НАУКА
И ТЕХНИЧЕСКИЙ
ПРОГРЕСС

Л. В. ВАРИЧЕНКО
В. Г. ЛАБУНЕЦ
М. А. РАКОВ

АБСТРАКТНЫЕ АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ И ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ

АКАДЕМИЯ НАУК УКРАИНСКОЙ ССР
ФИЗИКО-МЕХАНИЧЕСКИЙ ИНСТИТУТ ИМ. Г. В. КАРПЕНКО

Л. В. ВАРИЧЕНКО
В. Г. ЛАБУНЕЦ
М. А. РАКОВ

АБСТРАКТНЫЕ АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ И ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ

КИЕВ НАУКОВА ДУМКА 1986

УДК 621.391.837,681.327.22

Абстрактные алгебраические системы и цифровая обработка сигналов / Вариченко Л. В., Лабунец В. Г., Раков М. А.— Киев : Наук. думка, 1986.— 248 с.

В монографии рассмотрены вопросы использования абстрактных алгебраических систем (конечные кольца и поля) для цифровой обработки сигналов. Изложены основы теории конечных колец и полей, методы использования их для реализации цифрового спектрального анализа, вычисления свертки, нелинейной обработки сигналов. Большое внимание уделено аппаратурной реализации алгоритмов цифровой обработки сигналов с помощью многозначной элементной базы, в частности вопросам построения устройств, реализующих операции в конечных полях.

Для научных и инженерно-технических работников, специализирующихся в области технической кибернетики и цифровой обработки сигналов; может быть полезна преподавателям, аспирантам и студентам вузов.

Ил. 61, Табл. 53, Библиогр.: с. 237—245 (214 назв.).

Ответственный редактор *Я. Е. Беленький*

Рецензенты *И. М. Вишенчук, Р. Ф. Федорив*

Редакция технической литературы

В $\frac{1502000000\text{-}116}{M221(04)\text{-}86}$ 147-86

ПРЕДИСЛОВИЕ

Цифровая вычислительная машина (ЦВМ) уверенно занимает место первого помощника современного человека. Существование экономически развитых стран без значительного парка вычислительных машин немыслимо. В этой связи вполне естествен процесс увеличения числа задач, решаемых с помощью ЦВМ, причем ЦВМ применяется не только как мощный арифмометр, но и как звено автоматизированного участка деятельности человека по переработке информации. Примерами такого использования ЦВМ являются автоматизированные системы управления различными процессами, автоматизированные системы проектирования, измерительные системы и др. Первостепенную роль в этих системах выполняет обработка сигналов. Перед обработкой на ЦВМ сигнал представляется в цифровой форме (цифровой сигнал). Развитие методов обработки таких сигналов — актуальная и важная задача. Практика показала, что перенесение методов, применяемых ранее при обработке аналоговых сигналов, неэффективно и в ряде случаев практически невозможно. Эффективными оказались нетрадиционные подходы, которые более полно учитывают специфику цифрового представления сигнала.

Научная дисциплина, занимающаяся разработкой методов обработки цифровых сигналов и специализированных средств для обработки таких сигналов, получила название «цифровая обработка сигналов» (ЦОС). Решение задач ЦОС заключается в построении математической модели системы ЦОС и ее реализации с помощью ЦВМ или специализированного вычислительного устройства. Эффективность ЦОС определяется эффективностью построенной математической модели и производительностью ЦВМ.

В последнее время получили распространение математические модели систем ЦОС, построенные с применением аппарата теории полей Галуа, конечных колец, алгебр k-значных функций (абстрактных алгебраических систем), благодаря ряду преимуществ: во-первых, такие модели более полно учитывают структуру цифрового сигнала и дискретную форму представления информации, во-вторых, упрощается реализация моделей на ЦВМ или уменьшаются аппаратурные затраты на реализацию специализированных устройств, в-третьих, такой подход позволяет с единых позиций рассматривать задачи ЦОС и задачи проектирования соответствующих специализированных вычислительных средств. Именно такие модели (вопросы построения и реализации) исследуются в настоящей монографии. Написать ее авторов побудило два обстоятельства: первое — это то, что в отечественной литературе нет книги, в которой систематически излагались бы теория и методы ЦОС с использованием абстрактных алгебраических систем; второе — практически отсутствуют работы, доступные для инженеров. Обычно изложение ведется на уровне, требующем для чтения высокой математической культуры. По мнению авторов, данная монография должна восполнить указанные пробелы и адресуется она в первую очередь инженерам.

В первой главе приводится классификация сигналов, определяются цифровые сигналы и рассматривается соотношение их с функциями k-значной логики, описываются цели и задачи ЦОС, а также рассматриваются виды преобразований, которым подвергаются цифровые сигналы в процессе обработки.

Во второй главе даются сведения из современной алгебры и теории чисел, описываются основные свойства конечных групп, полей, колец, а также векторных пространств. Эту главу ни в коем случае не следует рассматривать как строгое математическое изложение указанных вопросов. В ней приводятся многие примеры (как и во всей книге вообще), используемые в последующих главах. Эта глава имеет еще одну специфику — ее писали не математики, а инженеры, освоившие материал, составляющий содержание главы, самостоятельно. Таким образом, результаты из алгебры как бы «пропускаются» сквозь призму восприятия инженера с его складом мышления. Это и обусловило степень подробности как второй главы, так и всей монографии — она должна быть доступна инженерам без помощи вспомогательных руководств по математике (определенные знания по теории сигналов и ЦОС предполагаются).

Третья глава посвящена изучению характеров конечных абелевых групп и их связи с ортогональными преобразованиями сигналов.

В четвертой главе рассматриваются теоретико-числовые преобразования, определяемые над полями Галуа, конечными кольцами и другими алгебраическими системами. В отдельную главу (пятую) выделен материал, касающийся комплексных теоретико-числовых преобразований Гаусса.

В шестой главе решаются вопросы преобразования спектров цифровых сигналов. Кроме обычных преобразований спектров в различные базисы рассмотрены методы преобразования значений спектров цифровых сигналов из поля комплексных чисел в конечное поле или кольцо, причем спектры определены в одном и том же базисе, а также обратная задача — преобразование значений спектров из конечного поля или кольца в поле комплексных чисел.

В седьмой главе описаны примеры математических моделей систем ЦОС, построение которых связано с использованием абстрактных алгебраических систем.

И наконец, восьмая глава посвящена вопросам аппаратурной реализации математических моделей систем ЦОС. Рассмотрены методы реализации с помощью многозначной элементной базы (обычная двоичная элементная база является частным случаем многозначной). Приведены конкретные примеры аппаратурной реализации узлов и блоков специализированных устройств, а также вариант архитектуры специализированного векторного процессора, ориентированного на решение задач ЦОС.

В большинстве глав приводятся упражнения, предназначенные для самостоятельной проработки. Основная часть их иллюстрирует приведенный материал и не вызовет затруднений при решении. Однако есть и более трудные упражнения, являющиеся, по существу, заданиями на приведение довольно сложных математических выкладок либо на проектирование специализированных вычислительных устройств. Возможно, что решения таких упражнений обусловят ряд задач, которые смогут послужить читателю основой для научных исследований.

В процессе работы над книгой авторам оказали помощь Я. П. Драган, Р. Ф. Федорив, Б. П. Русын, а также И. М. Беген, Е. Г. Бирюкова, А. Р. Онысык. Авторы считают своим приятным долгом выразить всем им благодарность.

Авторы будут признательны всем читателям, которые пришлют свои замечания и пожелания по адресу: 290601, г. Львов, ул. Научная, 5, Физико-механический институт им. Г. В. Карпенко АН УССР.

СПИСОК ПРИНЯТЫХ ОСНОВНЫХ СОКРАЩЕНИЙ

АЛУ — арифметико-логическое устройство
АЦП — аналого-цифровое преобразование
БИС — большая интегральная схема
БПФ — быстрое преобразование Фурье
ДПФ — дискретное преобразование Фурье
ИВТ — информационно-вычислительная техника
КПСНВ — полная система наименьших вычетов по комплексному модулю
КСАНВ — полная система абсолютно наименьших вычетов по комплексному модулю
КУВ — коэффициент ускорения вычислений
КФ — корреляционная функция
НК-АКФ — автокорреляционная функция, определенная в пространстве $L(H, K)$
НК-ВКФ — взаимно корреляционная функция, определенная в пространстве $L(H, K)$
ОДПФ — обратное дискретное преобразование Фурье
ОЗУ — оперативное запоминающее устройство
ОПФГ — обратное преобразование Фурье — Галуа
ППЗУ — перепрограммируемое постоянное запоминающее устройство
ПСАНВ — полная система абсолютно наименьших вычетов по вещественному модулю
ПСВ — полная система вычетов
ПСНВ — полная система наименьших вычетов
ПФГ — преобразование Фурье — Галуа
СБИС — сверхбольшая интегральная схема
ТИИЭР — Труды института инженеров по электротехнике и радиоэлектронике (США)
ТЧП — теоретико-числовое преобразование
ТЧПМ — теоретико-числовое преобразование Мерсенна
ТЧПР — теоретико-числовое преобразование Рейдера
ТЧПФ — теоретико-числовое преобразование Ферма
ЦАП — цифроаналоговое преобразование
ЦВЧ — целые вещественные числа
ЦКЧ — целые комплексные числа
ЦОС — цифровая обработка сигналов

СПИСОК ПРИНЯТЫХ ОБОЗНАЧЕНИЙ

$a \mid b$ — a делит b

$\langle a + bi \mid_m^+$ — полная система наименьших вычетов по комплексному модулю m

$\langle a + bi \mid_m^-$ — полная система абсолютно наименьших вычетов по комплексному модулю m

$\langle A \mid_m$ — выделение из числа A остатка по модулю m

$]a[$ — округление числа a до ближайшего целого

$\rfloor a \lfloor$ — округление числа a до ближайшего большего целого

$A \supset B$ — множество A включает множество B

$A \cup B$ — объединение множеств A и B

$A \cap B$ — пересечение множеств A и B

$a \Leftrightarrow b$ — a равно по определению b

C — поле комплексных чисел

card A — число элементов множества A

deg $(f(x))$ — степень полинома $f(x)$

$ENT(F)$ — кольцо целых чисел поля F

$F[x]/p(x)\,F[x]$ — поле, элементами которого являются многочлены с коэффициентами поля F, приведенные по модулю неприводимого многочлена $p(x)$

CF (p^n) — поле Галуа характеристики p^n

НОК $(a_1, a_2, \ldots, a_m)$ — наименьшее общее кратное чисел $a_1, a_2, \ldots, a_m$

