МАТЕМАТИКА. ПРИКЛАДНАЯ МАТЕМАТИКА

АРИФМЕТИЧЕСКИЕ МЕТОДЫ

СИНТЕЗА БЫСТРЫХ АЛГОРИТМОВ ДИСКРЕТНЫХ ОРТОГОНАЛЬНЫХ ПРЕОБРАЗОВАНИЙ

В.М. ЧЕРНОВ

Чернов В.М.

Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований

МОСКВА
ФИЗМАТЛИТ ®

УДК 519.72, 512.547
511.334
ББК 32.81, 22.132
Ч 49

Чернов В. М. **Арифметические методы синтеза быстрых алгоритмов дискретных ортогональных преобразований.** — М.: ФИЗМАТЛИТ, 2007. — 264 с. — ISBN 978-5-9221-0940-6.

Содержание книги относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел). Результаты, изложенные в книге, затрагивают наиболее сложные, фундаментальные вопросы теории синтеза так называемых быстрых алгоритмов дискретных ортогональных преобразований и разработки на их основе эффективных методов анализа дискретной информации

Для специалистов в области цифровой обработки сигналов и изображений, в области прикладной математики, а также для студентов и аспирантов соответствующих специальностей.

ISBN 978-5-9221-0940-6

© ФИЗМАТЛИТ, 2007
© В. М. Чернов, 2007

ОГЛАВЛЕНИЕ

Предисловие 8

Введение 10

Глава 1. **Модулярная арифметика и быстрое «безошибочное» вычисление свертки** 15

1.1. Постановка задачи, основные идеи 15
1.1.1. Теоретико-числовые преобразования и целочисленные свертки (15).

1.2. Реализация арифметических операций для модулей специального вида 18
1.2.1. Арифметика в полях по модулю числа Мерсенна (18). 1.2.2. Арифметика в полях по модулю числа Ферма. (19). 1.2.3. Арифметика в полях по модулю числа Голомба (20).

1.3. Редуцированные системы счисления в конечных полях 21
1.3.1. Двоично-избыточная система счисления (21). 1.3.2. Редуцированные системы счисления в комплексном поле Мерсенна (23).

1.4. Алгоритмы вычисления свертки в полях p-адических чисел 26
1.4.1. p-адические числа (26). 1.4.2. Вычисление свертки с помощью ТЧП по модулю степени простого числа (28). 1.4.3. Реализация арифметических операций в кольце классов вычетов по модулю степени числа Мерсенна (30). 1.4.4. Реализация арифметических операций в кольце классов вычетов по модулю степени числа Ферма (30).

1.5. Алгоритмы вычисления свертки в расширениях неархимедово нормированных полей 31
1.5.1. Продолжение p-адических нормирований на квадратичные расширения поля Q (31). 1.5.2. Метрическая форма китайской теоремы об остатках (32). 1.5.3. Случай $\mathsf{Q}(\sqrt{d})$, d-невычет $(\mathrm{mod}\ p)$ (33). 1.5.4. Случай $\mathsf{Q}(\sqrt{d})$, d-вычет $(\mathrm{mod}\ p)$ (34).

1.6. Приложения аппроксимационной теоремы 35
1.6.1. Параллельные алгоритмы вычисления свертки: случай неархимедово нормированных полей (35). 1.6.2. Параллельные алгоритмы вычисления свертки: случай архимедово и неархимедово нормированных полей (35).

Комментарии к главе 1 36

Литература к главе 1 37

Глава 2. **Рекуррентные системы счисления и дискретные ортогональные преобразования с рекуррентным базисом** 39

2.1. Постановка задачи, основные идеи 39

2.2. Вспомогательные сведения, примеры 42
2.2.1. Рекуррентные системы счисления высших порядков (42). 2.2.2. Рекуррентные системы счисления с иррациональным основанием (44). 2.2.3. Дискретное преобразование Фибоначчи (45).

2.3. Квазитреугольные дискретные ортогональные преобразования . . . 47
2.3.1. Основные определения (47). 2.3.2. Регулярный случай реализации КТП без умножений (49). 2.3.3. Сингулярный случай реализации КТП без умножений: $q = 0$, $\omega = \sqrt{2}$ (50). 2.3.4. Быстрые алгоритмы КТП (51).

2.4. Теоретико-числовые преобразования и рекуррентные системы счисления 52
2.4.1. Постановка задачи, основные идеи (52).

2.5. Дискретное преобразование Люка–Мерсенна 54
2.5.1. Коды Люка–Мерсенна (54). 2.5.2. Дискретное преобразование Люка–Мерсенна (56). 2.5.3. Вычисление дискретной круговой свертки с помощью LMT (58).

2.6. Некоторые обобщения 59
2.6.1. Обобщение на квазимерсенновы модули (59). 2.6.2. Обобщение на случай рекуррентных систем счисления третьего порядка (61).

Комментарии к главе 2 61

Литература к главе 2 62

Глава 3. **Неоднозначность разложения на множители и параллельные алгоритмы вычисления свертки** 65

3.1. Введение, основные идеи. 65

3.2. Параллельные алгоритмы вычисления свертки по модулю составного числа Мерсенна 68
3.2.1. Альтернативное представление разложения (составных) чисел Мерсенна (68). 3.2.2. Вычисление свертки по модулю составного числа Мерсенна (72).

3.3. Параллельные алгоритмы вычисления свертки по модулю составного числа Ферма 75
3.3.1. Альтернативное разложение (составных) чисел Ферма (75). 3.3.2. Вычисление свертки по модулю составного числа Ферма (80).

Комментарии к главе 3 81

Литература к главе 3 82

Глава 4. **Канонические системы счисления в полях алгебраических чисел и параллельные алгоритмы вычисления свертки** . . . 84

4.1. Введение, основные идеи. 84
4.1.1. Требования, предъявляемые к системам счисления (84).

4.2. Предварительные сведения 86
4.2.1. Целые элементы в квадратичных полях (86). 4.2.2. «Канонические» системы счисления в квадратичных полях (86). 4.2.3. Примеры канонических систем счисления (89).
4.3. Параллельные алгоритмы вычисления свертки в «канонических» системах счисления для квадратичных полей 91
4.3.1. Параллельные алгоритмы вычисления свертки в РКСС с основанием $(i-1)$ (91). 4.3.2. Параллельные алгоритмы вычисления свертки в РКСС с основанием $\frac{1}{2}(-1 \pm i\sqrt{7})$ (95). 4.3.3. Параллельные алгоритмы вычисления свертки в РКСС с основанием $(\pm i\sqrt{2})$ (98).
4.4. Параллельные алгоритмы вычисления свертки в канонических системах счисления для расширений высоких степеней 102
Литература к главе 4 106

Глава 5. **Круговые поля и редукция Галуа дискретных ортогональных преобразований** 109
5.1. Постановка задачи, основная идея 109
5.2. Вспомогательные сведения из теории Галуа круговых полей 111
5.3. Дискретные ортогональные преобразования с базисами из периодов полей деления круга 116
5.4. Редукция Галуа дискретных преобразований, порожденных периодами круговых полей 120
5.4.1. Схема декомпозиции ДПГ типа Кули–Тьюки (120). 5.4.2. Редукция Галуа ДПГ (общий случай) (127). 5.4.3. Быстрые алгоритмы многомерных ДПФ, использующие редукцию Галуа (128).
5.5. Некоторые замечания об эффективности алгоритмов Рейдера–Винограда 132
Комментарии к главе 5 138
Литература к главе 5 139

