МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«САМАРСКИЙ ГОСУДАРСТВЕННЫЙ АЭРОКОСМИЧЕСКИЙ
УНИВЕРСИТЕТ имени академика С.П.КОРОЛЕВА
(НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ)»

В.М. Чернов, А.О. Корепанов

Теоретико-числовые преобразования в задачах цифровой обработки сигналов

Электронное учебное пособие

САМАРА
2010

ŋqdqɐeɎ bɆ dədɆbɎзə d ɕɔɑbɔɐ Ɉqddɏqɐè

Авторы: ЧЕРНОВ Владимир Михайлович,
КОРЕПАНОВ Андрей Олегович

Содержание пособия относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел).

Специалисты в области анализа и обработки цифровой информации давно и успешно используют алгебраические и теоретико-числовые методы, прежде всего в таких областях, как криптография, корректирующие коды, синтез быстрых алгоритмов дискретных ортогональных преобразований. Несмотря на это, существует относительно мало доступной монографической литературы, охватывающей не только одну или несколько из указанных уже традиционных областей применения методов абстрактной алгебры и теории чисел к решению задач информатики, но и рассматривающей относительно новые приложения указанных математических методов и теорий к решению перспективных задач анализа цифровых сигналов. Ряд монографий отечественных или зарубежных авторов давно уже стал библиографической редкостью, а книги, изданные за рубежом, практически недоступны широкому кругу специалистов. Данное пособие ставит своей целью частичное восполнение указанного пробела.

Пособие предназначено для магистров направления 010400.68 “Прикладная математика и информатика”, обучающихся по программе «Математические и компьютерные методы обработки изображений и геоинформатики».

ВВЕДЕНИЕ

При вычислении свертки двух N-периодических последовательностей спектральным методом с помощью теоремы о свертке (см., например, [1], [2]) и использовании дискретного преобразования Фурье значения сворачиваемых последовательностей считаются, как правило, принадлежащими полю рациональных чисел $\mathbf{Q}$ (естественное "пользовательское" допущение) или, после соответствующего масштабирования, принадлежащими кольцу целых чисел $\mathbf{Z}$. В то же время значения базисных функций дискретного преобразования Фурье принадлежит полю комплексных чисел $\mathbf{C}$ - алгебраическому расширению $\mathbf{R}(i)$ поля $\mathbf{R}$ с индуцированной метрикой, связанной с обычным понятием модуля комплексного числа, которое, в свою очередь, является пополнением поля $\mathbf{Q}$ относительно метрики, связанной с абсолютной величиной числа. Таким образом, поле $\mathbf{Q}$ вкладывается в полное поле $\mathbf{C}$, причем при реализации на ЭВМ в силу конечноразрядного представления чисел вычисление преобразования (1.2) производится в $\mathbf{Q}(i)$, что приводит к погрешности, часто весьма значительной.

Для ряда задач цифровой обработки сигналов (задач криптографии, задачи умножения больших целых чисел, в частности) *принципиально* не допускается "приближенный" ответ. Либо точный, либо – не ответ. Паллиативным решением в этом случае является использование вместо дискретного преобразования Фурье его "модулярных аналогов" – теоретико-числовых преобразований (ТЧП, преобразований Фурье-Галуа).

Модулярные вычисления можно интерпретировать как "приближенные вычисления" в некоторой алгебраической структуре, причем эта "приближенность" характеризуется делимостью "погрешности" на простое число p.

Одной из целей данного пособия является метрическая формализация вышеприведенной интерпретации, что позволило бы с единой точки зрения проанализировать, как и особенности спектральных методов вычисления свертки, так и экстраполировать эти спектральные методы для вложений поля $\mathbf{Q}$ в его пополнения относительно других, так называемых неархимедовых, метрик поля $\mathbf{Q}$. Реализация программы для тех или иных конкретных метрик позволит с единой точки зрения анализировать точность как известных алгоритмов (ДПФ, преобразование Фурье-Галуа), так и позволит увеличить точность вычисления свертки даже при относительно скромных вычислительных возможностях.