Министерство образования Республики Беларусь
Учреждение образования
Белорусский государственный университет
информатики и радиоэлектроники

УДК 004.046

Авдеева
Галина Андреевна

Вычисление свертки с применением конечных полей

АВТОРЕФЕРАТ
на соискание степени магистра технических наук
по специальности 1-40 80 01 «Элементы и устройства вычислительной техники и систем управления»

Научный руководитель
Качинский Михаил Вячеславович
Доцент, кандидат технических наук

Минск 2019

ВВЕДЕНИЕ

В связи с ростом объемов глобальных коммуникаций проблемы хранения и эффективной передачи информации становятся все более актуальными. На сегодняшний день большую роль играет цифровая обработка информации, а именно фильтрация, механизм действия которой базируется на вычислении свертки входного сигнала и импульсной характеристики фильтра.

В настоящее время существует целый ряд алгоритмов, нацеленных на вычислении свертки с применением конечных полей. Однако даже при использовании современных методов вычисления свертки по-прежнему актуальными являются исследования, результаты которых позволяют как повысить точность известных методов расчета свертки, так и получить новые алгоритмы вычисления, которые могут быть успешно использованы при реализации цифровых фильтров.

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

Так как все больше растут объемы глобальных коммуникаций, вопросы хранения и эффективной передачи информации становятся все более актуальными. На сегодняшний день существенную роль играет цифровая обработка информации, а именно фильтрация, основанная на вычислении свертки входного сигнала и импульсной характеристики фильтра.

В то же время в ряде криптографических задач на одном из этапов алгоритма появляется необходимость перемножения двух чисел с величинами, которые превышают границы, возможные для аппаратной реализации операций на базе современных устройств. Такие числа могут быть рассмотрены в качестве значения соответствующих полиномов в точке, равной основанию системы счисления.

Недостаток применения дискретного преобразования Фурье состоит в том, что значения базисных функций – это иррациональные числа. Поэтому в связи с конечностью разрядной сетки вычислительной машины при вычислениях они могут быть представлены только с ограниченной точностью.

Существует круг задач, в которых потеря точности недопустима, что обуславливает необходимость использования вместо дискретного преобразования Фурье его модулярного аналога – теоретико-числового

преобразования. Также в данной работе предлагается реализация цифрового фильтра в полях Галуа.

Цель и задачи исследования

Целью данного исследования является разработка алгоритма вычисления свертки с применением конечных полей.

В соответствии с поставленной целью, в работе сформулированы и решены следующие задачи:

1. Провести анализ существующих методов вычисления свертки с применением конечных полей.
2. Разработать метод вычисления свертки с применением конечных полей с помощью теоретико-числового преобразования.
3. Реализовать цифровой фильтр с применением конечных полей

Объектом исследования выступает свертка в цифровой обработке сигналов.

Предметами исследования является метод вычисления свертки с применением конечных полей и способ реализации соответствующего цифрового фильтра.

Область исследования и содержание диссертационной работы соответствует образовательному стандарту высшего образования второй ступени (магистратуры) специальности 1-40 80 01 «Элементы и устройства вычислительной техники и систем управления».

Научная новизна диссертационной работы заключается в реализации вычисления свертки с применением теоретико-числовых преобразований. В данной работе предлагается расширить класс чисел, порождающих модулярные кольца с сохранением преимуществ арифметики с использованием чисел Мерсена и Ферма, в которых операция умножения реализуется с помощью циклических сдвигов. Предлагаемый метод основывается на представлении канонических систем счисления. Реализация цифрового фильтра в конечных полях позволяет существенно сэкономить аппаратные ресурсы и разработать фильтры с усовершенствованными характеристиками.

Положения, выносимые на защиту

1. Алгоритм вычисления свертки с помощью теоретико-числовых преобразований, основанный на представлении канонических систем

счисления.