НОД $(a_1, a_2, \ldots, a_m)$ — наибольший общий делитель чисел $a_1, a_2, \ldots, a_m$

$[H : 1]$ — порядок группы H

$L(H, K)$ — пространство функций с областью определения на группе H и областью значений в кольце K

$M(Z_M)$ — абелева группа по умножению кольца Z_M

$|\cdot|_M^+$ — наименьшие неотрицательные вычеты по модулю M, т. е. множество $\{0, 1, \ldots, M-1\}$

$|\cdot|_M^-$ — абсолютно наименьшие вычеты по модулю M, т. е. множество $\{0, \pm 1, \ldots, \pm(M+1)\cdot 1/2$ при нечетных M и $\{0, \pm 1, \ldots, \pm M/2 - 1, \pm M/2\}$ при четном M

$|\cdot|_m$ — полная система вычетов по вещественному модулю m

$|\cdot|_m$ — полная система наименьших вычетов по модулю m

$\|m\|$ — норма комплексного числа m

$\langle\cdot|_m$ — полная система вычетов по комплексному модулю m

N — множество натуральных чисел

P_k^n — множество функций k-значной логики n переменных

Q — поле рациональных чисел

R — поле действительных чисел

$R(+)$ — аддитивная группа действительных чисел

$R^+(\cdot)$ — мультипликативная группа положительных действительных чисел

$T(\varepsilon)$, $N(\varepsilon)$ — период элемента ε

$T(a, M)$, $N(a, M)$ — период элемента a по модулю M

$T_p(2)$, $N_p(2)$ — период элемента 2 по модулю p

U — алгебра

Z — кольцо целых чисел

Z_M — кольцо вычетов по модулю целого числа M

$Z[i]$ — кольцо целых комплексных чисел

$Z_p[i]$, Z_p^c — конечное поле целых комплексных чисел по модулю простого числа p

Z_p^H — конечное кольцо кватернионов

Z_p^k — конечное неассоциативное кольцо чисел Кэли

$\varphi(M)$ — функция Эйлера

ГЛАВА 1

СИГНАЛЫ И ИХ ОБРАБОТКА

1. Классификация сигналов

Под сигналом в общем случае понимают физический процесс, который является средством переноса информации во времени и пространстве [42, 61, 62, 117, 168]. Сигналы описываются математическими моделями, отражающими общие свойства различных по физической природе сигналов. Как значения сигнала, так и его параметры могут характеризоваться действительными числами. Следовательно, сигнал можно определить как отображение

$$x(t): R_t \to \underbrace{R \times R \times \cdots \times R}_{m \text{ раз}}, \tag{1.1}$$

где R — множество действительных чисел, являющееся областью значений сигнала; R_t — область определения сигнала, представляющая собой также множество действительных чисел (в области определения могут принимать значения моменты времени t; в этом случае говорят о временном сигнале. Такие сигналы наиболее часто встречаются на практике); $\times$ — знак прямого произведения; m — размерность сигнала. Кроме параметра t функция $x(t)$ может зависеть от других параметров:

$$x = x(t, a, b, \ldots). \tag{1.2}$$

Среди параметров могут быть случайные величины. Например, случайный процесс [23] — это функция $x(t, \xi)$, аргумент ξ которой принимает значения в пространстве элементарных событий с заданной вероятностной мерой. Значения функции $x(t, \xi)$ являются случайными величинами.

В этой работе нас будут интересовать динамические свойства сигналов, т. е. будем изучать только зависимость x от t. При построении систем обработки сигналов необходимо учитывать еще и статистические (зависимость x от ξ) свойства сигналов, а также зависимость от других параметров. Однако в данной книге эти вопросы не рассматриваются, так как описываемые системы обработки сигналов являются только «детерминированной» частью общей системы обработки. Вопросы статистической теории сигналов, а также учет статистических свойств сигналов при построении систем обработки можно найти в [18, 23, 42, 44, 56, 61, 62, 118, 150, 168, 170].

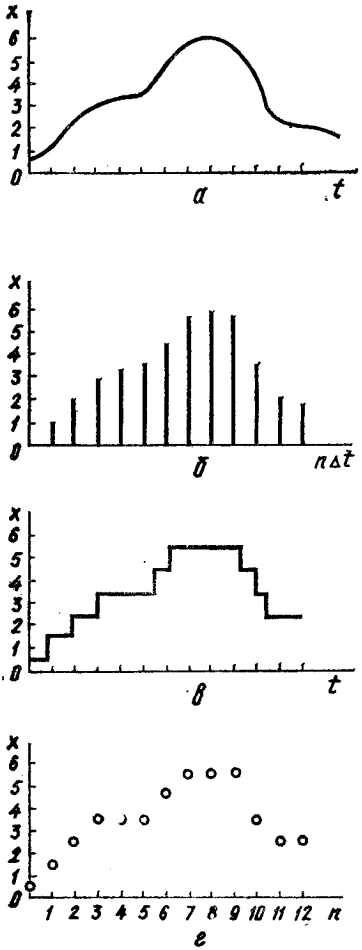
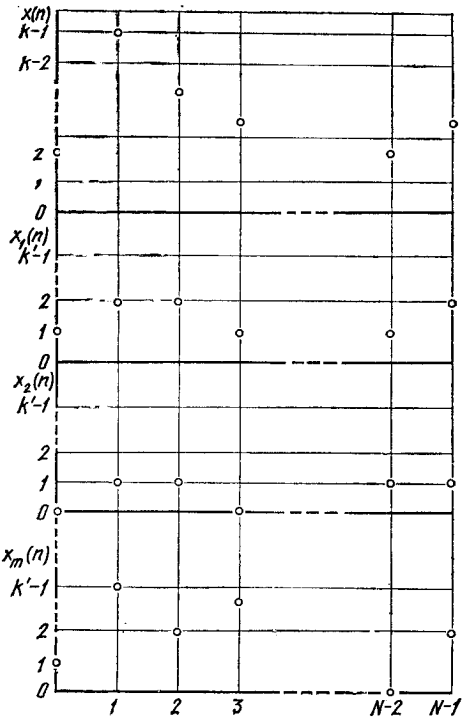


Рис. 1. Графическое изображение непрерывного (*а*), дискретизованного по времени (*б*), квантованного по уровню (*в*) и цифрового (*г*) сигналов.

Рис. 2. Декомпозиция цифрового сигнала.



Анализ и обработка сигналов могут производиться с помощью различных технических средств: аналоговых (непрерывных), цифровых, гибридных (сочетающих в себе как аналоговые, так и цифровые блоки). Сигналы в гибридных вычислительных устройствах могут представляться как в цифровой, так и в аналоговой форме [110, 131, 132, 139]. Непрерывный сигнал, определяемый выражениями (1.1) и (1.2), непосредственно может обрабатываться с помощью аналоговых средств. Для того чтобы можно было обработать этот сигнал с помощью цифровых средств, он подвергается специальным преобразованиям: дискретизации во времени и (или) квантованию по уровню (значению). Этот процесс называется аналого-цифровым преобразованием, а устройства, его осуществляющие — аналого-цифровыми преобразователями [42, 102, 154]. В этой связи сигналы подразделяют на непрерывные, дискретные, квантованные и цифровые. Аргумент непрерывного сигнала (рис. 1, *а*) и значения самого сигнала являются

кантинуальными величинами. Этот сигнал, дискретизованный во времени (рис. 1, *б*), представляется своими значениями только в некоторые фиксированные моменты времени. Область значений является континуумом. Моменты времени при дискретизации отстоят друг от друга на интервал Δt. Для того чтобы по полученным при дискретизации отсчетам сигнала можно было восстановить исходный сигнал $x(t)$, необходимо, чтобы величина интервала Δt удовлетворяла условиям теоремы Кательникова [66, 84]. При этом предполагается, что сигнал $x(t)$ имеет ограниченный спектр.

Сигнал, полученный в результате квантования непрерывного сигнала $x(t)$ (квантованный сигнал) (рис. 1, *в*), принимает фиксированные (квантованные) значения, отстоящие друг от друга на некоторый интервал Δx. Заметим, что такого вида сигналы представляют информацию в цифровых многозначных элементах и структурах [143]. В частном случае, когда значность сигнала равна 2, т. е. квантованный сигнал может принимать только два значения, кодируемые цифрами 0 и 1, получаем информационный сигнал двоичной вычислительной структуры.

Цифровой сигнал [12, 160], который получается в результате дискретизации во времени и квантования по уровню непрерывного сигнала (рис. 1, *г*), можно представить с помощью таблицы цифр. Причем любой непрерывный сигнал с ограниченным спектром может быть представлен цифровым сигналом с любой степенью точности. В работе [54] отмечается, что вследствие ограниченной точности измерений человек фактически воспринимает в дискретном виде даже непрерывную информацию. Поэтому цифровое представление информации (сигналов) является универсальным.

На практике сигнал $x(t)$ определен не для всех значений t, а только для некоторого ограниченного интервала. Именно такие сигналы мы будем рассматривать. В случае цифрового сигнала интервал определения, как и интервал значений, получается конечным.

Определение 1.1. Цифровым сигналом $x(n)$ называется отображение $x : E_N \to E_k$, где $E_N = \{0, 1, 2, .., N-1\}$ — множество, в котором принимает значения аргумент цифрового сигнала n, $n \in E_N$; $E_k = \{0, 1, 2, ..., k-1\}$ — множество значений цифрового сигнала $x(n) \in E_k$.

В дальнейшем, когда не могут возникнуть недоразумения, приставку «цифровой» будем опускать и называть цифровые сигналы просто сигналами. Кроме того, иногда множество E_n называют конечным интервалом изменения переменной n, или просто интервалом N.

В случае равенства $E_N = E_k$ определение 1.1 совпадает с определением функции k-значной логики одной переменной $f(n)$ [179]. Если $E_N \supset E_k$, то можно считать, что $f(n)$ может принимать не все значения из E_k; если $E_k \supset E_N$, то $f(n)$ определена не для всех значений из E_N. Такой подход полезен при гармоническом анализе сигналов, аппаратурной реализации устройств для ЦОС [29, 30, 91, 92] и используется в настоящей работе.

