Теорема 2. Оптимальная кривая C задается следующими уравнениями:

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \beta_0 y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

или

$$\begin{cases} z^2 = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \alpha_3 x^3 + (\beta_0 + \beta_1 x) y, \\ y^2 = x^3 + ax + b, \end{cases}$$

где $\alpha_0, \alpha_1, \alpha_2, \beta_0, \beta_1, a, b$ — коэффициенты из $\mathbb{F}_q$. Эллиптическая кривая E задана уравнением $y^2 = x^3 + ax + b$.

ЛИТЕРАТУРА

1. *Waterhouse W. C.* Abelian varieties over finite fields // Ann. Sci. Ecole Norm. Sup. 1969. No. 2. P. 521–560.
2. *Andreotti A.* On a Theorem of Torelli // American J. of Math. V. 80. 1958. No. 4. P. 801–828.

УДК 512.6

НЕКОТОРЫЕ СВОЙСТВА ДИСКРЕТНОГО ПРЕОБРАЗОВАНИЯ ФУРЬЕ В ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ И ПОЛЯХ КОНЕЧНОЙ ХАРАКТЕРИСТИКИ

А. М. Гришин

Дискретное преобразование Фурье — это один из видов ортонормированного преобразования векторов [1, 2]. Для конечной последовательности элементов $\{s_0, s_1, ..., s_{N-1}\}$ дискретное преобразование Фурье (ДПФ) заключается в поиске другой последовательности $\{S_0, S_1, ..., S_{N-1}\}$, элементы которой вычисляются по формуле (прямое преобразование)

$$S_k = \sum_{n=0}^{N-1} s_n \cdot W_N^{kn};\ k = \overline{0, N-1}, \tag{1}$$

где W_N — примитивный корень степени N из единицы [1, 3]. В предположении, что элемент $N^{-1} = 1/N$ существует, для обратного преобразования можно записать выражение

$$s_n = \frac{1}{N} \sum_{k=0}^{N-1} S_k \cdot W_N^{-kn};\ n = \overline{0, N-1}. \tag{2}$$

Считается, что вектор $s = (s_0, s_1, ..., s_{N-1})$ является представлением данных во временной области, а вектор $S = (S_0, S_1, ..., S_{N-1})$ — в частотной (спектральной).

Векторы s и S можно задать с помощью соответствующих многочленов $s(X)$ и $S(X)$

$$s(X) = s_0 + s_1 X + ... + s_{N-1} X^{N-1}; \tag{3}$$

$$S(X) = S_0 + S_1 X + ... + S_{N-1} X^{N-1}. \tag{4}$$

Если конечная последовательность

$$\{s_n = s[nT] = s(t),\ n = \overline{0, N-1};\ t = nT\} \tag{5}$$

получена в результате дискретизации действительной (комплексной) функции $s(t)$, то, в предположении $T = 1$, $s(t)$ соответствует преобразование Фурье

$$S(e^{i\omega}) = \sum_{n=0}^{N-1} s_n e^{-i\omega n}, \tag{6}$$

где $S(e^{i\omega})$ — непрерывная 2π-периодическая функция, $i = \sqrt{-1}$.

Согласно теореме Котельникова [4, 5], в частотной области функция $S(e^{j\omega})$ полностью определяется последовательностью своих равноотстоящих отсчетов $\{S(e^{i2\pi k/N}) = S_k;\ k = \overline{0, N-1}\}$, взятых с интервалом $\Delta\omega = 2\pi/N$, что соответствует применению в (1), (2) $W_N = e^{-i2\pi/N}$. Это позволяет вычислять значения функции $S(e^{i\omega})$ различными методами. Например:

1. В любых точках с помощь интерполяционной формулы [4]

$$S(e^{i\omega}) = \frac{1}{N}\sum_{k=0}^{N-1} S_k \frac{\sin[(\omega N - 2\pi k)/2]}{\sin[(\omega N - 2\pi k/N)/2]} \cdot e^{-i[(N-1)/2](\omega - 2\pi k/N)}, \quad k = \overline{0, N-1}, \tag{7}$$

которая позволяет вычислить значение спектра для любого ω.

2. Методом подбора значения $N_F \geqslant N$, дополнением вектора $s = (s_0, s_1, ...s_{N-1})$ нулевыми значениями до длины N_F и вычислением (1) для $k = \overline{0, N_F - 1}$.

В поле комплексных чисел C лежат корни из 1 для любого натурального N; таким образом, в (1), (2) N может принимать любое натуральное значение, и $W_N = e^{-i2\pi/N}$ является примитивным корнем степени N из 1.