2. Реализация КИХ-фильтра с применением конечных полей

Апробация результатов диссертации

Основные положения и результаты диссертационной работы докладывались и обсуждались на 55-й научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, 2019).

Опубликованность результатов исследования

По результатам исследований, представленных в диссертации, опубликована 1 печатная работа, а именно 1 тезис в сборниках и материалах научных конференций.

Структура и объем диссертации

Структура диссертационной работы обусловлена целью, задачами и логикой исследования. Работа состоит из введения, четырёх глав и заключения, библиографического списка и приложений. Общий объем диссертации − 76 страниц. Работа содержит 1 таблицу, 26 рисунков. Библиографический список включает 31 наименование, графический материал включает 10 слайдов презентации.

СОДЕРЖАНИЕ РАБОТЫ

Во **введении** рассмотрено современное состояние проблемы вычисления свертки сигналов, определены основные направления исследований, а также дается обоснование актуальности темы диссертационной работы.

В **общей характеристике работы** сформулированы ее цель и задачи, показана связь с научными программами и проектами, даны сведения об объекте исследования и обоснован его выбор, представлены положения, выносимые на защиту, приведены сведения о личном вкладе соискателя, апробации результатов диссертации и их опубликованность, а также, структура и объем диссертации.

В **первой главе** рассматриваются понятие свёртки, ее определение с точки зрения частотных характеристик, графическое представление свертки, проанализированы два вида дискретных сверток: линейная и циклическая, установлена связь между ними. Также было показано, что применение быстрого преобразования Фурье обеспечивает существенное уменьшение вычислительных операций при вычислении как циклических, так и линейных сверток.

Свертка – это одна из наиболее используемых операций в цифровой обработке сигналов (ЦОС). Это также основная операция в цифровой фильтрации.

Значение свертки станет очевидным, если рассматривать ее в частотных координатах и иметь в виду то, что свертка во временной области равносильна умножению в частотной области. Свертка, помимо всего прочего, описывает, как выходная последовательность системы определяется взаимодействием входа с этой системой. Чаще всего выход системы – это запаздывающая и подавленная или усиленная версия входа. Поэтому особенно эффективно рассмотреть выход системы, порожденный импульсным входом. Так как любой вход можно представить в качестве последовательности импульсов разной мощности. Таким образом, выход системы, порождающий импульсный вход, не будет соответствующим ему импульсом, а будет меняться во временной области, в какой-то момент достигая максимального значения. В момент приема выборки m выходная характеристика, порожденная единичным импульсом, поданным в момент 0, равна $h(m)$. Такая величина называется импульсной характеристикой системы или, по-другому, ее импульсным откликом.

Данное понятие можно расширить на свертку любых двух массивов данных и рассматривать термин шире. Если сигналы поддаются определенному

математическому описанию, свертку можно выполнить аналитически.

Свертка имеет некоторые свойства:

1) закон коммутативности;
2) закон дистрибутивности;
3) закон ассоциативности.

В дискретном случае различают два вида сверток: линейную (или апериодическую) и циклическую. Циклическую свертку еще часто называют круговой или периодической.

Спектр циклической свертки есть произведение спектров сворачиваемых сигналов, и для ее вычисления может быть применен алгоритм быстрого преобразования Фурье (БПФ).

Во **второй главе** было определено понятие конечного поля, рассмотрено пять аксиом конечного поля, изучено его построение на основе примера, выявлены основные свойства полей Галуа. Также рассмотрена китайская теорема об остатках и определена выгода ее использования в случае вычислений больших объемов.

Полем F называют коммутативное кольцо с единицей, в котором каждый ненулевой элемент имеет мультипликативный обратный элемент. Число элементов поля называется порядком поля.

Весьма важное значение имеют поля, образованные конечным множеством элементов – так называемые конечные поля Галуа (Galois Field), обозначаемые GF.