Глава 6. **Гиперкомплексные алгебры и совмещенные алгоритмы дискретных ортогональных преобразований** 141
6.1. Постановка задачи, основная идея 141
6.2. Вспомогательные сведения 143
6.2.1. Общие принципы синтеза совмещенных алгоритмов (143). 6.2.2. Алгебра кватернионов (145). 6.2.3. Четырехмерная коммутативная гиперкомплексная алгебра (147). 6.2.4. Алгебры Клиффорда (150).
6.3. Примеры синтеза совмещенных БА многомерных ДПФ 152
6.3.1. Двумерные алгоритмы ДПФ с совмещением в алгебре кватернионов (152). 6.3.2. Алгоритмы многомерных ДПФ с совмещением в алгебрах Клиффорда (154).
6.4. Алгоритмы дискретных ортогональных преобразований, реализуемые в циклотомических кодах 156

6.4.1. Циклотомические коды (156). 6.4.2. Алгоритмы одномерных ДОП, реализуемые в циклотомических кодах (158). 6.4.3. Коды Гамильтона–Эйзенштейна (163). 6.4.4. Быстрый алгоритм двумерного ДПФ (166). 6.4.5. Быстрый алгоритм дискретного косинусного преобразования (168).

6.5. Совмещенное вычисление спектров многоканального изображения 170
6.5.1. Алгебра Гурвица (170). 6.5.2. Алгоритм совмещенного вычисления трех фурье-спектров цветного изображения (174).

6.6. Алгоритм ДПФ с «экстремальным» совмещением в групповой алгебре циклической группы 176
6.6.1. Некоторые свойства групповых алгебр циклических групп (176). 6.6.2. Быстрый алгоритм вспомогательного преобразования со значениями в групповой алгебре (179). 6.6.3. Быстрый алгоритм ДПФ с асимптотическим понижением порядка мультипликативной сложности (180). 6.6.4. Некоторые специальные случаи (182).

Комментарии к главе 6 186

Литература к главе 6 186

Глава 7. **Арифметические свойства значений тригонометрических функций и быстрые алгоритмы дискретного косинусного преобразования** 189

7.1. Постановка задачи, основные идеи 189

7.2. Сложность операции умножения в конечномерных алгебрах 192

7.3. Алгебраические принципы синтеза алгоритмов ДКП коротких длин 195
7.3.1. Дискретное косинусное преобразование длины 8 (195). 7.3.2. Связь между алгебраическими свойствами значений базисных функций ДКП и структурой матрицы преобразования (197).

7.4. Примеры алгоритмов ДКП с минимальной мультипликативной сложностью 200
7.4.1. Алгоритм ДКП длиной 9 (200). 7.4.2. Алгоритм ДКП длиной 10 (203). 7.4.3. Алгоритм ДКП длиной 12 (204). 7.4.4. Алгоритм ДКП длиной 15 (205).

7.5. Некоторые экспериментальные результаты 207

Комментарии к главе 7 208

Литература к главе 7 210

Глава 8. **Канонические системы счисления и многомерное обобщение количественной задачи Бореля** 212

8.1. Постановка задачи, основная идея 212

8.2. Предварительные сведения из теории рекуррентных функций в конечных полях 215
8.2.1. Показательные и рекуррентные функции в конечных полях (215). 8.2.2. Тригонометрические суммы и суммы характеров с показательными функциями (217).

8.3. Некоторые свойства пополнения алгебр $Q(\sqrt{d})$ 221

8.3.1. Фундаментальные области алгебр $\widetilde{Q}(\sqrt{d})$ (221). 8.3.2. Меры Хаара на алгебрах $\widetilde{Q}(\sqrt{d})$ (222).

8.4. Основная теорема о равномерном распределении в фундаментальных областях . . . 225

Комментарии к главе 8 . . . 231

Литература к главе 8 . . . 232

Глава 9. **Показательные функции в конечных полях и дискретные преобразования с «хаотическими» базисами** . . . 234

9.1. Постановка задачи, основная идея . . . 234

9.2. Одномерные M-преобразования . . . 235

9.2.1. «Хаотические» базисы с равномерным распределением значений (236). 9.2.2. «Хаотические» базисы с полиномиальным законом распределением значений (238). 9.2.3. Специальный случай: «хаотические» базисы, порожденные показательной функцией в конечном поле (247).

9.3. Двумерные преобразования с хаотическим базисом . . . 249

9.3.1. Синтез базисов двумерных хаотических преобразований (251). 9.3.2. Хаотичность последовательности значений базисных функций (255). 9.3.3. Некоторые практические рекомендации и результаты (257).

Комментарии к главе 9 . . . 258

Литература к главе 9 . . . 260

Предисловие

Моим Учителям:
Льву Павловичу Усольцеву
и Николаю Григорьевичу Чудакову

Содержание книги 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.

Данная книга ставит своей целью отчасти восполнить указанный пробел. Книга предназначается специалистам в области цифровой обработки сигналов и изображений, в области прикладной математики, а также для использования в учебном процессе — студентам и аспирантам по прикладной математике и информатике.

Автор не нашел слов более точных, чем прочитанных им в книге Г. Вейля «Классические группы, их инварианты и представления» [1]), которыми по мере возможностей руководствовался при написании этой книги.

«...предмет этой книги довольно специальный. Как бы важны ни были общие понятия и предложения, которыми одарило нас современное деятельное увлечение аксиоматизированием и обобщениями, распространенное в алгебре, быть может, большее, чем в какой бы ни было другой области, — все же я убежден в том, что именно специальные проблемы во всей их сложности составляют опору и стержень математики; и преодоление их трудностей требует, вообще говоря, наиболее серьезных усилий ⟨...⟩. Общие теории показаны здесь

[1]) Г. Вейль. «Классические группы, их инварианты и представления», М.: ИЛ, 1947.

в их возникновении из специальных проблем, анализ которых приводит к этим теориям как действенному инструменту решения, с почти принудительной необходимостью; но, однажды появившись, эти теории освещают широкую область за пределами ограниченного участка их возникновения. ⟨...⟩ Книга предназначена, главным образом, тем, кто скромно хочет узнать изложенные в ней новые вещи, а не тем гордым ученым, уже знакомым с предметом и желающим получить лишь быструю или точную справку о той или иной детали. Она не является ни элементарным учебником, ни монографией. В том же духе выдержаны ссылки на литературу».

Автор выражает глубокую признательность:

- академику РАН Ю. И. Журавлеву, без постоянного внимания которого к исследованиям автора эта книга никогда не была бы написана;
- Российской общественной организации «Ассоциация распознавания образов и анализа изображений» за плодотворное сотрудничество;
- члену-корреспонденту РАН В. А. Сойферу за постоянное внимание и помощь в работе;
- доктору физико-математических наук Н. Л. Казанскому за организационно-методическую помощь;
- всем сотрудникам лаборатории математических методов обработки изображений Института систем обработки изображений РАН (Зав. лабораторией — доктор технических наук В. В. Сергеев).