Величина W_N^{kn} периодична по k и n с периодом N:

$$W_N^{kn} = W_N^{(k+AN)(n+BN)}, \tag{8}$$

где A, B — любые целые. Для четных n и N имеет место равенство

$$W_N^{kn} = W_{N/2}^{kr}, \text{ где } \quad n = 2r. \tag{9}$$

Используя (9), для четного N выражение (1) можно переписать в виде

$$S_k = \sum_{r=0}^{N/2-1} s_{2r} \cdot W_{N/2}^{kr} + W_N^k \cdot \sum_{r=0}^{N/2-1} s_{2r+1} \cdot W_{N/2}^{kr};\ r = \overline{0, N/2-1}. \tag{10}$$

Таким образом можно построить быстрые алгоритмы вычисления ДПФ (БПФ) для любого составного N. Оценка сложности выполнения алгоритма БПФ носит логарифмический характер, и для $N = 2^M$ эта оценка равна $O(NM)$ [6].

Особенности строения поля C позволяют построить алгоритмы БПФ логарифмической сложности для любого, в том числе простого N [7]. Это достигается дополнением вектора $s = (s_0, s_1, ..., s_{N-1})$ нулевыми значениями до длины $N_F = 2^M$, ближайшей к $2N$ (метод 2). Например, для $N = 13$ получим $N_F = 32$. При этом всегда $N_F < 4N$.

В поле C алгоритмы БПФ позволяют определять свойства анализируемых данных, эффективно проводить вычисления сверток и многое другое. Свойства данных исследуются путем определения спектральных максимумов и минимумов в амплитудной характеристике (6), разрывов в фазовой характеристике, при этом нахождение точных значений корней многочленов (3), (4), как правило, не требуется [4, 5].

В конечном поле Галуа GF(q) [1, 3] N в (1), (2) уже не может принимать произвольное значение, так как порядок элемента W_N должен быть кратен порядку мультипликативной группы GF(q), равному $q-1$. В частности, корни из 1 степени 2^M принадлежат GF(q), где q — простое, если $q = c2^M + 1$, где c — натуральное. В этом случае можно использовать (10) с максимальной эффективностью.

Многие свойства ДПФ переносятся на случай конечных полей, но с учетом сформулированного выше ограничения. Произвольное дополнение вектора $s = (s_0, s_1, ..., s_{N-1})$ нулевыми значениями с целью построения алгоритмов БПФ с максимальным быстродействием невозможно. Для GF(q) справедливы следующие утверждения.

Утверждение 1. Спектральная координата S_k вектора S равна 0 тогда и только тогда, когда W_N^k является корнем многочлена $s(X)$ (3).

Утверждение 2. Координата s_n вектора s равна 0 тогда и только тогда, когда W_N^{-n} является корнем многочлена $S(X)$ (4).

Доказательства утверждений 1, 2 очевидны, так как

$$s(W_N^k) = s_0 + s_1 W_N^k + ... + s_{N-1} W_N^{k(N-1)} = S_k;$$
$$S(W_N^{-n}) = S_0 + S_1 W_N^{-n} + ... + S_{N-1} W_N^{-n(N-1)} = s_n.$$

Элементы GF(p^m), где p — простое, могут быть представлены в надполе GF(p^{mK}) или расширении поля GF(p^m) [1, 3]. При этом корни и спектральные нули исходного поля GF(p^m) будут «видны» во всех этих расширениях.

Например, пусть $G_1 = \mathrm{GF}(p^m) = \mathrm{GF}(2^6)$, $N = 2^6 - 1 = 63$. Возможные расширения поля G_1: $G_2 = \mathrm{GF}(p^{2m}) = \mathrm{GF}(2^{12})$ и $G_3 = \mathrm{GF}(p^{3m}) = \mathrm{GF}(2^{18})$ содержат элементы поля G_1, и корни многочлена $s(W_N^k) = 0$ над G_1 могут быть найдены и в G_2, и в G_3. Это свойство позволяет по спектральным нулям в максимально возможном для исследования поле строить предположения о возможных подполях, в которых эти нули также проявятся.

ЛИТЕРАТУРА

1. *Глухов М. М., Елизаров В. П., Нечаев А. А.* Алгебра. Т. 1, 2. М.: ГелиосАРВ, 2003.
2. *Ярославский Л. П., Мерзляков Н. С.* Методы цифровой голографии. М.: Наука, 1977.
3. *Фомичев В. М.* Методы дискретной математики в криптологии. М.: Диалог-МИФИ, 2010.
4. *Оппенгейм А., Шафер Р.* Цифровая обработка сигналов. М.: Техносфера, 2009.
5. *Солонина А. И., Улахович Д. А., Арбузов С. М., Соловьева Е. Б.* Основы цифровой обработки сигналов. 2-е изд. СПб.: БХВ-Петербург, 2006.
6. *Черемушкин А. В.* Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002.
7. `http://psi-logic.shadanakar.org/fft/fft.htm`