Конечным полем GF называется конечное множество элементов, замкнутое по отношению к двум заданным в нем операциям комбинирования элементов. Под замкнутостью понимается тот факт, что результаты операций не выходят за пределы конечного множества введенных элементов. Для конечных полей выполняются следующие аксиомы:

GF.1 Из введенных операций над элементами поля одна называется сложением и обозначается как $a + b$, а другая – умножением и обозначается как ab.

GF.2 Для любого элемента a существует обратный элемент по сложению $(-a)$ и обратный элемент по умножению a^{-1} (если $a \neq 0$) такие, что $a + (-a) = 0$ и $a \cdot a^{-1} = 1$. Наличие обратных элементов позволяет наряду с операциями сложения и умножения выполнять также вычитание и деление. Поэтому иногда просто говорят, что в поле определены все четыре арифметические операции (кроме деления на 0).

GF.3 Поле всегда содержит мультипликативную единицу *1* и аддитивную единицу *0*, такие что $a + 0 = a$, и $a \cdot 1 = a$ для любого элемента поля.

GF.4 Для введенных операций выполняются обычные правила ассоциативности $a + (b + c) = (a + b) + c$, коммутативности $a(bc) = (ab)c$, и дистрибутивности $a(b + c) = ab + ac$.

GF.5 Результатом сложения или умножения двух элементов поля является третий элемент из того же конечного множества.

Конечные поля существуют не при любом числе элементов, а только в том случае, если их количество – простое число p или его степень p^m, где m – целое. В первом случае поле *GF(p)* называется простым, а во втором – расширением $GF(p^m)$ простого поля.

В теории конечных полей доказывается, что все поля $GF(2^m)$ одного порядка p изоморфны («подобны по форме»), т.е. между $GF_1(2^m)$ и $GF_2(2^m)$ существует взаимнооднозначное отображение f друг на друга, сохраняющее операции сложения и умножения.

Любое неотрицательное целое число, не превосходящее произведения модулей, можно однозначно восстановить, если известны его вычеты по этим модулям. Этот результат был известен еще в Древнем Китае и носит название китайской теоремы об остатках.

Вообще переход к системе вычетов позволяет разбить целые числа на маленькие кусочки, которые легко складывать, вычитать и умножать. Если вычисления состоят только из этих операций, то такое представление является альтернативной арифметической системой. Если вычисления достаточно просты, то переход от естественной записи целых чисел к записи через систему остатков и обратное восстановление ответа в целочисленном виде могут свести на нет все возможные преимущества при вычислениях. В случаях же, когда объем вычислений достаточно велик, такой переход может оказаться выгодным.

В **третьей главе** был рассмотрен алгоритм вычисления БПФ с применением конечных полей, реализованы алгоритмы вычисления свертки длины $N = p$, $N = p^k$ и алгоритм вычисления свертки помощью ТЧП.

Преобразование Фурье в конечном поле обладает почти такими же свойствами, что и преобразование Фурье в комплексном поле. Однако преобразование Фурье длины блока n существует в $GF(p)$, только если n делится на $q - 1$. Это означает, что длина блока в преобразовании Фурье с применением конечных полей ограничена выбором поля, тогда как длина блока в преобразовании Фурье над комплексным полем является произвольной. Быстрыми алгоритмами вычисления преобразований Фурье в

полях Галуа являются алгоритм Кули-Тьюки со смешанным основанием, алгоритм Гуда-Томаса и алгоритм Винограда. Эти алгоритмы подходят для любого поля, включая поля Галуа.

Линейная свертка длины N может быть вычислена одним умножением и двумя линейными свертками длины $p-1$. Этот процесс может применяться многократно, пока не останутся только линейные свертки с длиной равной двум. Тогда для вычисления понадобится три операции умножения для каждой. Многомерные методы Бурруса могут быть использованы для построения алгоритмов свертки длины $N = p^k$. Одномерные последовательности могут быть преобразованы в многомерные. Количество умножений для вычисления таких сверток рассчитывается по специально выведенной формуле. Второй метод вычисления циклической свертки длины $N = p^k$ состоит в добавлении $N-1$ сложений в алгоритмы вычисления линейной свертки длины $N = p^k$для модуля редукции $z^n - 1$. Этот алгоритм может быть преобразован в новый с помощью тензорного транспонирования.

