \in 1 : s$. Это даёт возможность записать представление

$$j = (j_1^*, j_2^*, \dots, j_s^*)_q, \quad (4)$$

где $q = (q_1, q_2, \dots, q_s)$. Для вычисления коэффициента j_{α}^* нужно решить уравнение $\langle x q_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$. Очевидно, что единственным на множестве $1 : n_{\alpha} - 1$ решением этого уравнения является $x = p_{\alpha}$. Отсюда следует, что

$$j_{\alpha}^* = \langle j p_{\alpha} \rangle_{n_{\alpha}}, \quad \alpha \in 1 : s.$$

Коды (3), (4) индекса $j \in 0 : N - 1$ назовём *сопряжёнными*. Если $p = q$, то эти коды совпадают. В таком случае код $j = (j_1, j_2, \dots, j_s)_p$ с $j_{\alpha} = \langle j p_{\alpha} \rangle_{n_{\alpha}}$ при $\alpha \in 1 : s$ назовём *самосопряжённым*.

4°. При $p_1 = p_2 = \dots = p_s = 1$, т. е. при $p = (1, 1, \dots, 1)$, p -код индекса j называется *руританским* [2]. Вернёмся к подробной записи формулы (3) для руританского кода:

$$j = \left\langle \sum_{\alpha=1}^s j_{\alpha} N_{\alpha} \right\rangle_N. \quad (5)$$

Здесь $j_{\alpha} = \langle j q_{\alpha} \rangle_{n_{\alpha}}$, причём q_{α} — единственное на множестве $1 : n_{\alpha} - 1$ решение уравнения $\langle x N_{\alpha} \rangle_{n_{\alpha}} = 1$.

Сопряжённый к руританскому код называется *китайским*. Он порождает представление

$$j = \left\langle \sum_{\alpha=1}^s j_{\alpha}^* q_{\alpha} N_{\alpha} \right\rangle_N \quad (6)$$

с $j_{\alpha}^* = \langle j \rangle_{n_{\alpha}}$.

ПРИМЕР 1. Пусть $s = 2$, $n_1 = 4$, $n_2 = 25$, так что $N = 100$, $N_1 = 25$, $N_2 = 4$. Вычислим $q_1 \in 1 : 3$ и $q_2 \in 1 : 24$. Для этого нужно решить уравнения $\langle 25 x \rangle_4 = 1$ и $\langle 4 x \rangle_{25} = 1$. Очевидно, что $q_1 = 1$, $q_2 = 19$. Согласно (5) любое число $j \in 0 : 99$ допускает руританское представление

$$j = \langle 25 j_1 + 4 j_2 \rangle_{100},$$

где $j_1 = \langle j \rangle_4$, $j_2 = \langle 19 j \rangle_{25}$. (Проверьте это на $j = 13$.)

Китайское представление числа $j \in 0 : 99$ определяется формулой (6):

$$j = \langle 25 j_1^* + 76 j_2^* \rangle_{100},$$

где $j_1^* = \langle j \rangle_4$, $j_2^* = \langle j \rangle_{25}$. (Проверьте это на $j = 31$.)

5°. Обратимся к самосопряжённым кодам. Напомним, что взаимно простые с n_{α} числа p_{α} , q_{α} принадлежат множеству $1 : n_{\alpha} - 1$ и связаны соотношением $\langle q_{\alpha} p_{\alpha} N_{\alpha} \rangle_{n_{\alpha}} = 1$. Выполнение условия $p_{\alpha} = q_{\alpha}$ можно обеспечить, решив уравнение

$$\langle x^2 N_{\alpha} \rangle_{n_{\alpha}} = 1. \quad (7)$$

Обозначим через b_{α} единственное на множестве $1 : n_{\alpha} - 1$ решение уравнения $\langle x N_{\alpha} \rangle_{n_{\alpha}} = 1$.