Книга базируется на оригинальных научных работах, опубликованных автором за последние 15 лет. Соавторами ряда работ были: М. В. Алиев, А. М. Белов, О. В. Бесполитов, А. Г. Дмитриев, А. Н. Калугин, Э. И. Коломиец, М. В. Першина, Н. В. Радченко, М. А. Чичева, А. В. Шабашев.

Основные результаты, представленные в книге, получены в ходе выполнения проектов РФФИ, руководителем которых являлся автор: №№ 95-01-00367, 97-01-00600, 00-01-00900, 03-01-00736. Непосредственно подготовка рукописи к печати осуществлялась по проекту Ц 0025 «Арифметические методы в задачах анализа многомерных сигналов» Федеральной целевой программы «Интеграция науки высшего образования России на 2002–2006 годы».

Введение

> Мне самому очень нравились эти вещи; но я никоим образом не был уверен в том, как их воспримут другие, и если кто-нибудь сказал «неплохо, но все же уж очень специальный вопрос», «не настоящая математика», я бы покорно согласился.
>
> *Дж. Литлвуд* [1])

Почему написана эта книга. Лет 15 назад автор, получивший ортодоксальное математическое образование, не помышлял не только о написании книги, но и вообще о своей работе в области обработки и анализа цифровых сигналов. Три события, произошедшие почти одновременно, заставили автора радикальным образом свое отношение к указанной проблематике. Это (в хронологическом порядке):

- знакомство с работами зарубежных исследователей (Аггарвал, Рейдер, Блейхут, Виноград и др.) в области теории синтеза быстрых алгоритмов, вызвавших некоторое недоумение автора: «А что, *это* раньше никто не смог сделать?»;
- знакомство с действительно пионерскими работами В. Г. Лабунца, использующих очень нетривиальную математику и опубликованных, к сожалению, в малотиражных межвузовских сборниках;
- и, наконец, знакомство с работами академика РАН Ю. И. Журавлева и его учеников, за кратчайшее время убедившее автора в возможности и необходимости рассмотрения алгоритмов как точек пространства (алгоритмов) с операциями, топологией, отношениями и т. д., причем, не просто точек, а точек с их окрестностями, в которые «проецируются» идеи и методы тех или иных математических теорий, в том числе и самых нетривиальных.

Последнее полностью сформировала у автора потребность пересмотра своих взглядов на математику вообще, а последующая работа убедила в правильности принятого решения.

Название книги достаточно полно отражает ее направленность. Автор предпочел «неавторитетный» термин «арифметические методы», хотя правильнее говорить о методах алгебраических. Но, во-первых, термин «алгебраические методы» применительно к проблемам синтеза быстрых алгоритмов дискретных преобразований, уже используется как метод поиска различных факторизационных тождеств для матриц преобразований. Во-вторых, автор желал подчеркнуть, что основное внимание в книге уделяется не столько структурным аспектам теории тех алгебраических структур, которые «естественным образом» ассо-

---

[1]) Дж. Литлвуд. «Математическая смесь», М.: Наука, 1978.

циированы с дискретными ортогональными преобразованиями и быстрыми алгоритмами их вычислений, сколько аспектам именно *арифметическим*, относящимся к сложности реализации операций в этих структурах.

Названия глав. Названия имеют унифицированную структуру, а именно «**Математическая теория и Прикладная задача**».

Главенствующую роль в содержании глав играют не столько математическая теория и/или прикладная задача сами по себе, сколько их взаимосвязь. Автор руководствовался тезисом: «Если какая-то математическая теория первоначально развивалась классиками для иных целей, если какая-то прикладная задача решалась другими методами; то давайте покажем что «нетрадиционное» для математиков использование математического аппарата может привести к результатам, «неожиданным» для специалистов в области цифровой обработки сигналов».

Кому не адресована книга. Автор не советует читать книгу «ортодоксальным», математикам, так как в чисто математическом плане они найдут в ней только хорошо известные им факты в приложении к специфическим задачам цифровой обработки сигналов. Как неоднократно убеждался автор, большинству математиков эти задачи неинтересны. Точно также автор не ориентировался на читателя — столь же ортодоксального «компьютерщика», предпочитающего в качестве средств решений прикладных задач исключительно компьютерные эксперименты и эвристические решения.

Отбор материала. Автор руководствовался исключительно своими личными вкусами и научными интересами. Это, в первую очередь, быстрые алгоритмы дискретных ортогональных преобразований. Кроме того, на отбор материала существенно повлияла результативность автора в решении тех или иных прикладных задач. Именно поэтому в книге не рассматриваются вопросы, связанные с алгебраическими кодами, вейвлетами, криптографией и т. п., несмотря на достаточно ясные перспективы приложений методов, рассматриваемых в книге, к задачам подобного рода.

Требования к математической подготовке читателя. Эти требования монотонно возрастают, достигают максимума в гл. 5 (необходимо минимальное знакомство с теорией Галуа круговых полей хотя бы в объеме соответствующей главы книги Б. Л. ван дер Вардена «Алгебра»), затем снова несколько снижаются. Автор изначально предполагает знакомство читателя со стандартным университетским курсом алгебры и поэтому отказался от главы, в которой были бы сконцентрированы необходимые теоретические сведения из алгебры и теории чисел. Более специальные вопросы включены в соответствующие главы книги. Тем не менее, в большинстве глав имеются достаточно длинные выкладки, с которыми желательно знакомиться с карандашом в руках (или пропустить вовсе).

Эклектика. Автор пытался, с одной стороны, сделать главы максимально независимыми и свободными от перекрестных ссылок (отсюда

повторы, дублирование основных формул и т. п.), а, с другой стороны, охватить содержанием как можно более широкий спектр *математических идей и методов*, которые с успехом можно применить к задачам синтеза быстрых алгоритмов дискретных ортогональных преобразований. Тем не менее, два математических понятия проходят «красной нитью» сквозь всё содержание книги: понятие позиционной (рекуррентной) системы счисления и понятие нормированного поля, в том числе и неархимедово нормированного.

Цитированная литература. Библиографический список не претендует на полноту. Необходимым (но не достаточным) условием включения работы X в список литературы являлось истинность высказывания

$$(P(X)\,\&Q(X)) \vee R(X) \vee S(X),$$

где

$P(X)$ истинно тогда и только тогда, когда автор, по крайней мере, держал работу X в руках;

$Q(X)$ истинно тогда и только тогда, когда работа X понравилась автору;

$R(X)$ истинно тогда и только тогда, когда X — пионерская работа, на которую все ссылаются; $S(X)$ истинно тогда и только тогда, когда автор сам написал работу X.

В случаях, когда тот или иной факт достаточным образом освещен в монографической литературе, предпочтение отдалось не оригинальной работе, а ее изложению в доступных монографиях.