На рис. 2 показан некоторый цифровой сигнал $x(n)$. При $N = k$ этот сигнал отождествляется с функцией k-значной логики одной

переменной. В принципе, в таком виде сигнал $x(n)$ может быть представлен в цифровом вычислительном устройстве, если это устройство работает в системе счисления с основанием, равным k (информация в нем представляется k различными уровнями). Однако на практике значность k функции $x(n)$ может принимать большие значения (десятки, сотни уровней), реализация которых с помощью полупроводниковой схемотехники затруднена в связи с технологическими ограничениями. Как правило, основание системы счисления вычислительного устройства k' значительно меньше k и выбирается в пределах 2—5, т. е. каждое значение сигнала $x(n)$ представляется m-разрядным числом в системе счисления с основанием k' ($m = \log_{k'} k$). Это значит, что функция k-значной логики, представляющая сигнал, выражается в виде композиции m функций, значность которых равна k' (см. рис. 2). Закон композиции функций $x_1(n)$, $x_2(n)$, ..., $x_m(n)$ может быть различным. В простейшем случае

$$x(n) = \sum_{i=0}^{m} x_i(n), \quad n = 0, 1, \ldots, N-1. \tag{1.3}$$

Каждый сигнал $x_i(n)$ является элементарным для вычислительной структуры и представляется в ней с помощью квантованного по уровню сигнала (см. рис. 1, *в*). Эти сигналы подвергаются преобразованиям в зависимости от реализуемых алгоритмов обработки.

Наименее жесткие требования к технологическим параметрам полупроводниковых элементов, на основе которых реализуются вычислительные устройства, имеют место при $k = 2$. Это и объясняет развитие в первую очередь двоичной элементной базы и вычислительных устройств на ее основе. Однако совершенствование технологии позволяет реализовать число уровней, больше 2 ($k = 3 \div 5$). Применение только двух уровней для кодирования информации в вычислительной структуре во многих случаях является неоправданным недоиспользованием точностных возможностей полупроводниковых структур. Переход к более высокой значности позволяет радикально уменьшить число межсхемных соединений и внешних выводов интегральных микросхем, сократить аппаратурные затраты и повысить быстродействие.

Как видно из приведенных выше примеров и определения, цифровые сигналы в общем случае могут принимать несколько значений, т. е. являются многозначными. Широко распространенные цифровые двоичные сигналы (и соответствующие технические средства) — частный, хотя и, несомненно, важный случай многозначных сигналов и систем. Обработка многозначных цифровых сигналов [136, 138] является в последнее время объектом повышенного интереса специалистов в связи с теми выгодами, которые обеспечивает многозначное представление информации. Создание структур вычислительной техники, оптимальных по совокупности технических параметров, наиболее естественно решается именно при использовании многозначного представления информации. В случае применения многоуровневых сигналов значность систем занимает промежуточное значение между 2 (цифровые двоичные системы) и бесконечностью (аналоговые систе-

мы). При этом можно суммировать положительные признаки обеих этих систем — высокую устойчивость работы, обусловленную отсутствием накопления погрешностей, и высокие относительные функциональные возможности, позволяющие рационально решать проблемы соединений.

2. Задачи и методы обработки сигналов

Обработкой сигнала называют процесс преобразования сигнала, исходящего от источника информации, с целью освобождения от различного рода помех и от информации, вносимой косвенным характером измеряемого физического процесса и нелинейными характеристиками датчиков, а также с целью представления полезной информации в наиболее удобной форме [82, 100, 135]. Очевидно это определение нельзя считать приемлемым для всех случаев. Однако в рамках рассматриваемых в настоящей книге задач приведенное определение обработки сигналов является удовлетворительным.

На рис. 3 показана схема, поясняющая принцип обработки сигналов [100, 135]. Сигнал появляется в результате измерения или наблюдения параметров физического объекта (источника информации). Для передачи и хранения сигнал преобразуется в удобную для этой цели форму посредством кодирования. При этом неизбежно вносится шум, так как практически всегда наблюдается неполная адекватность получаемого представления сигнала по отношению к истинному сигналу. Шум вносится также в результате передачи и приема сигнала. Кроме того, в результаты измерения может вноситься информация, которая является следствием косвенного характера измеряемого процесса, несовершенства датчиков и др. Процесс обработки сигнала происходит в приемнике, и целью данного процесса является наилучшее восстановление первоначального сигнала. Если сигнал представляется в цифровой форме и в таком виде подвергается обработке, то говорят о цифровой обработке сигналов — ЦОС.

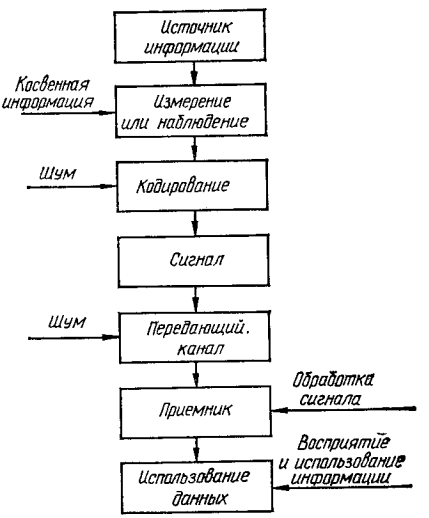


Рис. 3. Условная схема процесса обработки сигнала.

Появление теории цифровых сигналов обусловлено появлением ЦВМ и возможностью решения с их помощью задач обработки сигналов. Развитие цифровой вычислительной техники позволило создать дешевые и надежные специализированные устройства для ЦОС, а также комплексы, состоя-

щие из ЦВМ и специализированных устройств. Изучение и разработка методов ЦОС, а также методов построения соответствующих аппаратных средств составляют предмет научной дисциплины, именуемой ЦОС. Следует заметить, что более удачным является название «обработка цифровых сигналов» [12]. Однако термин «цифровая обработка сигналов» укоренился в отечественной литературе и мы будем им пользоваться наряду с термином «обработка цифровых сигналов».

Задачи ЦОС можно формализовать. В процессе цифровой обработки сигнал $x(n)$ подвергается дискретному преобразованию:

$$\hat{x}(n) = \Phi[x(n)] = \varphi_1\{\varphi_2\{\ldots\ \varphi_m[x(n)]\ \ldots\}\}. \qquad (1.4)$$

На преобразование $\Phi[\ ]$ пока не будем накладывать никаких ограничений. В общем случае — это нелинейное преобразование, которое может состоять из цепочки последовательно проводимых преобразований общего вида (см. (1.4)). В результате преобразования (1.4) находим обработанный сигнал $\hat{x}(n)$. Пусть $\tilde{x}(n)$ — первоначальный сигнал, полученный от источника информации и преобразованный в цифровую форму. В работе [82] вводится понятие расстояния между сигналами $\tilde{x}(n)$ и $\hat{x}(n)$ — $\rho[\tilde{x}(n), \hat{x}(n)]$ и задача обработки трактуется как нахождение экстремума функционала, описывающего это расстояние. Экстремум находится выбором соответствующего преобразования $\Phi[x(n)]$.

Основным методом, применяемым в ЦОС, является метод математического моделирования, так как построение моделей позволит надежно описывать сигналы и системы [82, 83, 104, 122]. С учетом математической модели сигнала и задач обработки строится математическая модель процесса ЦОС. Если эта модель будет реализована в виде отдельного специализированного устройства, то ее можно рассматривать как модель системы ЦОС. Очевидно, различие между математическими моделями процесса и системы ЦОС условно и обусловлено конкретной реализацией. В принципе различия нет. Отметим, что математическая модель системы ЦОС может быть реализована с помощью универсальной ЦВМ. Конкретный вид реализации определяется с учетом требований к производительности системы, быстродействию, конструктивному исполнению, гибкости (возможности перестройки на реализацию различных моделей процессов ЦОС) и др.

В последнее время ЦОС занимает доминирующее положение в связи с ее неоспоримыми достоинствами — точности и гибкости обработки. Кроме того, в связи с развитием средств цифровой вычислительной техники системы ЦОС становятся все дешевле и компактнее [93]. Совершенствуются методы ЦОС. Например, в последнее время реализуются методы ЦОС с помощью аналоговых средств [173, 176]. При этом получаются системы, воплощающие в себе положительные качества как цифровых, так и аналоговых устройств.

Эффективность ЦОС полностью определяется объемом вычислений, который получается при реализации математической модели процесса ЦОС с помощью ЦВМ или специализированного вычислительного устройства. Снижение объема вычислений приводит к уменьшению

аппаратурных затрат при реализации системы ЦОС в виде специализированного устройства или к уменьшению затрат машинного времени при реализации модели на ЦВМ. Следовательно, разработка и исследование методов построения оптимальных с точки зрения минимума объема вычислений при реализации математических моделей систем ЦОС являются актуальной и важной задачей.

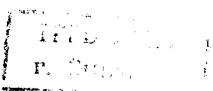
3. Виды моделей систем ЦОС

Математические модели систем ЦОС можно классифицировать по нескольким признакам. Например, известна классификация с точки зрения вида решаемых задач, с точки зрения вида математического аппарата, применяемого для описания сигнала, и др.

Классы моделей, отличающиеся по виду решаемой задачи, весьма разнообразны и зависят от конкретной задачи и типа физического сигнала. Например, при обработке двухмерных сигналов (изображений) выделяют модели улучшения, реставрации и анализа изображений [60, 129, 130, 180]. Каждый из этих классов содержит ряд подклассов. Так, класс моделей улучшения изображений можно разделить на подклассы моделей изменения контраста, подчеркивания контуров изображений, устранения импульсных помех и др. Число примеров можно было бы без труда увеличить, рассматривая различные физические сигналы. Однако и приведенных примеров достаточно для понимания существа вопроса. Отметим еще только классы моделей, применяемых при обработке многих видов физических сигналов. К таковым относятся классы моделей линейной фильтрации, некоторых видов нелинейной фильтрации, спектрального анализа, определения статистических характеристик и др.

По виду применяемого для описания сигнала математического аппарата модели систем ЦОС подразделяются на две большие группы: детерминированные и статистические. В свою очередь, каждый из этих классов можно разделить на подклассы в зависимости от конкретной задачи и используемых математических методов и теорий. Выбор модели зависит от ее точности (адекватности оригиналу) и от структуры алгоритма, получающегося при реализации модели с помощью ЦВМ или специализированных вычислительных устройств. На выбор математического аппарата, применяемого для построения модели ЦОС, влияет вид аппаратных средств, с помощью которых осуществляется реализация этой модели. В большинстве случаев вид используемой элементной базы и связанный с этим вид системы обработки сигналов (аналоговая, гибридная, цифровая) определяются заранее с учетом класса решаемых задач, требований к производительности, быстродействию и т. д. [110, 126]. В зависимости от вида реализующей системы изменяется и математическая модель. С этой точки зрения модели удобно подразделить на непрерывные, непрерывно-цифровые и цифровые.

Непрерывные модели строятся с помощью аппарата непрерывной математики и реализуются аналоговыми средствами.