Недостатком применения дискретного преобразования Фурье в вычислении свертки можно назвать то, что при вычислении такие алгоритмы могут быть реализованы с ограниченной точностью. Есть круг задач, где потеря точности недопустима, следовательно, необходимо использовать вместо ДПФ его аналога – теоретико-числового преобразования.

Предлагаемый алгоритм, основан на вычислении свертки без использования умножений. Поэтому алгоритм является эффективным и при прямой реализации вычисления свертки, в частности, в случае, когда длина свертки является простым числом.

В **четвертой главе** реализован КИХ-фильтр и представлены результаты экспериментальных исследований.

Была проиллюстрирована структурная схема данного КИХ-фильтра, разработана его реализация, проанализированы амплитудно-частотная характеристика (АЧХ) и выходные характеристики системы. Выявлены достоинства такой реализации: независимость каналов, адаптированность к перепроектировке FPGA, уменьшение потребляемой мощности.

Анализ АЧХ показал превосходство в точности реализации нерекурсивного фильтра в полях Галуа над фильтром без применения коенчных полей.

Сравнительный анализ выходных характеристик модулярного и позиционного фильтров доказал верность проводимых вычислений.

В **приложениях** представлены ответ проверки на плагиат, графический материал и исходное описание разработанной системы на языке C++.

ЗАКЛЮЧЕНИЕ

В настоящей работе было проведено исследование методов вычисления дискретной свертки с применением конечных полей.

В результате был разработан алгоритм вычисления свертки в конечных полях с помощью теоретико-числового преобразования в канонических системах счисления. Предлагаемый алгоритм, основан на реализации свертки без использования умножений. Поэтому алгоритм является эффективным и при прямой реализации вычисления свертки, и в случае, когда длина свертки является простым числом.

Предложенная методика позволяет расширить класс используемых чисел для вычисления свертки с применением ТЧП. Реализация алгоритма и возможная его оптимизация зависят от длины вычисляемой свертки. В работе рассмотрены бинарные системы счисления в полях алгебраических чисел высоких степеней.

Также был реализован КИХ-фильтр в конечных полях. Достоинства такого подхода достигаются благодаря замене умножителей и сумматоров эквивалентными схемами, которые при определенных условиях позволяют существенно сэкономить аппаратные ресурсы и реализовать фильтры с улучшенными параметрами. Оптимизация структуры КИХ-фильтра в алгебре поля конечных вычетов за счет уменьшения длины его импульсного отклика в 1,94 раза обеспечивает почти вдвое сокращение затрат на оборудование на количество единиц по сравнению с традиционными фильтрами. Основным показателем качества работы фильтра является то, что его частотная характеристика имеет более высокую прямоугольность по сравнению с позиционными фильтрами и, следовательно, имеет лучшую селективность. В этих условиях предлагаемая структура фильтра обладает лучшими характеристиками, чем уже существующие решения. Кроме того, разработанная структура имеет ряд неоспоримых преимуществ:

1) все каналы независимы по каждому модулю;

2) реализация таких устройств на основе FPGA легко поддается перепроектировке;

3) каналы трассировки распространяются исключительно внутри вычислительного канала, следовательно, уменьшается потребляемая мощность.

СПИСОК ОПУБЛИКОВАННЫХ РАБОТ

[1] Авдеева, Г. А. Реализация фильтров в конечных полях / Г. А. Авдеева // Компьютерные системы и сети: 55-я юбилейная научная конференция аспирантов, магистрантов и студентов, Минск, 22-26 апреля 2019 г. / Белорусский государственный университет информатики и радиоэлектроники. – Минск. – 2019. – С. 246 – 247.