Содержание книги. Как уже отмечалось, содержание книги относится к пограничной области между информатикой (теория и практика анализа и обработки многомерных цифровых сигналов) и математикой (абстрактная алгебра и теория чисел). Несмотря на явную прикладную направленность описанных в книге методов и алгоритмов, результаты, включенные в нее, затрагивают наиболее сложные, фундаментальные аспекты теории синтеза так называемых быстрых алгоритмов дискретных ортогональных преобразований и разработки на их основе эффективных методов анализа дискретной информации.

Как ни парадоксально, но существует относительно мало монографической литературы, доступной российскому читателю, в которой рассматривались бы не только традиционные области применения методов алгебры и теории чисел к решению задач информатики, но и 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 (например, Н. В. Вариченко, В. Г. Лабунец, М. А. Раков «Абстрактные алгебраические системы и цифровая обработка сигналов», Киев, «Наукова думка», 1986; Д. Х. Маккеллан, Ч. М. Рейдер «Применение теории чисел в цифровой обработке сигналов», М., «Радио и связь», 1983, и др.), а книги, изданные за

рубежом (например, R. Tolmieri, Myong An, Chao Lu «Algorithms for discrete Fourier transform and convolution», Springer, 1997; R.Tolmieri, Myong An, Chao Lu «Mathematics of multidimensional Fourier transform algorithms», Springer, 1997), практически недоступны широкому кругу специалистов.

Основное внимание в книге уделяется алгебро-арифметическим методам синтеза быстрых алгоритмов дискретных преобразований. Отметим, что историю быстрых алгоритмов (БА) дискретных ортогональных преобразований (ДОП) принято отсчитывать с 1965 г., когда Кули и Тьюки опубликовали свой быстрый алгоритм вычисления дискретного преобразования Фурье. За время, прошедшее с первых публикаций, дискретный спектральный анализ стал одним из основных средств решения задач цифровой обработки сигналов, распознавания образов, машинного зрения, компьютерной оптики и т. д.

Несмотря на то, что за сорокалетнюю историю развития БА ДОП неоднократно предпринимались попытки построения на единой концептуальной основе теории синтеза быстрых алгоритмов, унифицированный конструктивный подход к этой проблеме до последнего времени не был еще разработан. Наиболее известными общими подходами считались метод кронекеровской факторизации матриц ДОП и метод полиномиальных преобразований. Отсутствие общих теорем о кронекеровской факторизации ограничивал возможности первого из них, по существу, классификацией алгоритмов, синтезированных независимыми методами. Метод полиномиальных преобразований существенно опирался на наличие априорной информации о факторизации циклотомических полиномов и на использование индивидуальных арифметических свойств коэффициентов полиномиальных сомножителей. Разработка унифицированного подхода к синтезу быстрых алгоритмов, при котором основным предметом исследования являлся бы алгоритм, а не дискретное преобразование, представлялось до последнего времени малоисследованным аспектом теории сложности алгоритмов дискретных ортогональных преобразований.

В работах автора предложен алгебро-арифметический конструктивный подход к синтезу быстрых алгоритмов достаточно общего класса дискретных ортогональных преобразований. Методологической основой этого подхода является трехэтапная процедура синтеза быстрых алгоритмов ДОП:

а) вложение поля, содержащего значения входных сигналов и базисных функций преобразований в некоторую топологическую алгебру;

б) вычисление вспомогательного ассоциированного преобразования со значениями в этой алгебре;

в) отображение полученного результата в поле, содержащее значения выходного сигнала.

Параметры, характеризующие выбранную алгебраическую структуру, способ вложения данных, принцип интерпретации значений вспомогательного преобразования определяют структуру алгоритмов и, тем

самым, параметризуют обширный класс этих алгоритмов. Принятая концепция описания алгоритмов определяет тематическую направленность отдельных глав, а именно:

1) исследование влияния *структурных свойств* вспомогательной алгебры (размерность, базис, свойства основного поля) на вычислительные характеристики алгоритмов;
2) исследование вычислительных характеристик алгоритмов, определяемых *алгебраичностью значений* параметров алгоритмов;
3) исследование связи вычислительных характеристик алгоритмов с *арифметическими свойствами систем счисления*, в которых представлены обрабатываемые данные.

Глава 1

МОДУЛЯРНАЯ АРИФМЕТИКА И БЫСТРОЕ «БЕЗОШИБОЧНОЕ» ВЫЧИСЛЕНИЕ СВЕРТКИ

Реальный мир полон отвратительных чисел типа 0,79134989..., мир же компьютеров имеет дело с милыми числами типа 0 и 1.

Дж. Конвей, Н. Слоэн [1)]

1.1. Постановка задачи, основные идеи

1.1.1. Теоретико-числовые преобразования и целочисленные свертки. При вычислении свертки двух N-периодических последовательностей,

$$(x * y)(k) = z(k) = \sum_{n=0}^{N-1} x(n)\, y(k-n), \quad k = 0, \ldots, N-1, \tag{1.1}$$

спектральным методом с помощью теоремы о свертке (см., например, [1.1], [1.2])

$$\widehat{z}(m) = \widehat{x}(m)\, \widehat{y}(m), \; m = 0, \ldots, N-1,$$

$$z(k) = \frac{1}{N} \sum_{m=0}^{N-1} \widehat{z}(m)\, h_{-m}(k), \; k = 0, \ldots, N-1,$$

где

$$\widehat{x}(m) = \sum_{n=0}^{N-1} x(n)\; h_m(n), \; m = 0, \ldots, N-1, \tag{1.2}$$

$$h_m(n) = \exp\left\{2\pi i \frac{mn}{N}\right\},$$

[1)] Дж. Конвей, Н. Слоэн. «Упаковки шаров, решетки и группы», М.: Мир, 1990.

есть дискретное преобразование Фурье (ДПФ), а

$$x(n) = \frac{1}{N} \sum_{m=0}^{N-1} \widehat{x}(m)\, h_{-m}(n),\ n = 0, \ldots, N-1$$

— обратное дискретное преобразование Фурье (ОДПФ), значения последовательностей $x(n)$ и $y(n)$ считаются, как правило, принадлежащими полю рациональных чисел Q (естественное «пользовательское» допущение) или, после соответствующего масштабирования, принадлежащими кольцу целых чисел Z. В то же время значения базисных функций $h_m(n)$ дискретного преобразования Фурье принадлежит полю комплексных чисел C — алгебраическому расширению $\mathsf{R}(i)$ поля R с индуцированной метрикой, связанной с обычным понятием модуля комплексного числа, которое, в свою очередь, является пополнением поля Q относительно метрики, связанной с абсолютной величиной числа. Таким образом, поле Q вкладывается в полное поле C, причем при реализации на ЭВМ в силу конечноразрядного представления чисел вычисление преобразования (1.2) производится в $\mathsf{Q}(i)$, 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 (1.2) его «модулярных аналогов» — теоретико-числовых преобразований (ТЧП, преобразований Фурье–Галуа):

$$\widehat{x}(m) = \sum_{n=0}^{N-1} x(n)\, \omega^{mn} \pmod p, \quad \omega^N \equiv 1 \pmod p. \tag{1.3}$$

Теорема о свертке остается справедливой и в этом случае, но уже для свертки (1.1) понимаемой не в целочисленной арифметике кольца Z, а в арифметике конечного поля $(\bmod\, p)$, существенно отличающейся от арифметики кольца Z.