В непрерывно-цифровых моделях учитывается эффект дискретизации сигнала во времени. Аппарат непрерывной математики заменяется аппаратом дискретной математики (интегралы заменяются суммами, дифференциальные уравнения — разностными и т. д.). Для реализации таких моделей с помощью ЦВМ необходимо произвести квантование сигналов по уровню, т. е. осуществить полностью процесс АЦП, записав выборочные значения непрерывного сигнала в виде кодовых комбинаций. Таким образом, получаем цифровой сигнал. Далее строится и реализуется цифровая модель. В теории ЦОС рассматриваются цифровые модели. Методы построения и реализации таких моделей в основном исследуются и в настоящей работе, т. е. предполагается, что система обработки сигналов реализуется с помощью цифровых аппаратных средств либо с помощью ЦВМ. Отметим, однако, что ЦОС можно осуществить, применяя аналоговые [173, 176], а также гибридные [110, 132, 138] аппаратные средства. В ряде случаев при таком подходе получаются системы ЦОС, оптимальные по точности, быстродействию и аппаратурным затратам.

4. Абстрактные алгебраические системы и ЦОС

Как упоминалось в предыдущем параграфе, основными факторами, определяющими выбор математического аппарата для построения модели системы обработки сигналов, являются адекватность модели оригиналу (точность модели) и вид элементной базы, с помощью которой осуществляется реализация данной модели. При реализации модели с помощью цифровых аппаратных средств необходимо учитывать эффекты дискретизации и квантования сигнала. Учет эффекта дискретизации сигнала во времени привел к необходимости применения при построении моделей нового математического аппарата — аппарата дискретной математики. До последнего времени эффект квантования учитывался простой аппроксимацией действительных чисел рациональными с заданной величиной погрешности. При этом не полностью использовались характер и свойства цифрового представления сигналов при построении модели. Тот факт, что значения сигнала принимают целочисленные уровни, позволяет использовать при построении моделей математический аппарат, отличный от классического и применяемого до сих пор (аппарат абстрактный алгебраических систем, в частности, аппарат конечных полей и колец). В результате можно добиться уменьшения объема вычислений при реализации модели. Этот вывод подтверждается первыми полученными результатами, связанными с использованием абстрактных числовых систем в ЦОС [2], а также вырастающим числом публикаций по этому вопросу [15, 28—30, 51, 89, 92, 99, 190, 195, 196, 199, 206]. Рассмотрим принцип использования аппарата абстрактных алгебраических систем при построении моделей систем ЦОС.

Значения сигнала $x(n) \in E_k$ являются подмножеством поля комплексных чисел C. Обычно (по аналогии с построением непрерывных моделей) преобразования $\varphi_i[\ \ ]$, $i = 1, 2, \ldots, m$, задаваемые выраже-

нием (1.4), определяются над этим полем, т. е. поле C используется для определения преобразований, применяемых при построении математической модели ЦОС. Следовательно, реализация таких моделей связана с реализацией арифметических операций поля комплексных чисел, что нельзя считать удачным. Действительно, сигнал $x(n)$, полученный в результате АЦП, представляет собой список чисел, объем информации которого — конечная и вполне определенная величина. Осуществив преобразование этого сигнала в соответствии с выражением (1.4), получим сигнал $\hat{x}(n)$, числовое представление которого обладает теоретически бесконечным объемом информации, так как в результате определения модели $\Phi[\hat{x}(n)]$ над бесконечным полем C значения $\hat{x}(n)$ умножаются (и суммируются) на коэффициенты из C, часто являющиеся иррациональными числами. Известно, что иррациональное число выражается бесконечной дробью, что приводит к бесконечному объему информации цифрового представления сигнала. Практически объем информации такого представления конечен, но больше первоначального и определяется точностью представления чисел в ЦВМ или, другими словами, длиной разрядной сетки. Длина разрядной сетки для представления результатов промежуточных вычислений обычно в два и более число раз превышает длину разрядной сетки, представляющей входные данные. Значит, благодаря такому построению моделей непроизвольно вводится информационная избыточность и усложняются вычисления, так как они проводятся в поле комплексных чисел.

Отметим, что значения сигнала $\hat{x}(n)$, полученного в результате обработки, в ряде случаев (например, при обработке изображения) не являются подмножеством поля C, а принадлежат множеству E_k, как и значения входного сигнала $x(n)$. Определение модели $\Phi[x(n)]$ над бесконечным полем C, элементы которого можно трактовать как векторы двухмерного пространства, приводит к значительному увеличению объема вычислений. Ниже будет показано, что даже если значения сигнала $\hat{x}(n)$ принадлежат полю C, то определение модели $\Phi[x(n)]$ над C не является обязательным. В поле C можно преобразовать только выходные данные.

Описанный выше подход к построению моделей ЦОС, основанный на использовании поля комплексных чисел для определения над ним преобразований, которым подвергается цифровой сигнал, не является единственным и обязательным. Значения сигнала $x(n)$ можно рассматривать не только как подмножество поля комплексных чисел, но и как подмножество других алгебраических систем, обладающих структурой кольца или поля, в том числе и конечных (например, конечное кольцо вычетов по модулю целого числа, конечное поле Галуа). Отметим, что в этом случае вносимая информационная избыточность может быть минимальной. Разрядная сетка для представления результатов промежуточных вычислений может быть не больше разрядной сетки, представляющей входные данные. Реализация арифметических операций конечного поля или кольца значительно проще по сравне-

нию с реализацией операций поля комплексных чисел. Элементы поля Галуа или конечного кольца вычетов обычно кодируются целыми числами. Операции сложения и умножения в этих системах представляют собой операции сложения и умножения по модулю целого числа, т. е. практически операции производятся над целыми, а не комплексными числами. Следовательно, мы вправе ожидать, что реализация моделей ЦОС, определенных над конечным полем или кольцом, окажется проще по сравнению с реализацией моделей, определенных над полем комплексных чисел. Действительно, для ряда задач ЦОС получается более простая реализация.

Наряду с указанными достоинствами моделей систем ЦОС, заключающимися в снижении объема вычислений при реализации, очевидны и недостатки. Основной недостаток — отсутствие привычного физического смысла у результатов вычислений в конечных полях и кольцах, что затрудняет интерпретацию промежуточных результатов. Для некоторых задач ЦОС это ограничение может быть существенным. Однако для большинства случаев эффективным оказывается преобразование результатов промежуточных вычислений из конечного поля в поле комплексных чисел с целью физической интерпретации. Далее результаты (после интерпретации) могут преобразовываться в конечное поле для дальнейшей их обработки.

Другим недостатком является необходимость разработки арифметических устройств для эффективной реализации операций конечного поля или кольца, которые представляют собой часть системы ЦОС, реализующей модели, определенные над указанными алгебраическими системами. Кроме того, требуется изучение теории конечных полей и колец для возможности разработки математического обеспечения.

* * *

Таким образом, исходя из изложенного в данной главе, можно сделать следующие выводы:

прямое перенесение методов построения моделей систем обработки аналоговых сигналов на построение моделей систем ЦОС неэффективно;

эффекты квантования сигнала по уровню учитываются не полностью. Более полный их учет путем определения математической модели системы ЦОС над конечным полем или кольцом позволит сократить объем вычислений при реализации;

методы построения моделей систем ЦОС, определенных над абстрактными алгебраическими системами, развиты частично. Их дальнейшее развитие является актуальной задачей в связи с необходимостью снижения объема вычислений при решении многих задач ЦОС в различных областях исследований.

ГЛАВА 2

ОСНОВЫ ТЕОРИИ КОНЕЧНЫХ ГРУПП, КОЛЕЦ И ПОЛЕЙ

1. Понятие алгебраической системы

В этой главе проводится общее определение алгебраической системы и алгебры [101].

Определение 2.1. Отображение $f: A \times A \times \ldots \times A \to A$ называется n-арной операцией на множестве A.

Обычно n-арную операцию записывают в виде функции от n переменных: $y = f(x_1, x_2, \ldots, x_n)$, где $y, x_1, x_2, \ldots, x_n \in A$. С системотехнической точки зрения n-арной операции соответствует $(n, 1)$-полюсник (рис. 4), на вход которого поступает n элементов $x_1, x_2, \ldots, x_n$ из множества A, а на выходе — один элемент $y \in A$, функционально связанный отображением f с входными элементами.

Любое подмножество P множества $\underbrace{A \times A \times \ldots \times A}_{n}$ называется n-арным отношением. Для обозначения отношений используют записи $P \subset A \times A \times \ldots \times A$ или $P(x_1, x_2, \ldots, x_n)$. Вторая запись означает, что элементы $x_1, x_2, \ldots, x_n$ находятся друг с другом в отношении P.

Определение 2.2. Индикаторная функция (рис. 5) подмножества P называется n-арным предикатом.

Предикат обычно обозначается тем же символом, что и отношение P:

$$P: A \times A \times \ldots \times A \to \{0, 1\}.$$

Предикат можно трактовать как логическую часть оператора условного перехода (рис. 6), на вход которого поступает n элементов $x_1, x_2, \ldots, x_n$ из множества A. Логическая часть оператора условного перехода определяет, находятся ли элементы $x_1, x_2, \ldots, x_n$ в отношении P или нет.

Определение 2.3. Алгебраической системой называется тройка объектов $U = \langle A, \Omega_F, \Omega_P \rangle$, где A — основное множество; $\Omega_F = \{f_0, f_1, \ldots, f_i, \ldots\}$ — множество n_i-арных операций, определенных на множестве A; $\Omega_P = \{P_0, P_1, \ldots, P_j, \ldots\}$ — множество m_j-арных предикатов, определенных на A.

Типом τ алгебраической системы U называется набор арностей операций и предикатов:

$$\tau = \langle n_0, n_1, \ldots; m_0, m_1, \ldots \rangle.$$

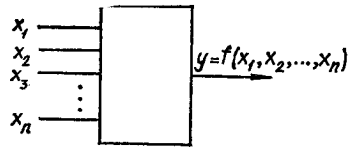
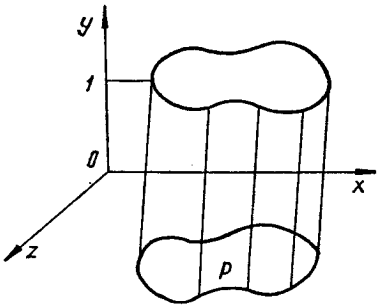
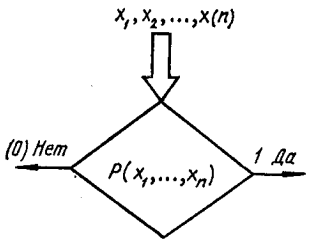


Рис. 4. Изображение n-арной операции в виде $(n, 1)$-полюсника.