ПРЕДЛОЖЕНИЕ 2. Уравнение (7) равносильно уравнению

$$\langle x^2 \rangle_{n_{\alpha}} = b_{\alpha}. \quad (8)$$

Доказательство. Пусть $\langle x_0^2 N_\alpha \rangle_{n_\alpha} = 1$. Тогда

$$\langle x_0^2 \rangle_{n_\alpha} = \langle x_0^2 \langle b_\alpha N_\alpha \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle \langle x_0^2 N_\alpha \rangle_{n_\alpha} b_\alpha \rangle_{n_\alpha} = \langle b_\alpha \rangle_{n_\alpha} = b_\alpha.$$

Наоборот, если $\langle x_0^2 \rangle_{n_\alpha} = b_\alpha$, то

$$\langle x_0^2 N_\alpha \rangle_{n_\alpha} = \langle \langle x_0^2 \rangle_{n_\alpha} N_\alpha \rangle_{n_\alpha} = \langle b_\alpha N_\alpha \rangle_{n_\alpha} = 1.$$

Предложение доказано. $\square$

В случае, когда уравнение (8) имеет решение, говорят, что b_α является *квадратичным вычетом по модулю n_α* [3]. Уравнение (8) не всегда имеет решение. Например, не существует целых x , удовлетворяющих уравнению $\langle x^2 \rangle_5 = 2$. В то же время уравнение $\langle x^2 \rangle_5 = 4$ имеет на множестве $1 : 4$ два решения $x = 2$ и $x = 3$.

Предположим, что уравнение (8) имеет решение $x = p_\alpha$ на множестве $1 : n_\alpha$ при всех $\alpha \in 1 : s$. Обозначим $p = (p_1, p_2, \dots, p_s)$. Тогда p -код числа $j \in 0 : N - 1$ является самоспряжённым, т. е. $j = (j_1, j_2, \dots, j_s)_p$, где $j_\alpha = \langle j p_\alpha \rangle_{n_\alpha}$.

ПРИМЕР 2. Сохраним данные примера 1: $n_1 = 4$, $n_2 = 25$. Покажем, что в этом случае существует четыре самоспряжённых кода.

Решив уравнения $\langle 25x \rangle_4 = 1$, $\langle 4x \rangle_{25} = 1$, найдём $b_1 = 1$, $b_2 = 19$. Перейдём к уравнениям

$$\langle x^2 \rangle_4 = 1, \quad \langle x^2 \rangle_{25} = 19.$$

Первое из них имеет два решения $p_1 = 1$ и $p_1 = 3$. Столько же решений имеет и второе уравнение: $p_2 = 12$, $p_2 = 13$. Комбинируя значения p_1 и p_2 , получаем четыре самоспряжённых кода для чисел $j \in 0 : 99$:

1) $p_1 = 1$, $p_2 = 12$;

$$j = \langle 25 j_1 + 48 j_2 \rangle_{100}, \quad j_1 = \langle j \rangle_4, \quad j_2 = \langle 12 j \rangle_{25}.$$

2) $p_1 = 1$, $p_2 = 13$;

$$j = \langle 25 j_1 + 52 j_2 \rangle_{100}, \quad j_1 = \langle j \rangle_4, \quad j_2 = \langle 13 j \rangle_{25}.$$

3) $p_1 = 3$, $p_2 = 12$;

$$j = \langle 75 j_1 + 48 j_2 \rangle_{100}, \quad j_1 = \langle 3 j \rangle_4, \quad j_2 = \langle 12 j \rangle_{25}.$$

4) $p_1 = 3$, $p_2 = 13$;

$$j = \langle 75 j_1 + 52 j_2 \rangle_{100}, \quad j_1 = \langle 3 j \rangle_4, \quad j_2 = \langle 13 j \rangle_{25}.$$

6°. Отметим одно замечательное свойство китайского кода (6).

ПРЕДЛОЖЕНИЕ 3. Пусть числа $k, j \in 0 : N - 1$ имеют китайские коды

$$k = (k_1^*, k_2^*, \dots, k_s^*)_q, \quad j = (j_1^*, j_2^*, \dots, j_s^*)_q,$$

где $k_\alpha^* = \langle k \rangle_{n_\alpha}$, $j_\alpha^* = \langle j \rangle_{n_\alpha}$. Тогда

$$\begin{aligned} \langle k + j \rangle_N &= (\langle k_1^* + j_1^* \rangle_{n_1}, \dots, \langle k_s^* + j_s^* \rangle_{n_s})_q, \\ \langle k j \rangle_N &= (\langle k_1^* j_1^* \rangle_{n_1}, \dots, \langle k_s^* j_s^* \rangle_{n_s})_q. \end{aligned}$$