Основная идея. Давайте выберем простое число p достаточно большим:

$$p > \max_{0 \leqslant n < N} \{x(n)\} \max_{0 \leqslant n < N} \{h(n)\}\, N, 0 < x(n),\ h(n) \in \mathsf{Z}. \tag{1.4}$$

Тогда наименьший неотрицательный вычет значения целочисленной свертки, вычисляемой непосредственно по формуле (1.1), равен значению этой свертки. При вычислении свертки (1.1) с помощью теоретико-числовых преобразований результаты промежуточных вычислений могут превзойти число p, и полученные значения компонент свертки оказываются «вычисленными с ошибкой», а именно, с точностью до слагаемого, делящегося на число p. Выбор числа p с условием (1.4) в

сочетании с (грубой) априорной информацией о диапазоне изменения значений сворачиваемых функций позволяет утверждать, что найденные значения свертки являются точными (следующее целое число, отличающееся от найденного слагаемым, делящимся на p, «слишком велико»).

Таким образом, модулярные вычисления можно интерпретировать как «приближенные вычисления» в некоторой алгебраической структуре, причем эта «приближенность» характеризуется делимостью «погрешности» на простое число p.

Одной из целей гл. 1 является метрическая формализация вышеприведенной интерпретации, что позволило бы с единой точки зрения проанализировать, как и особенности спектральных методов вычисления свертки, а именно:

- значения последовательностей $x(n)$ и $h(n)$ считаются принадлежащими полю рациональных чисел Q;
- значения базисных функций $h_m(n)$дискретного преобразования Фурье принадлежит полю комплексных чисел C, которое является пополнением поля $\mathsf{Q}(i)$ относительно метрики, связанной с модулем комплексного числа;
- при реализации на ЭВМ в силу конечноразрядного представления чисел вычисление свертки производится в $\mathsf{Q}(i)$,

так и экстраполировать эти спектральные методы для вложений поля Q в его пополнения относительно других, так называемых неархимедовых, метрик поля Q. Реализация этой 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 (1.1) даже при относительно скромных вычислительных возможностях.

Отметим, что вычисление свертки (1.1) с помощью ТЧП содержит ряд вполне объективных трудностей, связанных с арифметическими особенностями конечных полей:

- арифметические операции $(\bmod p)$ не являются «элементарными компьютерными операциями», а простые числа p с «дружественными» для машинной реализации свойствами модулярных операций встречаются в натуральном ряду достаточно редко;
- в отличие от поля комплексных чисел, в конечном поле $\mathsf{GF}(p)$ (поле классов вычетов по простому $(\bmod p)$) существуют корни не любой степени N из единицы, а только удовлетворяющие условию делимости $N|(p-1)$.

К сожалению, эти особенности отчасти конфликтуют между собой: «хорошие» для машинной реализации операций простые числа имеют «плохие» делители числа $(p-1)$, что несколько осложняет алгоритмическую поддержку вычислений ТЧП и наоборот. Поэтому второй задачей, рассматриваемой в гл. 1, является разработка неких

компромиссных решений, базирующихся на использовании представления элементов конечных полей в специальных системах счисления.

1.2. Реализация арифметических операций для модулей специального вида

Настоящий раздел имеет вспомогательный характер и включен лишь для удобства цитирования. По крайней мере, по теме двух его первых подразделов существует множество публикаций, в которых рассматриваются различные версии программной и аппаратной реализации арифметических операций в кольцах классов вычетов по модулям простых чисел специального вида – простых чисел Мерсенна и Ферма. Краткий анализ этих работ приведен в комментариях к гл. 1. Несколько меньшей известностью пользуются простые числа Голомба (п. 1.2.3) и их мы рассматриваем чуть более подробно также в п. 1.3.1.

1.2.1. Арифметика в полях по модулю числа Мерсенна. Простым числом Мерсенна называется простое число вида $p = 2^q - 1$. Из вида числа Мерсенна сразу следует необходимое (но не достаточное) ограничение на число q, которое также должно быть простым.

Сформулируем основные правила вычислений в поле $\mathsf{M} \cong \mathsf{Z}/p\mathsf{Z}$, $p = 2^q - 1$:

1) любой элемент поля M представляется в форме
$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{q-1} 2^{q-1}, \quad x_j \in \{0, 1\}; \tag{1.5}$$
2) это представление однозначно для всех $0 \neq x \in \mathsf{M}$; нулевой элемент представим двумя способами в форме (1.5):
$$0 \cdot 2^0 + \ldots + 0 \cdot 2^{q-1} \equiv 1 \cdot 2^0 + \ldots + 1 \cdot 2^{q-1} \equiv 2^q - 1 \equiv 0 \pmod p;$$
3) так как $2^q \equiv 1 \pmod p$, то в случае возникновения «бита переполнения» $1 \cdot 2^q$ при вычислениях эта единица «самого старшего разряда» переносится в «самый младший разряд» и суммируется с полученным числом;
4) умножение элемента $x \in \mathsf{M}$ на элемент $2 \in \mathsf{M}$ равносильно циклическому сдвигу «цифр» x_j в представлении (1.5):
$$2x = x_{q-1} 2^0 + x_0 2^1 + \ldots + x_{q-2} 2^{q-1};$$
5) умножение элементов поля M «столбиком» сводится к циклическим перестановкам цифр и сложениям;
6) мультипликативный порядок элемента $2 \in \mathsf{M}$ равен q: $\mathbf{Ord}(2) = q$ (следовательно, при $\omega = 2 \in \mathsf{M}$ возможна реализация ТЧП (1.3) длиной $N = q$ без умножений);
7) мультипликативный порядок элемента $(-2) \in \mathsf{M}$ равен $2q$: $\mathbf{Ord}(-2) = 2q$ (следовательно, при $\omega = (-2) \in \mathsf{M}$ возможна реализация ТЧП (1.3) длиной $N = 2q$ без умножений);

8) максимальная степень двойки, делящая число $(p-1)$ равна единице.

Следует заметить, что свойства 1–5, сформулированные выше, остаются справедливыми и для составных чисел Мерсенна. Отметим также, что последнее свойство чисел Мерсенна несколько осложняет задачу эффективного вычисления ТЧП Мерсенна, так как требование делимости $N\,|(p-1)$ приводит к необходимости синтеза быстрых алгоритмов таких преобразований для весьма «экзотических» длин N. Например,

$$\left(2^{31}-1\right)-1=2\cdot\left(2^{30}-1\right)=2\cdot 3^2\cdot 7\cdot 11\cdot 31\cdot 151\cdot 331$$

и так далее.

Паллиативным способом преодоления указанной трудности является рассмотрение ТЧП в «комплексном поле Мерсенна»:

$$\mathsf{M}(i)=\left\{z:\ a+bi;\ \ a,b\in\mathsf{M},\quad i^2\equiv -1\ (\mathrm{mod}p)\right\}.$$

В этом случае условие делимости имеет вид $N\,\big|(p^2-1)$ и, в силу равенства

$$(p^2-1)=(p-1)(p+1)=2^{q+1}\left(2^{q-1}-1\right),$$

в поле $\mathsf{M}(i)$ существуют корни степени $N=2^t,\quad (t=1,2,\ldots,q+1)$.