Рис. 5. Изображение индикаторной функции отношения.

Рис. 6. Изображение n-арного предиката в виде логической части оператора условного перехода.





Определение 2.4. Алгебраическая система называется алгеброй, если на множестве A определены только одни операции $U = \langle A, \Omega_F \rangle$, и реляционной моделью, если определены только одни предикаты $U = \langle A, \Omega_P \rangle$. Алгебра $U = \langle A, \Omega_F \rangle$ называется конечной, если множество A — конечно.

Наиболее простыми алгебрами являются алгебры типа $\langle 2 \rangle$, которые состоят из множества A и определенной на нем одной бинарной операции.

Примерами алгебр могут служить группы, кольца, поля [8, 26, 72, 81, 85, 96, 101].

2. Группы

Исследование различных свойств чисел и алгебраических уравнений привело к необходимости выделения особого математического объекта — множества с заданными на нем алгебраическими операциями. Напомним, что отображение

$$A \times A \to A \tag{2.1}$$

называется законом композиции (на множестве A в себя), или бинарной операцией.

Если $x, y \in A$, то образ пары (x, y) при отображении (2.1) называется также ее произведением относительно закона композиции и обозначается через $x * y$. Звездочкой обозначается закон композиции, который может быть различным (например, сложение, умножение на множестве действительных чисел и т. д.); употребляются и другие обозначения (например, точка $\cdot$, кружок $\bigcirc$, крестик $+$ и др.; иногда знак вообще опускается и записывают $z = xy$).

Для задания бинарной операции составляют таблицу операции (табл. 1). Строки и столбцы этой таблицы нумеруют элементами мно-

Таблица 1. Таблица Кэли бинарной операции на конечном множестве

$\cdot$	a_1	a_2	a_3	...	a_n
a_1	a_1a_1	a_1a_2	a_1a_3	...	a_1a_n
a_2	a_2a_1	a_2a_2	a_2a_3	...	a_2a_n
a_3	a_3a_1	a_3a_2	a_3a_3	...	a_3a_n
...	...	...	...	...	...
a_n	a_na_1	a_na_2	a_na_3	...	a_na_n

жества A. На пересечении строки и столбца ставится соответствующий результат операции. Эта таблица называется таблицей Кэли данной операции [96, 101].

Пусть множество G конечно и состоит из n элементов. Сколькими способами можно задать на этом множестве алгебраическую операцию? Это легко выяснить с помощью таблицы Кэли, где имеется n^2 мест, на каждом из которых может стоять любой из n элементов. Значит, всего есть n^{n^2} возможностей. Однако большинство операций, заданных таким образом, оказывается «неинтересными». Для содержательного изучения на операцию нужно наложить ограничения, чтобы ее свойства не слишком отличались от свойств тех операций, которые уже встречались (например, от свойств операций сложения, умножения, рассматриваемых на множестве рациональных чисел).

Первым важнейшим ограничением является ассоциативность. Операция называется ассоциативной, если для любых трех элементов a, b, c из множества G имеет место равенство $a\,(bc) = (ab)\,c$.

Нетрудно доказать, что если операция ассоциативная, то два произведения, составленные из одинаковых сомножителей и отличающиеся только расстановкой скобок, всегда равны. Например:

$$(ab)\,(cd) = a\,((bc)\,d) = (abc)\,d = abcd$$

и т. д. Поэтому скобки можно опускать и записать это произведение просто как $abcd$.

Следующим важным свойством операции является существование нейтрального элемента. Элемент e называется нейтральным, если для любого $a \in A$ имеем $ea = ae = a$. Нейтральный элемент может быть только один, так как если e' — другой такой элемент, то $e = ee' = e'$.

Определение 2.5. Группой называется алгебра с одной бинарной операцией, удовлетворяющая следующим аксиомам: бинарная операция ассоциативна; группа обладает единичным элементом; для каждого элемента группы x существует обратный элемент $y * x = e$.

Группу с бинарной операцией $*$, определенной на множестве G, будем обозначать $\langle G, * \rangle$ или просто G, если из текста ясно, о какой бинарной операции идет речь. Множество G, на котором определена бинарная операция группы, называется носителем группы.

Таблица 2. **Таблица Кэли групповой операции $\oplus$ на множестве G_m**

$\oplus$	0	1	2	...	$m-1$
0	0	1	2	...	$m-1$
1	1	2	3	...	0
2	2	3	4	...	1
...	...	...	...	...	...
$m-1$	$m-1$	0	1	...	$m-2$

Определение 2.6. Группа $\langle G, * \rangle$ называется коммутативной, или абелевой, если для двух произвольных элементов $x, y \in G$ справедливо равенство $x * y = y * x$, и конечной, если множество G конечно.

Как будет показано ниже, абелевы группы имеют большое прикладное значение в теории ЦОС. В области определения цифрового сигнала можно рассматривать абелеву группу, если ввести на множестве определения бинарную операцию определенного вида. Такой подход позволил обобщить понятия ортогонального базиса и облегчить изучение ортогональных разложений цифровых сигналов.

Если для обозначения групповой операции абелевой группы $\langle G, * \rangle$ вместо знака $*$ используется знак «$+$», то группа $\langle G, + \rangle$ называется аддитивной группой. Обратный элемент элемента x в этом случае обозначается $-x$. Если используется мультипликативная запись $\langle G, * \rangle$, то обратный элемент обозначается через x^{-1}.

Пример 2.1. Если на множестве $G_m = \{0, 1, 2, ..., m\}$ определить операцию $\oplus$ с помощью табл. 2, то множество G_m становится абелевой группой относительно введенной операции (другими словами, $\langle G_m, \oplus \rangle$ — группа). Операция $\oplus$ является сложением по модулю m. Единичный элемент — 0.

Для элементов группы можно ввести понятие степени с целым показателем, как это обычно делается для чисел. А именно: естественная запись $g^n = g \cdot g \cdot g \cdot ... \cdot g$, а также $g^0 = e$, $g^{-n} = (g^n)^{-1}$. Тогда, конечно, выполняется равенство

$$g^m \cdot g^n = g^{m+n}, \quad m, n \in Z,$$

где Z — группа целых чисел.

В коммутативных группах, в которых групповая операция обозначается знаком «$+$», степени называются кратными элемента g и обозначаются ng.

Пусть $\langle G, * \rangle$ — группа; H — подмножество G, являющееся группой относительно той же групповой операции $*$. Тогда H называется подгруппой группы G. Число элементов в группе G называется ее порядком. Порядок конечной группы конечен. Если порядок группы бесконечен, то она называется бесконечной. Порядок группы G обозначим через $[G : 1]$.

Теорема 2.1. Порядок любой подгруппы конечной группы является делителем порядка группы.

Доказательство данной теоремы опускаем и условимся, что доказательство теорем будет приводиться только в том случае, если в нем содержатся результаты или сведения, необходимые для

понимания дальнейшего текста, или результаты, используемые в последующем изложении.

Пример 2.2. Пусть $G_6 = \langle\{0, 1, 2, 3, 4, 5\}, \oplus\rangle$ — группа порядка 6, операция $\oplus$ которой задается табл. 2 при $m = 6$. Найдем все ее подгруппы. Подгруппами группы G являются группы $\langle\{0\}, \oplus\rangle$, сама группа G_6, а также группы порядка 2 и 3. Легко видеть, что это группы $H_1 = \langle\{0, 3\}, \oplus\rangle$; $H_2 = \langle\{0, 2, 4\}, \oplus\rangle$.

Упражнение 2.1. Составить таблицу Кэли бинарной операции группы G_6. Проверить, что H_1 и H_2 — группы. Составить таблицы Кэли бинарных операций этих групп. Сравнить их с табл. 2.

Элемент g группы G называется элементом конечного порядка (или периодическим), если существует такое натуральное число n, что $g^n = e$. Наименьшее натуральное число с таким свойством называется порядком элемента g, или его периодом, и обозначается $T(g)$ или Ord (g). Группа, в которой все элементы конечного порядка, называется периодической. В любой группе по крайней мере один элемент конечного порядка — e.

Теорема 2.2. Всякая конечная группа периодична.

Доказательство. Пусть в группе G всего m элементов. Рассмотрим степени фиксированного элемента $g \in G$:

$$e = g^0, \quad g^1, \; g^2, \; \ldots, \; g^m, \; g^{m+1}, \; \ldots$$

Поскольку группа G конечная, то в этом ряду найдутся такие элементы g^k и g^r, что $g^k = g^r$. Умножая слева на g^{-k}, получаем $g^{r-k} = e$, что и требовалось доказать.

Пример 2.3. Определим порядок каждого элемента группы из примера 2.2. Для этого найдем степени каждого элемента:

0 : $0 = 0 = 0$, порядок 1;
1 : $1; \; 1 \oplus 1 = 2; \; 2 \oplus 1 = 3; \; 3 \oplus 1 = 4; \; 4 \oplus 1 = 5; \; 5 \oplus 1 = 0$, порядок 6;
2 : $2; \; 2 \oplus 2 = 4; \; 4 \oplus 2 = 0$, порядок 3;
3 : $3; \; 3 \oplus 3 = 0$, порядок 2;
4 : $4; \; 4 \oplus 4 = 2; \; 2 \oplus 4 = 0$, порядок 3;
5 : $5; \; 5 \oplus 5 = 4; \; 4 \oplus 5 = 3; \; 3 \oplus 5 = 2; \; 2 \oplus 5 = 1; \; 1 \oplus 5 = 0$, порядок 6.

Теорема 2.3. Порядок каждого элемента конечной группы G является делителем порядка G.

Доказательство теоремы опускаем.

Если в группе G существует такой элемент a, что $G = \{e, a_1, a^2, \ldots, a^{n-1}\}$ и $n = [G : 1]$ $(a^n = e)$, то группа G называется циклической группой, порожденной элементом a.

Теорема 2.4. Для произвольного целого числа a существует циклическая группа порядка a.

Теорема 2.5. Все конечные группы, порядок которых является простым числом, циклические.

Упражнение 2.2. Построить циклическую группу порядка 7, задав в виде таблицы ее бинарную операцию.

3. Изоморфизм, гомоморфизм

В предыдущем параграфе установлен ряд свойств групп. Однако еще почти ничего не известно о том, какие бывают группы, в частности, сколькими способами можно на данном множестве определить групповую операцию, насколько полученные группы могут отличаться друг от друга и т. п. Попытаемся описать таблицы Кэли групп малых порядков. Вначале установим некоторые общие свойства таблиц Кэли групп:

1) из существования нейтрального элемента следует, что в таблице Кэли есть столбец и строка (будем считать, что это первый столбец и первая строка), в которых элементы стоят «по порядку» (см. табл. 2);

2) из однозначности разрешимости уравнения $ax = b$ и $yx = b$ следует, что в каждой строке (каждом столбце) таблицы содержатся все элементы группы и притом по одному разу.