Доказательство. Запишем

$$(\langle k + j \rangle_N)_\alpha^* = \langle \langle k + j \rangle_N \rangle_{n_\alpha} = \langle k + j \rangle_{n_\alpha} = \langle \langle k \rangle_{n_\alpha} + \langle j \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle k_\alpha^* + j_\alpha^* \rangle_{n_\alpha}.$$

Аналогично

$$(\langle k j \rangle_N)_\alpha^* = \langle \langle k j \rangle_N \rangle_{n_\alpha} = \langle k j \rangle_{n_\alpha} = \langle \langle k \rangle_{n_\alpha} \langle j \rangle_{n_\alpha} \rangle_{n_\alpha} = \langle k_\alpha^* j_\alpha^* \rangle_{n_\alpha}.$$

Предложение доказано. $\square$

7°. Сопряжённые коды применяются в методе простых множителей быстрого вычисления дискретного преобразования Фурье [2]. Точнее, используется следующее свойство комплексного числа $\omega_N = \exp(2\pi i/N)$, являющегося корнем N -й степени из единицы.

ПРЕДЛОЖЕНИЕ 4. Пусть $k, j \in 0 : N - 1$, причём известны p -код числа j и сопряжённый код числа k :

$$j = (j_1, j_2, \dots, j_s)_p, \quad k = (k_1^*, k_2^*, \dots, k_s^*)_q,$$

где $j_\alpha = \langle j q_\alpha \rangle_{n_\alpha}$, $k_\alpha^* = \langle k p_\alpha \rangle_{n_\alpha}$. Тогда

$$\omega_N^{kj} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha}. \quad (9)$$

Доказательство. Поскольку $\langle q_\alpha p_\alpha N_\alpha \rangle_{n_\alpha} = 1$, то

$$\begin{aligned} \omega_N^{kj} &= \omega_N^{\left(\sum_{\alpha=1}^s k_\alpha^* q_\alpha N_\alpha\right) \left(\sum_{\alpha=1}^s j_\alpha p_\alpha N_\alpha\right)} = \omega_N^{\sum_{\alpha=1}^s k_\alpha^* j_\alpha q_\alpha p_\alpha N_\alpha^2} = \\ &= \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha \langle q_\alpha p_\alpha N_\alpha \rangle_{n_\alpha}} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha^* j_\alpha}. \end{aligned}$$

Предложение доказано. $\square$

СЛЕДСТВИЕ. В случае самосопряжённых кодов

$$k = (k_1, k_2, \dots, k_s)_p, \quad j = (j_1, j_2, \dots, j_s)_p$$

с $k_\alpha = \langle k p_\alpha \rangle_{n_\alpha}$, $j_\alpha = \langle j p_\alpha \rangle_{n_\alpha}$ формула (9) принимает вид

$$\omega_N^{kj} = \prod_{\alpha=1}^s \omega_{n_\alpha}^{k_\alpha j_\alpha}.$$

8°. Вопросы кодирования индексов рассматривались также в работах [4, 5].

ЛИТЕРАТУРА

1. Малозёмов В. Н., Машарский С. М. *Основы дискретного гармонического анализа*. СПб.: НИИММ, 2003. Часть первая. Предварительные сведения.
2. Гуд И. Дж. *О взаимоотношении между двумя быстрыми преобразованиями Фурье*. В кн.: Макклеллан Дж. Х., Рейдер Ч. М. *Применение теории чисел в цифровой обработке сигналов*. М.: Радио и связь, 1983.
3. Виноградов И. М. *Основы теории чисел*. Изд. седьмое. М.: Наука, 1965. Глава пятая.
4. Burrus C. S. *Index mappings for multidimensional formulation of the DFT and convolution* // IEEE Trans. Acoust., Speech, Signal Processing. 1977. Vol. ASSP-25. No. 3. P. 239–242.
5. Свердлик М. Б. *Матричная интерпретация алгоритма БПФ для взаимно простых сомножителей* // Радиотехника и электроника. 1983. № 10. С. 1931–1938.