Следует отметить, что арифметические действия в поле $\mathsf{M}(i)$ совершено аналогичны операциям в комплексном поле C и отличаются лишь необходимостью вычисления остатков по $(\mathrm{mod}p)$. В п. 1.3.2 мы рассматриваем также специфические системы счисления в поле $\mathsf{M}(i)$, позволяющие еще более упростить некоторые операции над элементами этого поля.

1.2.2. Арифметика в полях по модулю числа Ферма. Простым числом Ферма называется простое число вида

$$f=f_k=2^{2^k}+1=2^B+1,\quad k=0,1,2,3,4.$$

В настоящее время известны только эти простые указанного вида и неизвестно конечно ли их количество. В задачах цифровой обработки сигналов наиболее часто используется четвертое простое число Ферма, равное $f_4=2^{2^4}+1=2^{16}+1=65537$.

Сформулируем основные правила вычислений в поле $\mathsf{F}\cong\mathsf{Z}/f\mathsf{Z}$, $f=2^B+1$:

1) любой элемент поля F представляется в форме

$$x=x_0 2^0+x_1 2^1+\ldots+x_B 2^B,\quad x_j\in\{0,1\};\tag{1.6}$$

2) это представление для всех $2^B\neq x\in\mathsf{F}$ имеет вид

$$x=x_0 2^0+x_1 2^1+\ldots+x_{B-1}2^{B-1}+0\cdot 2^B;$$

«исключительный» нулевой элемент представим в форме

$$2^B=0\cdot 2^0+0\cdot 2^1+\ldots+0\cdot 2^{B-1}+1\cdot 2^B;$$

3) так как $2^B \equiv -1 \pmod{f}$, то в случае возникновения «бита переполнения» $1 \cdot 2^B$ при вычислениях эта единица, в случае «неисключительного» результата, переносится в «самый младший разряд» и вычитается из полученного числа;
4) умножение элемента $x \in \mathsf{F}$ на элемент $2 \in \mathsf{F}$ равносильно циклическому сдвигу «цифр» x_j в представлении (1.6) с инверсией знака в младшем разряде:
$$2x = (-x_B) \cdot 2^0 + x_0 \cdot 2^1 + \ldots + x_{B-1} 2^B;$$
5) умножение элементов поля F «столбиком» сводится к циклическим перестановкам цифр и сложениям-вычитаниям;
6) мультипликативный порядок элемента $2 \in \mathsf{F}$ равен $2B$: $\mathbf{Ord}\,(2) = 2B$ (следовательно, для $\omega = 2 \in \mathsf{F}$ возможна реализация ТЧП (1.3) длиной $N = 2B$ без умножений).

Следует отметить, что относительными недостатками чисел Ферма является более сложная реализация арифметических операций в поле F по сравнению с мерсенновским полем M: наличие «исключительного» элемента, необходимость вычитания, а также то, что простых чисел Ферма известно мало. Но эти недостатки несколько компенсируются тем фактом, что условие делимости $N|(f-1)$ имеет вид $N|2^B$ и, следовательно, в поле F существуют корни степени $N = 2^t, \quad (t = 1, 2, \ldots, B)$.

1.2.3. Арифметика в полях по модулю числа Голомба. Простым числом Голомба будем называть простое число вида
$$g = g_k = 3 \cdot 2^k + 1 = 2^{k+1} + 2^k + 1.$$
В частности, простыми числами Голомба являются числа
$$\begin{array}{ll} g_8 = 769, & g_{30} = 3\,221\,225\,473, \\ g_{12} = 12\,289, & g_{36} = 206\,158\,430\,209, \\ g_{18} = 786\,433, & g_{41} = 6\,597\,069\,776\,657. \end{array}$$
Сформулируем основные правила вычислений в поле $\mathsf{G} \cong \mathsf{Z}/g\mathsf{Z}$, $g = g_k = 2^{k+1} + 2^k + 1$:

1) любой элемент поля G представляется в форме
$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{k+1} 2^{k+1}, \quad x_j \in \{0, 1\}; \tag{1.7}$$
2) так как
$$2^{k+1} \equiv -2^k - 1 \pmod{g}, \tag{1.8}$$
то в случае возникновения «бита переполнения» $1 \cdot 2^{k+1}$ при вычислениях эта единица, в случае необходимости, переносится и вычитается дважды согласно (1.8);
3) умножение элемента $x \in \mathsf{G}$ на элемент $2 \in \mathsf{G}$ сводится к циклическим перестановкам цифр x_j в представлении (1.7) и сложениям-вычитаниям;

4) умножение элементов поля G «столбиком» также сводится к циклическим перестановкам цифр и сложениям-вычитаниям;
5) мультипликативный порядок элемента $2 \in \mathsf{G}$ равен $3 \cdot 2^{k-1}$: $\mathsf{Ord}\,(2) = 3 \cdot 2^{k-1}$ (следовательно, при $\omega = 2 \in \mathsf{G}$ возможна реализация ТЧП (1.3) длиной $N = 3 \cdot 2^{k-1}$ без умножений);
6) мультипликативный порядок элемента $8 \in \mathsf{G}$ равен 2^{k-1}: $\mathsf{Ord}(2^3) = 2^{k-1}$ (следовательно, при $\omega = 2^3 \in \mathsf{G}$ возможна реализация ТЧП (1.3) длиной $N = 2^{k-1}$ без умножений).

Несмотря на наличие корней ω «удобной» степени $N = 2^{k-1}$, арифметические операции в поле G имеют более сложную реализацию при представлении элементов поля в «модулярной» двоичной системе счисления в форме (1.7). Это связано в первую очередь с необходимостью одновременного или последовательного вычитания для двух разрядов представления (1.7), причем каждое из этих вычитаний может также привести к переполнению разрядной сетки. В п. 1.3.1 мы рассмотрим некоторые методы преодоления отмеченных трудностей.

1.3. Редуцированные системы счисления в конечных полях

1.3.1. Двоично-избыточная система счисления. Рассмотренные выше примеры реализации модулярных вычислений для модулей специального вида (Мерсенна, Ферма, Голомба) используют некоторую модификацию обычной двоичной системы счисления, причем реализация модулярной арифметики будет тем эффективнее, чем меньше возникает специфических отличий, связанных с нахождением вычета целого числа по $(\bmod p)$. Эти имеющиеся отличия «двоичных» вычислений в конечных полях (кольцах) определяют специфические правила «переноса в старший разряд», то есть, своеобразие двоичной модулярной арифметики, двоичной модулярной системы счисления. Позиционные системы счисления в конечных кольцах будем называть далее *редуцированными системами счисления*.