Пусть группа G состоит из двух элементов. Один из них нейтральный e, другой обозначим через a. Тогда можно заполнить таблицу Кэли (табл. 3). Первые строка и столбец составлены согласно свойству ассоциативности, единственное оставшееся место заполняется так, чтобы выполнялось равенство $a \cdot a = e$.

Таким образом, на множестве из двух элементов групповую операцию можно задать не более чем одним способом. Не будет ли множество с бинарной операцией, заданной в табл. 3, группой? Можно было бы проверить закон ассоциативности непосредственно (пришлось бы рассмотреть 8 случаев). Однако проще воспользоваться косвенными соображениями. Если бы операция, заданная табл. 3, не была ассоциативной, то на множестве из двух элементов никогда нельзя было бы определить групповую операцию. Мы знаем примеры групп второго порядка G_2, группа $G = \langle \{+1, -1\}, \cdot \rangle$ (где $\cdot$ — операция обычного умножения). Значит, таблица Кэли (см. табл. 3) обязана описывать групповую операцию. Итак, мы пришли к выводу, что группы второго порядка существуют и у всех таких групп одинаковые таблицы Кэли.

Таблица 3. **Таблица Кэли бинарной операции группы порядка 2**

*	e	a
e	e	a
a	a	e,

Таблица 4. **Построение таблицы Кэли бинарной операции группы порядка 3**

*	a	a	b
e,	e	a	b
a	a	a^2	ab
b	b	ba	b^2

Таблица 5. **Таблица Кэли бинарной операции группы порядка 3**

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Перейдем к группам третьего порядка. В такой группе кроме нейтрального элемента e есть еще два. Обозначим их через a и b. Начнем составлять таблицу Кэли (табл. 4). Чему может равняться a^2? Это не может быть a (во второй строке a уже есть). Если $a^2 = e$, то во второй строке на оставшемся месте ab должно стоять b, что невозможно, так как в третьем столбце уже есть b. Значит, $a^2 = b$. Тогда остальные места можно заполнить единственным образом (табл. 5). Итак, групп третьего порядка не может быть более одной. Известны примеры групп третьего порядка: группа сложения по модулю 3 $G_3 = \langle\{0, 1, 2\}, \oplus\rangle$, $\langle\{e^{j2\pi/3}\}^\alpha, \cdot\rangle$, где $\alpha = 0, 1, 2$, $j^2 = -1$. Можно привести и другие примеры, и у всех таких групп будут одинаковые таблицы Кэли. Все эти группы отличаются лишь названиями своих элементов. Естественно, что с точки зрения теории групп их следует считать одинаковыми. Это приводит нас к очень важному понятию алгебры и всей математики — понятию изоморфизма.

Определение 2.7. Две группы $\mathfrak{G}_1$, $\mathfrak{G}_2$ называются изоморфными, если существует взаимооднозначное отображение $\varphi : \mathfrak{G}_1 \to \mathfrak{G}_2$, такое, что для любых двух элементов имеет место равенство $\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2)$. Отображение φ в этом случае называют изоморфизмом.

Изоморфизм между двумя группами $\mathfrak{G}_1$ и $\mathfrak{G}_2$ иногда обозначают символом $\mathfrak{G}_1 \sim \mathfrak{G}_2$. Если $\mathfrak{G}_1 = \mathfrak{G}_2$, то изоморфизм называется автоморфизмом. Легко видеть, что изоморфизм сохраняет все свойства операций: он переводит нейтральный элемент в нейтральный, обратный в обратный, элемент конечного порядка — в элемент того же порядка, подгруппу в подгруппу и т. п. Поэтому изоморфные группы имеют совершенно одинаковые свойства и с точки зрения теории групп неразличимы. Однако с прикладной точки зрения изоморфные группы могут представлять значительный интерес, например, при технической реализации групповых операций.

Введем еще понятие, с которым будем иметь дело.

Определение 2.8. Отображение $\varphi : \mathfrak{G}_1 \to \mathfrak{G}_2$ называется гомоморфизмом, если для любых $g_1, g_2 \in \mathfrak{G}_1$

$$\varphi(g_1 * g_2) = \varphi(g_1) * \varphi(g_2).$$

В этом случае отображение может быть не взаимно однозначным.

Пример 2.4. Приведем ряд примеров изоморфных групп. Обозначим через $R(+)$ аддитивную группу действительных чисел, а через $R^+(\cdot)$ — мультипликативную группу положительных действительных чисел. Оказывается, что группы $R(+)$ и $R^+(\cdot)$ изоморфны. Изоморфизм указанных групп хорошо известен: он осуществляется, например, функцией

$$\varphi = \log : R^+(\cdot) \to R(+).$$

Изоморфизм в данном случае означает, что логарифм переводит «умножение положительных действительных чисел в сложение всех действительных чисел».

Упражнение 2.3. Проверить, изоморфны ли группы, приведенные в примере 2.4. Привести пример гомоморфных групп.

Среди всех групп класс абелевых групп играет важную роль. Во-первых, абелевы группы довольно часто встречаются в приложениях, во-вторых, строение абелевых групп куда более прозрачно, чем строение произвольной некоммутативной группы [76]. Это относится особенно к конечным абелевым группам, строение которых обозревается полностью. В общей теории групп теория конечных абелевых групп является примером законченного раздела. Рассмотрим свойства абелевых групп более подробно.

В качестве примеров абстрактных конечных абелевых групп нам уже известны конечные циклические группы G_m для всякого натурального m, изоморфные аддитивной группе классов вычетов по модулю m [81]. Прежде чем перейти к изложению основ теории абелевых групп, покажем, как можно строить новые группы, исходя из некоторого набора известных.

Пусть задано n не обязательно различных групп $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_n$ и пусть $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \ldots \times \mathfrak{G}_n$ — декартово (прямое) произведение множеств $\mathfrak{G}_i$:

$$\mathfrak{G} = \{(g_1, g_2, \ldots, g_n) \mid g^i \in \mathfrak{G}, \quad i = 1, 2, \ldots, \}.$$

В множестве $\mathfrak{G}$ определим умножение согласно выражению

$$(g_1', g_2', \ldots, g_n') * (g_1'', g_2'', \ldots, g_n'') \triangleq (g_1' * g_1'', g_2' * g_2'', \ldots, g_n' * g_n''). \quad (2.2)$$

Тогда справедлива следующая теорема.

Теорема 2.6. Множество $\mathfrak{G}$ с умножением, определяемым выражением (2.2), является группой.

Группа $\mathfrak{G}$ называется прямым (внешним) произведением групп $\mathfrak{G}_1, \mathfrak{G}_2, \ldots, \mathfrak{G}_n$ и обозначается через $\mathfrak{G} = \mathfrak{G}_1 \times \mathfrak{G}_2 \times \ldots \times \mathfrak{G}_n$.

Ясно, что прямое произведение абелевых групп всегда будет абелевой группой. В соответствии с аддитивной записью в абелевых группах говорят не о прямом произведении, а о прямой сумме абелевых групп

$$\mathfrak{G} = \mathfrak{G}_1 + \mathfrak{G}_2 + \cdots + \mathfrak{G}_n.$$

Таким образом, например, из конечных циклических групп можно строить всевозможные прямые суммы циклических групп, чем существенно расширяется класс известных примеров абелевых групп. Оказывается, что таким классом примеров исчерпываются все конечные абелевые группы. А именно имеет место следующая теорема.

Теорема 2.7. Всякая конечная абелева группа H порядка $[H : 1] = h$ является прямой суммой циклических групп порядков, равных степеням простых чисел. Пусть $h = p_1^{h_1} p_2^{h_2} \ldots p_n^{h_n}$ — каноническое разложение числа h в произведения степеней простых чисел. Тогда теорема 2.7 утверждает, что

$$H \sim H_1 + H_2 + \cdots + H_n,$$

где $[H : 1] = h$; $[H_i : 1] = p_i^{h_i}$, $i = 1, 2, \ldots, n$.

Конечная группа H, порядок $[H : 1]$ которой является степенью простого числа p, называется p-группой.

Теорема 2.8. Всякая конечная абелева p-группа H_{p^m} является прямой суммой циклических групп порядков, равных степеням простого числа p, т. е. абелева группа H_{p^m} допускает разложение

$$H_{p^m} = H_{p^{m_1}} + H_{p^{m_2}} + \cdots + H_{p^{m_s}},$$

где $m_1 \geqslant m_2 \geqslant \ldots \geqslant m_s \geqslant 1$ и $m = m_1 + m_2 + \ldots + m_s$.

Последовательность p^{m_1}, p^{m_2}, ..., p^{m_s} называется типом группы H_{p^m}. Таким образом, абелевых p-групп имеется в точности столько, сколько имеется различных разложений натурального числа m в сумму неотрицательных слагаемых. Следовательно, каждая подгруппа H_i ($[H_i : 1] = p_i^{k_i}$) из теоремы 2.7 прямо разложима в сумму циклических групп, которые называются примарными. Это означает, что каждому разложению числа

$$h = p_1^{k_{11}} p_1^{k_{12}} \ldots p_1^{k_{1s_1}} p_2^{k_{21}} p_2^{k_{22}} \cdots p_2^{k_{2s_2}} \ldots p_n^{k_{n_1}} p_n^{k_{n_2}} \cdots p_n^{k_{n s_n}} =$$

$$= p_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$$

$\left(\text{где } \sum_{i=1}^{s_1} k_{1i} = k_1;\ \sum_{i=1}^{s_2} k_{2i} = k_2,\ \ldots;\ \sum_{i=1}^{s_n} k_{n_i} = k_n\right)$ соответствует некоторая абелева группа. Абелевых групп порядка h столько, сколько существует различных разложений числа h.

Пример 2.5. Найдем все абелевы группы порядка 12. Число 12 можно разложить на множители следующими способами:

$$12 = 2 \cdot 2 \cdot 3;\quad 12 = 4 \cdot 3;\quad 12 = 2 \cdot 6;\quad 12 = 12.$$

Этим разложениям соответствуют следующие прямые суммы:

$H_{12} = H_2 + H_2 + H_3$; $H_{12} = H_4 + H_3$; $H_{12} = H_2 + H_6$; $H_{12} = H_{12} \sim G_{12}$.

Перестановка сомножителей в разложении числа h приводит к изоморфным группам, например $H_4 + H_3 \sim H_3 + H_4$.

