ОБ ОДНОМ КЛАССЕ ТЕОРЕТИКО-ЧИСЛОВЫХ ПРЕОБРАЗОВАНИЙ

Ивашко А. В. [1)], **Лунин Д. А.** [1)]
[1)] ***Национальный технический университет «Харьковский политехнический институт», г. Харьков, E-mail: ivashkoauts@ gmail.com, lunindenis77@gmail.com***

При решении задач радиолокации, связи, технической и медицинской диагностики и многих других широко применяется дискретный спектральный и корреляционный анализ [1].

Так, широкое распространение получили алгоритмы спектрального оценивания, основанные на представлении сигнала как результата прохождения белого шума через цифровой фильтр. При вычислении оценок параметров модели используется система уравнений Юла-Уолкера, коэффициентами которой являются отсчеты автокорреляционной функции (АКФ) анализируемого сигнала:

$$\begin{bmatrix} r_{xx}[0] & r_{xx}[-1] & \cdots & r_{xx}[-p] \\ r_{xx}[1] & r_{xx}[0] & \cdots & r_{xx}[-p+1] \\ \vdots & \vdots & \ddots & \vdots \\ r_{xx}[p] & r_{xx}[p-1] & \cdots & r_{xx}[0] \end{bmatrix} \begin{bmatrix} 1 \\ a[1] \\ \vdots \\ a[p] \end{bmatrix} = \begin{bmatrix} \rho_\omega \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \quad (1)$$

где

$$r_{xx}[m] = \frac{1}{N-m} \sum_{i=0}^{N-m-1} x_i \cdot x_{i+m}\,, \quad (2)$$

Оценивание АКФ согласно формуле (2) требует значительного объема вычислений, пропорционального квадрату числа отсчетов сигнала N.

В [2] был предложен метод вычисление АКФ на основе быстрого преобразования Фурье, что позволяет значительно уменьшить объем вычислений при больших N. Однако, это приводит к определенным вычислительным неудобствам, так как при расчете ДПФ необходимо проведение операций с комплексными иррациональными числами. Кроме того, в ходе вычислений неизбежно накапливается ошибка при округлении и переполнении разрядной сетки.

Поэтому в [2] были разработаны теоретико-числовые преобразования (ТЧП), в которых вычисления производятся над конечным полем $GF(p)$, то есть по модулю простого числа p.

ТЧП последовательности x_i, $i = 0 \ldots N-1$ определяется как

$$X_k = \sum_{i=0}^{N-1} x_i \cdot g^{ik} \pmod p\,, \quad (3)$$

где g – первообразный корень, который выбирается так, чтобы

выполнялось условие:

$$g^N = 1 (\mathrm{mod}\ p), \qquad (4)$$

Были проведены поиски модулей p, удобных с точки зрения реализации ТЧП. Наиболее подходящими оказались преобразования по модулям чисел Ферма $2^{2^m}+1$ и Мерсенна $2^q - 1$ (q – простое) [2]. Однако, известно небольшое количество простых чисел Ферма и Мерсенна, поэтому был проведен поиск простых модулей $p = 3 \cdot 2^n + 1$, известных как числа Голомба [3].

С вычислительной точки зрения, наиболее подходящими являются следующая последовательность модулей:

$M_1 = 3 \cdot 2^1 + 1 = 6 + 1 = 7$ $\qquad$ $M_{12} = 3 \cdot 2^{12} + 1 = 12288 + 1 = 12289$

$M_2 = 3 \cdot 2^2 + 1 = 12 + 1 = 13$ $\qquad$ $M_{18} = 3 \cdot 2^{18} + 1 = 786432 + 1 = 786433$

$M_5 = 3 \cdot 2^5 + 1 = 96 + 1 = 97$ $\qquad$ $M_{30} = 3 \cdot 2^{30} + 1 = 3221225472 + 1 = 3221225473$

$M_6 = 3 \cdot 2^6 + 1 = 192 + 1 = 193$ $\qquad$ $M_{36} = 3 \cdot 2^{36} + 1 = 68719476736 + 1 = 68719476737$

$M_8 = 3 \cdot 2^8 + 1 = 768 + 1 = 769$ $\qquad$ $M_{41} = 3 \cdot 2^{41} + 1 = 2199023255552 + 1 = 2199023255553$

Такие модули, с одной стороны, позволяют применять эффективные алгоритмы быстрых преобразований, с другой – упрощают вычисление арифметических операций.

Также был проведен поиск минимального значения g для заданных модуля p и длины последовательности N. В табл.1 приведены несколько простых модулей вида $p = 3 \cdot 2^n + 1$, меньшие $3 \cdot 2^{20}$ и соответствующие им $256 \le N \le 262144$ и g.

Таблица 1 – Простые модули для размерностей ТЧП с быстрыми алгоритмами

N	p	g	N	p	g
256	769	7	2048	786433	19
256	12289	9	4096	12289	41
512	12289	3	4096	786433	14
512	786433	724	16384	786433	43
1024	12289	49	65536	786433	3
1024	786433	361	131072	786433	8
2048	12289	7	262144	786433	5

Список литературы

1. Марпл.-мл. С.Л. Цифровой спектральный анализ и его приложения. – М.: Мир, 1990. – 584 с.

2. Рабинер Л., Гоулд Б. Теория и применение цифровой обработки сигналов. – М.: Мир, 1990. – 850 с.

3. Чернов В.М. Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований. – М.: ФИЗМАТЛИТ, 2007. – 264 с.