Следует отметить, что для вычислений по модулю чисел Ферма и, в особенности Голомба, при умножении на степень двойки приходится производить вычитание, так как простая инверсия знаков одного или нескольких бит выводит вычисления за рамки двоичности. Если допустить «законность» цифр $\{-1, 0, 1\}$, сохраняя при этом двоичное основание системы, то получается редуцированная система счисления, в которой элементы кольца классов вычетов по, например, модулю числа Ферма $f = 2^B + 1, \quad (B = 2b)$ представляются неоднозначно в форме

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_B 2^B, \quad x_j \in \{-1, 0, 1\}. \tag{1.9}$$

Отмеченную избыточность представления (1.9) можно несколько уменьшить, заметив, что справедливы соотношения:

$$0 \leqslant x_0 2^0 + x_1 2^1 + \ldots + x_{b-1} 2^{b-1} < 2^b, \quad x_j \in \{0, 1\},$$

$$-2^b < x_0 2^0 + x_1 2^1 + \ldots + x_{b-1} 2^{b-1} \leqslant 0, \quad x_j \in \{-1, 0\},$$

а также то, что любое целое число из промежутка $(-2^b, 0]$ сравнимо по $(\mathrm{mod}\, f)$ с некоторым целым числом из промежутка $[2^b, f)$ и наоборот. Аналогичные соображения справедливы и элементов кольца классов вычетов по модулю чисел Голомба.

Конечно, добиться полной однозначности представления не удается. Действительно, в рассмотренном случае поля по $(\mathrm{mod}\, f)$ справедливы, например, равенства

$$1 \cdot 2^2 + (-1) \cdot 2^0 = 3 = 1 \cdot 2^1 + 1 \cdot 2^0.$$

Пример 1.1. Пусть g есть простое число Голомба, элемент $x \in \mathsf{G}$ запишем в виде

$$x = x_0 2^0 + x_1 2^1 + \ldots + x_{k-3} 2^{k-3} + \delta_1 2^{k-2} + \ldots + \delta_4 2^{k+1},$$

а элемент $8x \in \mathsf{G}$ — в виде

$$2^3 x = y_1 2^0 + y_2 2^1 + y_3 2^2 + x_0 2^3 + \ldots + x_{k-3} 2^k + y_4 2^{k+1}.$$

Таблица 1.1

δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4	δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4	δ_1	δ_2	δ_3	δ_4	y_1	y_2	y_3	y_4
0	0	0	0	0	0	0	0	1	0	0	0	−1	1	−1	1	−1	0	0	0	1	−1	1	−1
0	0	0	1	1	0	0	0	1	0	0	1	0	1	−1	1	−1	0	0	1	−1	−1	1	0
0	0	0	−1	−1	0	0	0	1	0	0	−1	1	1	−1	0	−1	0	0	−1	0	−1	1	−1
0	0	1	0	−1	0	0	1	1	0	1	0	1	1	0	−1	−1	0	1	0	0	−1	1	0
0	0	1	1	0	0	0	1	1	0	1	1	−1	1	0	0	−1	0	1	1	1	−1	1	0
0	0	1	−1	1	0	0	0	1	0	1	−1	−1	1	0	−1	−1	0	1	−1	−1	−1	1	0
0	0	−1	0	1	0	0	−1	1	0	−1	0	0	1	−1	0	−1	0	−1	0	−1	−1	0	1
0	0	−1	1	−1	0	0	0	1	0	−1	1	1	1	−1	0	−1	0	−1	1	1	−1	0	1
0	0	−1	−1	0	0	0	−1	1	0	−1	−1	−1	1	−1	0	−1	0	−1	−1	1	−1	0	0
0	1	0	0	1	0	1	−1	1	1	0	0	0	1	0	0	−1	1	0	0	−1	−1	1	1
0	1	0	1	−1	0	1	0	1	1	0	1	1	1	0	0	−1	1	0	1	1	−1	1	1
0	1	0	−1	0	0	1	−1	1	1	0	−1	−1	1	0	0	−1	1	0	−1	1	−1	1	0
0	1	1	0	0	0	1	0	1	1	1	0	−1	1	0	1	−1	1	1	0	1	−1	1	0
0	1	1	1	1	0	1	0	1	1	1	1	0	1	0	1	−1	1	1	1	1	0	0	0
0	1	1	−1	−1	0	1	0	1	1	1	−1	1	1	0	0	−1	1	1	−1	−1	−1	1	0
0	1	−1	0	−1	0	0	1	1	1	−1	0	1	1	−1	0	−1	1	−1	0	1	−1	1	0
0	1	−1	1	0	0	0	1	1	1	−1	1	−1	1	0	0	−1	1	−1	1	1	0	0	0
0	1	−1	−1	1	0	0	0	1	1	−1	−1	0	1	0	−1	−1	1	−1	−1	−1	−1	1	0
0	−1	0	0	−1	0	−1	−1	1	−1	0	0	1	1	−1	−1	−1	−1	0	0	0	−1	0	0
0	−1	0	1	0	0	−1	1	1	−1	0	1	−1	1	−1	0	−1	−1	0	1	1	−1	0	0
0	−1	0	−1	1	0	−1	0	1	−1	0	−1	−1	1	−1	−1	−1	−1	0	−1	−1	−1	0	0

В табл. 1.1 указано соответствие между «цифрами» $\delta_1, \dots \delta_4$ элемента x и «цифрами» $y_1, \dots y_4$ элемента $8x \in \mathsf{G}$ для представления в двоично-избыточной системе счисления.

1.3.2. Редуцированные системы счисления в комплексном поле Мерсенна. Редуцированные системы счисления с «нетрадиционными» основаниями могут быть рассмотрены и для алгебраических расширений конечных полей.

Приводимый ниже пример целиком заимствован из книги [1.3].

Пример 1.2. Выбор основания $2i$ приводит к системе счисления, которую естественно назвать «мнимо-четверичной» (по аналогии с «четверичной») ввиду того, что каждое комплексное число может быть представлено в этой системе при помощи цифр $0, 1, 2, 3$ (причем тех же цифр, взятых со знаком минус, не требуется). Например,

$$(11210.31)_{2i} = \\ = 1 \cdot 16 + 1 \cdot (-8i) + 2 \cdot (-4) + 1 \cdot (-2i) + 3 \cdot \left(-\frac{1}{2}i\right) + 1 \cdot \left(-\frac{1}{4}\right) = \\ = 7\frac{3}{4} - 7\frac{1}{2}i.$$

Так как справедливо равенство

$$(a_{2n} \dots a_1 a_0 . a_{-1} \dots a_{-2k})_{2i} = \\ = (a_{2n} \dots a_2 a_0 . a_{-2} \dots a_{-2k})_{-4} + 2i\,(a_{2n-1} \dots a_3 a_1 . a_{-1} \dots a_{-2k+1})_{-4}\,,$$

то перевод числа в мнимо-четверичную форму и обратно сводится к переводу в «негативно-четверичную» форму и обратно. Интересное свойство этой системы состоит в том, что она допускает выполнение умножения и деления комплексных чисел целостным образом без раздельного рассмотрения вещественных и мнимых частей. Например, перемножить два числа мы можем в этой системе так же, как и при любом другом основании, используя только несколько иное «правило переноса». В случае если цифра становится больше 4, мы вычитаем 4 и «переносим» -1 на два столбца влево, а когда получается отрицательная цифра, мы прибавляем к ней 4 и «переносим» $+1$ на два столбца влево. Разбор нижеследующего примера пояснит, как работает это своеобразное правило переноса:

$$\begin{array}{rl} 12231 & [9-10i] \\ 12231 & [9-10i] \\ \hline 12231 & \\ 10320213 & \\ 13022 & \\ 13022 & \\ 12231 & \\ \hline 021333121 & [-19-180\,i]. \end{array}$$