Упражнение 2.4. Построить таблицы Кэли для различных вариантов разложения группы H_{12} в прямую сумму, приведенных в примере 2.5, приняв $H_2 = G_2$; $H_3 = G_3$; $H_4 = G_4$; $H_6 = G_6$.

Рассмотрим групповые законы в абелевых группах при их прямом разложении. Пусть

$$H_h = H_{h_1} + H_{h_2} + \cdots + H_{h_m} = H_{p_1^{k_1}} + H_{p_2^{k_2}} + \cdots + H_{p_n^{k_n}},$$

где p_i не обязательно все разные.

Тогда все элементы $x \in H_h$ можно представить в виде m-ки:

$$x = (x_1, x_2, \ldots, x_m), \quad x_i \in H_{h_i}, \quad i = 1, 2, \ldots, m.$$

Сложение элементов группы H_h происходит в соответствии со следующими правилами:

$$z = x \oplus y = (x_1, x_2, \ldots, x_m) \oplus (y_1, y_2, \ldots, y_m) =$$

$$= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_m \oplus y_m) = (z_1, z_2, \ldots, z_m),$$

где

$$z_i = x_i \oplus y_i \pmod{h_i}$$

($\pmod{h_i}$ — обозначение операции по модулю целого числа h_i), т. е. в каждой координате идет сложение по своему модулю. Конечно, в некоторых координатах модули могут совпадать.

Если все $h_i = 2$, $i = 1, 2, \ldots, m$, то будем иметь группу двоичных чисел с поразрядным сложением; если $h_i = p$, то имеем группу p-ичных чисел с поразрядным сложением.

4. Поля и кольца (основные сведения)

Поля и кольца являются алгебрами с двумя бинарными операциями. Пусть R — множество, для любых двух элементов которого определены две операции «+, ·».

Определение 2.9. Алгебра $\langle R, +, \cdot \rangle$ называется кольцом, если выполнены следующие условия:

а) $\langle R, + \rangle$ — абелева группа;

б) $\langle R, \cdot \rangle$ — множество с ассоциативной бинарной операцией;

в) для любых трех элементов a, b, и c из R

$$a(b + c) = ab + ac; \quad (a + b)c = ac + bc.$$

Если множество R конечно, то кольцо называется конечным. Если операция «·» коммутативная в кольце, то такое кольцо называется коммутативным. В случае когда в кольце существует единичный элемент относительно операции «·», то это кольцо называется кольцом с единицей.

Если к указанным условиям добавить требование существования обратного элемента для всех $a \neq 0$, то соответствующая алгебра будет называться телом. Если к тому же умножение коммутативно, то такая алгебра называется полем. Итак, мы пришли к следующему определению поля.

Определение 2.10. Алгебра $\langle F, +, \cdot \rangle$ (где F — множество, содержащее по крайней мере 2 элемента, такое, что для любых двух элементов a и b из F определены две операции $+$ и $(\cdot)$) называется полем, если она удовлетворяет следующим условиям:

а) $\langle F, + \rangle$ — абелева группа;

б) $\langle F^*, \cdot \rangle$ — абелева группа, где F^* — множество, полученное удалением из F единичного элемента по сложению.

Любое подмножество P элементов поля F, содержащее 0 и 1, называется подполем поля F, если оно замкнуто относительно операций умножения и сложения. При этом очень часто говорят, что поле F является расширением поля P.

Подкольцо I кольца R называется идеалом в R, если для любых элементов a из I и x из R элементы ax и xa принадлежат I.

Классическим примером кольца является кольцо целых чисел Z. Не менее известными примерами полей являются поля рациональных Q, вещественных R и комплексных C чисел.

Приведенные алгебры (поля и кольца) широко используются в ЦОС. Множество значений сигнала является подмножеством некото-

рого поля или кольца (например, поля комплексных чисел, кольца целых чисел). Особое значение приобретает изучение конечных полей и колец, так как множество значений цифрового сигнала можно рассматривать как подмножество этих систем и можно использовать эти системы при построении математических моделей систем ЦОС.

Для дальнейшего изложения очень важным примером является кольцо $F[x]$ полиномов от одной переменной с коэффициентами из некоторого поля F. Пусть x — некоторый символ, называемый переменной. Под полиномом с коэффициентами из поля F понимается выражение вида

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_m x^m = \sum_{i=0}^{m} a_i x^i,$$

где a_i — коэффициенты полинома, принадлежащие полю F.

Степенью полинома $f(x)$, обозначаемой $\deg(f(x))$, называется наибольший индекс m, такой, что $a_m \neq 0$. Если все коэффициенты a_i равны нулю, то такой полином называется нулевым и степень ему не приписывается. Ненулевой полином записывается обычно в стандартной форме, при которой $a_m \neq 0$, т. е. $m = \deg(f(x))$. Коэффициент a_m называется старшим коэффициентом полинома, а $a_m x^m$ — старшим его одночленом. Если старший коэффициент $a_m = 1$, то полином называется нормированным.

Операция сложения полиномов осуществляется, по определению, «покоэффициентно»; если

$$f(x) = a_0 + a_1 x + \cdots + a_m x^m = \sum_{i=0}^{m} a_i x^i;$$

$$g(x) = b_0 + b_1 x + \cdots + b_n x^n = \sum_{i=0}^{n} b_i x^i,$$

то сумма $h(x) = f(x) + g(x)$ означает полином

$$h(x) = (a_0 + b_0) + (a_1 + b_2)\, x + \cdots + (a_k + b_k)\, x^k = \sum_{i=0}^{\max(m,n)} (a_i + b_i)\, x^i.$$

Умножение полиномов $f(x)$ и $g(x)$ определяется по формуле

$$H(x) = f(x)\, g(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)\, x + \cdots + (a_0 b_r + a_1 b_{r-1} + \cdots$$

$$\cdots + a_2 b_0)\, x^2 + \cdots = \sum_i \sum_j a_i b_j x^{i+j} = \sum_{r=0}^{m+n} \left(\sum_{i=0}^{r} a_i b_{r-i} \right) x^r.$$

После этого можно уже проверить, что совокупность полиномов с коэффициентами из поля F образует кольцо: его обозначают через $F[x]$. Элементы $a \in F$, $a \neq 0$, принято отождествлять с полиномами степени 0 и элемент $0 \in F$ — с нулевым полиномом. Тогда кольцо $F[x]$ содержит поле F в качестве подкольца (очевидно, что любое поле является одновременно и кольцом).

Отметим еще одно важное понятие теории колец — понятие делителя нуля. Элемент $a \in A$, $a \neq 0$ (где A — произвольное кольцо),

называется делителем нуля, если существует элемент $b \in A$, $b \neq 0$, такой, что $ab = 0$. Ясно, что при таком определении элемент b автоматически также становится делителем нуля. Если кольцо A — поле, то, конечно, в нем делителей нуля нет. Говорят, что a делит b (и записывают это утверждение $a \mid b$), если уравнение $ax = b$ имеет решение в кольце A. В кольце с делителями нуля всегда существует несколько решений этого уравнения, что приходит в противоречие со свойствами делимости в кольце целых и вещественных чисел. Здесь решение уравнения $ax = b$ или не существовало, или было единственным.

Пример 2.6. В кольце $\boldsymbol{Z}$ уравнение $4x = 3$ не имеет решения, а уравнение $4x = 24$ имеет единственное решение $x = 6$. В поле вещественных чисел уравнение $ax = b$ ($a \neq 0$) всегда имеет единственное решение. Не так обстоят дела в кольцах с делителями нуля. Пусть $ax = b$ имеет решение $x = ba^{-1}$ и пусть a к тому же является делителем нуля, т. е. $ac = 0$. Тогда, прибавляя к правой и левой частям уравнения $ax = b$ по нулю, имеем $ax + ac = b$. Решая это уравнение относительно x, получаем второе решение $x = \frac{b}{c} - c$.

Ясно, что целесообразно выделить те кольца, которые делителями нуля не обладают. Такие кольца называются областями целостности, или целостными кольцами. К примеру кольцо $\boldsymbol{Z}$ является целостным кольцом. Легко видеть, что для степеней полиномов $f(x)$ и $g(x)$, отличных от нулевого, имеет место равенство

$$\deg(f(x)\, g(x)) = \deg(f(x)) + \deg(g(x)).$$

Отсюда сразу следует, что кольцо $F[x]$ не содержит делителей нуля и является областью целостности.

Делимость в кольце $F[x]$ определяется так: обозначая через $g(x) \mid f(x)$ отношение «$g(x)$ делит $f(x)$», можно написать, что

$$g(x) \mid f(x) \Leftrightarrow f(x) = q(x)\, g(x),$$

т. е. $g(x)$ делит $q(x)$ тогда и только тогда, когда существует такой полином $q(x)$, что имеет место равенство $f(x) = q(x)\, g(x)$. Существенной оказывается возможность деления с остатком в кольце $F[x]$. Если $f(x)$ и $g(x)$ — два полинома из $F[x]$ и $g(x) \neq 0$, то существуют полиномы $q(x)$ и $r(x)$ из $F[x]$, причем или степень полинома $r(x)$ строго меньше, чем степень полинома $q(x)$, или $r(x)$ — нулевой полином, так, что $f(x) = q(x)\, g(x) + r(x)$ и «неполное частное» $q(x)$ и «остаток» $r(x)$ однозначно определены.

Аналогичное утверждение имеет место и в кольце $\boldsymbol{Z}$. Для любого $a \in \boldsymbol{Z}$ и $b \in \boldsymbol{Z}$, $b \neq 0$, существуют такие элементы q и r, что $|r| < |b|$ и $a = qb + r$. Понятию простого числа в кольце $\boldsymbol{Z}$ соответствует понятие неприводимого полинома в кольце $F[x]$. Полином $p(x) \in F(x)$, для которого $\deg(p(x)) > 0$, называется неприводимым в $F[x]$, если он не допускает представления $p(x) = f(x)\, g(x)$, такого, что $\deg(f(x)) < \deg(p(x))$ и $\deg(g(x)) < \deg(p(x))$. В этих терминах, как и в кольце $\boldsymbol{Z}$, имеет место следующая основная теорема.

Теорема 2.9. Всякий полином $f(x) \in F[x]$ может быть представлен в виде произведения

$$f(x) = p_1^{k_1}(x)\, p_2^{k_2}(x) \ldots p_s^{k_s}(x)$$

степеней неприводимых в $F[x]$ полиномов $p_i(x)$, и такое представление можно осуществить лишь единственным образом, если не считать различными представления, отличающиеся друг от друга порядком следования сомножителей.