Пусть $\mathsf{M} \cong \mathbf{F}_p$ и $p = 2^q - 1$ является простым числом Мерсенна. Рассмотрим «модулярный» аналог этой системы счисления для «комплексного поля Мерсенна»:

$$\mathsf{M}(i) = \left\{z:\ a + bi;\ \ a, b \in M, \quad i^2 \equiv -1 \pmod p\right\}.$$

Лемма 1.1. *Любой элемент $z \in \mathsf{M}(i)$ может быть представлен в форме*

$$z = a_{-1}(2i)^{-1} + a_0(2i)^0 + a_1(2i)^1 + \ldots + a_\nu(2i)^\nu,\ a_j = 0, 1, 2, 3, \quad (1.10)$$

где $\nu = \nu(q) = q - 1$.

Доказательство. Положим

$$z = x - (2i)^{-1}(2y') = x - (2i)^{-1}y;\ \ x, y \in \mathsf{M}, \qquad (1.11)$$

где

$$\begin{aligned} &x \equiv x_0(-4)^0 + x_2(-4)^1 + \ldots + x_{2t}(-4)^t \ (\mathrm{mod} p), \\ &y \equiv y_0(-4)^0 + y_2(-4)^1 + \ldots + y_{2t}(-4)^t (\mathrm{mod} p), \\ &x_j, y_j \in \{0, 1, 2, 3\}. \end{aligned} \qquad (1.12)$$

Тогда доказательство леммы сводится к доказательствам:

а) принципиальной возможности представления элементов поля M в форме (1.10),

б) определению минимального натурального $t = t(p)$, при котором возможно такое представление.

Для доказательства утверждений (а)–(б) достаточно заметить, что представление произвольного элемента поля M в четверичной системе счисления возможно и требует не более $t = (q+1)/2$ слагаемых. Далее, так как

$$\begin{aligned} x \equiv x_0(-4)^0 + x_2(-4)^1 + \ldots + x_{2t}(-4)^t \pmod p \equiv \\ \equiv \left(x_0(4)^0 + x_4(4)^2 + \ldots\right) - 4\left(x_2(4)^0 + x_6(4)^2 + \ldots\right) (\mathrm{mod}\, p) \equiv \\ \equiv X^{(+)} - 4X^{(-)} (\mathrm{mod}\, p), \quad X^{(+)}, X^{(-)} \in \mathsf{M}, \end{aligned}$$

то и для элемента $X^{(+)} - 4X^{(-)} \in \mathsf{M}$ также требуется не более $t = (q+1)/2$ слагаемых.

Находя для элементов $x, y \in \mathsf{M}$ их представление в «негачетверичной» системе счисления (системе счисления с основанием (-4)) и полагая далее, в соответствии с равенством (1.10),

$$a_{-1} = y_0,\ a_0 = x_0,\ a_1 = y_1,\ a_2 = x_1 \ldots$$

получаем утверждение Леммы 1.2. ■

Лемма 1.2. *Мультипликативный порядок элемента $2i$ в поле $\mathsf{M}(i)$ равен* $\mathbf{Ord}\,(2i) = 4q$.

Доказательство. Вычисляя последовательно, получаем

$$(2i)^2 = -4, \quad (2i)^4 = 16.$$

Далее, в силу того, что н.о.д $(16, 2^q - 1) = 1$, мультипликативный порядок элемента $16 = 2^4$ равен мультипликативному порядку элемента 2 и, следовательно, для элемента $2i$ в поле $\mathsf{M}(i)$ справедливо соотношение

$$\mathbf{Ord}\,(2i) = 4\,\mathbf{Ord}\,(16) = 4\,\mathbf{Ord}\,(2) = 4q. \qquad \blacksquare$$

Таким образом, для $\omega = 2i$ возможна реализация ТЧП длиной $N = 4q$ без умножений в поле $\mathsf{M}(i)$.

Как и в комплексном случае, при сложении и умножении элементов поля $\mathsf{M}(i)$ в редуцированной мнимо-четвертичной системе счисления в промежуточных результатах могут возникнуть «цифры», не являющиеся элементами множества $\{0, 1, 2, 3\}$. Другими словами, необходимо сформулировать «правила переноса» в старшие разряды для действий, производимых над элементами в форме (1.10). Сформулируем эти непосредственно проверяемые правила в виде леммы.

Лемма 1.3. *В поле* $\mathsf{M}(i)$ *справедливы равенства*:

$$\begin{gathered}
4 = 1\cdot(2i)^4 + 3\cdot(2i)^2 = 1\cdot(-4)^2 + 3\cdot(-4)^1 =,\\
5 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 1\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 1\cdot(-4)^0,\\
6 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 2\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 2\cdot(-4)^0,\\
7 = 1\cdot(2i)^4 + 3\cdot(2i)^2 + 3\cdot(2i)^0 = 1\cdot(-4)^2 + 3\cdot(-4)^1 + 3\cdot(-4)^0,\\
8 = 1\cdot(-4)^2 + 2\cdot(-4)^1,\\
9 = 1\cdot(-4)^2 + 2\cdot(-4)^1 + 1\cdot(-4)^0.
\end{gathered}$$

Несмотря на «четверичность» рассмотренной системы счисления, вычисления в ней легко реализуются на обычное «бинарной» вычислительной технике, если рассмотреть для каждого из возможных значений «цифр» $a_j = 0, 1, 2, 3$ их двухбитовое представление.

«Бинарную» редуцированную систему счисления для поля $\mathsf{M}(i)$ можно также получить, используя основание $(i - 1)$, (см. более подробно в гл. 4.

Лемма 1.4. *Любой элемент* $z \in \mathsf{M}(i)$ *может быть представлен в форме*

$$z = a_0(i-1)^0 + a_1(i-1)^1 + \ldots + a_\nu(i-1)^\nu,\ a_j = 0, 1, \tag{1.13}$$

где $\nu = \nu(q) \leqslant 8([q/4] + 1)$.

Доказательство. Положим $i - 1 = \alpha$. Так как $\alpha^8 = 16$, то для элемента $z \in \mathsf{M}(i)$ справедливо представление в шестнадцатеричной системе счисления

$$z = b_0 16^0 + b_1 16^1 + \ldots + b_\mu 16^\mu,\ b_j = 0, 1, \ldots, 15,$$

где $\mu = [q/4] + 1$. В свою очередь, шестнадцатиричные «цифры» b_j представляются в виде сумм степеней элемента $i - 1 = \alpha$, что и доказывает Лемму 1.4. $\blacksquare$

Как и в случае мнимо-четверичной системы счисления, при сложении и умножении элементов поля $\mathsf{M}(i)$ в редуцированной системе