Ясно, что у неприводимого полинома кольца $F[x]$ нет корней в поле F.

Упражнение 2.5. Проверить, является ли неприводимым полином $x^2 + 1$ над полем R?

Такое глубокое сходство свойств колец Z и $F[x]$ позволяет достаточно просто строить различные алгебраические конструкции в одном кольце, если подобные уже построены в другом. Так, исходя из кольца Z, можно построить кольцо классов вычетов по модулю M и конечные поля Галуа GF (p). Аналогично, исходя из элементов кольца $F[x]$, можно построить кольцо классов вычетов по полиному $M(x)$ и конечные поля Галуа GF (p^n).

Ввиду важности кольца классов вычетов по модулю M, которое обозначается через Z_M, рассмотрим более подробно его свойства.

5. Кольцо вычетов по модулю целого числа

Выше было показано, что основой для построения кольца Z_M является кольцо целых чисел Z. Обычно кольцо Z_M получают в связи с остатками от деления целых чисел на данное положительное число M, которое называют модулем. Каждому целому числу $a \in Z$ отвечает определенный остаток $r = a - mg$, $0 \leqslant r \leqslant M - 1$ от деления его на M, если двум целым числам a и b отвечает один и тот же остаток r, то они называются равноостаточными по модулю M, или сравнимыми по модулю M. Для обозначения сравнимости чисел a и b употребляется символ $a \equiv b \pmod{M}$. Ясно, что $a \equiv b \pmod{M}$ тогда и только тогда, когда разность $a - b$ делится на M. Если $a - b$ не делится на M, то говорят, что a и b несравнимы по модулю M, и записывают это следующим образом: $a \not\equiv b \pmod{M}$.

Отношение сравнимости по модулю M является отношением эквивалентности и разбивает множество всех целых чисел на непересекающиеся классы, причем два целых числа сравнимы между собой по модулю M тогда и только тогда, когда они лежат в одном и том же классе. Эти классы называются классами вычетов по модулю M.

Очевидно, что целые числа $0, 1, \ldots, M - 1$ лежат в разных классах вычетов, а так как каждое целое число сравнимо по модулю с одним из этих чисел, то имеется точно M классов вычетов по модулю M. Пусть $r \in \{0, 1, \ldots, M - 1\}$. Тогда класс вычетов, содержащий число r, состоит из целых чисел вида $r \pm lM$, где l пробегает все целые числа.

Пример 2.7. Пусть $M = 4$. Построим классы вычетов по этому модулю:

$$l_0 = \{\ldots, -8, -4, 0, 4, 8, 12, \ldots\};$$

$$l_1 = \{\ldots, -7, -3, 1, 5, 9, 13, \ldots\};$$

$$l_2 = \{\ldots, -6, -2, 2, 6, 10, 14, \ldots\};$$
$$l_3 = \{\ldots, -5, -1, \ldots, 3, 7, 11, 15, \ldots\}.$$

Подобно обычным равенствам сравнения можно складывать, вычитать и перемножать. Если $a \equiv b \pmod M$ и $c \equiv d \pmod M$, то $a \pm c \equiv b \pm d \pmod M$ и $ac \equiv bd \pmod M$. В общем случае делить сравнения нельзя. Однако обе части сравнения можно сократить на множитель, взаимно простой с модулем. Операции сложения, вычитания и умножения сравнений индуцируют аналогичные операции на множестве классов вычетов. Пусть K_i и K_j — два класса вычетов по модулю M. Каковы бы ни были числа $a \in K_i$ и $b \in K_j$, их сумма $a + b$ всегда лежит в одном и том же классе вычетов K_l, который называют суммой $K_l = K_i + K_j$ классов K_i и K_j. Аналогично определяется произведение K_i и K_j двух классов вычетов по модулю M. Легко проверить, что классы вычетов по модулю M образуют относительно сложения абелеву группу. Нулевым элементом этой группы является класс вычетов, состоящий из всех целых чисел, кратных M, а обратным к классу K_i является класс — K_i, состоящий из всех элементов класса K_i, взятых со знаком минус.

Более того, классы вычетов по модулю M образуют коммутативное кольцо. Единичным элементом служит класс ε, содержащий целое число 1, а дистрибутивный закон $K_1(K_2 + K_3) = K_1K_2 + K_1K_3$ непосредственно следует из дистрибутивного закона для целых чисел. Это кольцо обозначают Z_M.

Любое число класса вычетов по модулю M называется вычетом по модулю M. Вычет r, $0 \leqslant r \leqslant M - 1$, равный остатку от его деления на модуль M, называется наименьшим неотрицательным вычетом. Вычет ρ, наименьший по абсолютной величине, называется абсолютно наименьшим вычетом. При $r < M/2$ имеем $\rho = r$; при $r > M/2$ имеем $\rho = r - m$; наконец, если M четное ($r = M/2$), в качестве ρ можно взять любое из двух чисел $M/2$ или $-M/2$.

Взяв из каждого класса вычетов по одному представителю, получим полную систему вычетов по модулю M. Чаще всего в качестве полной системы вычетов употребляются наименьшие неотрицательные вычеты $\{0, 1, \ldots, M - 1\}$, которые обозначим через $|\cdot|_M^+$, или абсолютно наименьшие вычеты, состоящие из чисел $\{0, \pm 1, \ldots, \pm$ $\pm$ M /2$\}$ в случае нечетного M и чисел $\{0, \pm 1, \ldots, M/2 - 1, M/2\}$, или $\{0, \pm 1, \ldots, \pm (M/2 - 1), -M/2,\}$ в случае четного M, для обозначения которых примем символ $|\cdot|_M^-$. В дальнейшем, говоря о кольце Z_M, будем понимать именно эти системы вычетов с законами сложения и умножения по модулю M.

Пример 2.8. Приведем таблицы бинарных операций кольца Z_M. Таблица операции сложения совпадает с таблицей групповой операции группы G_m (см. табл. 2). Таблица Кэли операции умножения кольца Z_M приведена в табл. 6. Примеры операций колец Z_M для различных значений M даны в табл. 7—12.

Упражнение 2.6. Каков порядок группы, бинарная операция которой задана табл. 6? Проверить выполнение условия $a(b + c) = ab + bc$ для $a, b, c \in Z_M$ (дистрибутивный закон).

Таблица 6. Таблица Кэли операции умножения кольца Z_M

$\odot$	0	1	2	...	$M-1$
0	0	0	0	...	0
1	0	1	2	...	$M-1$
2	0	2	4	...	$M-2$
...	...	...	...	...	...
$M-1$	0	$M-1$	$M-2$	...	1

Таблица 7. Сложение в кольце $Z_5 = |\cdot|_5^-$

$\oplus$	-2	-1	0	1	2
-2	1	2	-2	-1	0
-1	2	-2	-1	0	1
0	-2	-1	0	1	2
1	-1	0	1	2	-2
2	0	1	2	-2	-1

Таблица 8. Умножение в кольце $Z_5 = |\cdot|_5^-$

$\odot$	-2	-1	1	2
-2	-1	2	-2	1
-1	2	1	-1	-2
1	-2	-1	1	2
2	1	-2	2	-1

Классы вычетов по модулю M, элементы которых взаимно просты с M, называют приведенными классами вычетов. Взяв из каждого класса по одному вычету, получим приведенную систему вычетов по модулю M. Например, если по модулю 10 полную систему вычетов выразить при помощи наименьших неотрицательных вычетов, то приведенная система будет состоять из чисел 1, 3, 7, 9.

Важный вопрос о числе вычетов в приведенной системе по модулю M решается при помощи функции Эйлера $\varphi(M)$. Функция Эйлера определяется для всех целых положительных M как число целых положительных чисел, не превосходящих M и взаимно простых с M, или как число чисел ряда 0, 1, 2, ..., M взаимно простых с M. Из этого определения очевидно, что в приведенной системе вычетов по модулю M имеется как раз $\varphi(M)$ чисел.

Пусть $f(x) = a_0x^n + a_1x^{n-1} + \ldots + a_n$ — многочлен с целыми коэффициентами. Решением сравнения $f(x) \equiv 0 \pmod M$ называется такой класс вычетов $x \equiv x_1 \pmod M$, что $f(x_1) \equiv 0 \pmod M$ для целого числа x_1. Обозначим через НОД (a, b) наибольший общий делитель a и b. Если НОД $(a, M) = 1$, то x пробегает приведенную систему вычетов по модулю M. Действительно, чисел $ax + k$ столько же, сколько и чисел x, т. е. $\varphi(M)$. Далее числа $ax + k$ несравнимы между собой по модулю M и взаимно просты с M. Предположим обратное, а именно, что для двух значений x_1 и x_2 из разных классов получаются сравнимые значения для $ax + b$ по модулю M, т. е. что

$$ax_1 + b \equiv ax_2 + k \pmod M.$$

Тогда $ax_1 \equiv ax_2 \pmod M$ и ввиду того, что НОД $(a, M) = 1$, справедливо сравнение $x_1 \equiv x_2 \pmod M$. Получается противоречие с усло-

Таблица 9. Сложение в кольце $Z_6 = \langle \cdot \rangle_6^+$

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Таблица 10. Умножение в кольце $Z_6 = \langle \cdot \rangle_6^+$

$\odot$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Таблица 11. Сложение в кольце $Z_6 = \langle \cdot \rangle_6^-$

$\oplus$	-2	-1	0	1	2	± 3
-2	2	3	-2	-1	0	1
-1	3	-2	-1	0	1	2
0	-2	-1	0	1	2	3
1	-1	0	1	2	3	-2
2	0	1	2	3	-2	-1
± 3	1	2	3	-2	-1	0

Таблица 12. Умножение в кольце $Z_6 = \langle \cdot \rangle_6^-$

$\odot$	-2	-1	1	2	3
-2	2	2	-2	2	0
-1	2	1	-1	-2	-3
1	-2	-1	1	2	3
2	2	-2	2	-2	0
3	0	-3	3	0	3

вием, что и доказывает наше утверждение. Следовательно, сравнение $ax \equiv 1 \pmod{M}$ имеет единственное решение $x \equiv x_1 \pmod{M}$, такое, что НОД $(x, M) = 1$. Другими словами, приведенные классы вычетов по модулю M образуют по умножению абелеву группу порядка $\varphi(M)$, которую обозначим $M(Z_M)$. Для этой группы справедлива следующая теорема.

Теорема 2.10 (теорема Эйлера). Если a взаимно просто с M, то

$$a^{\varphi(M)} \equiv 1 \pmod{M}.$$

Рассмотрим теперь кольцо классов вычетов по простому модулю p. В этом случае все классы вычетов, за исключением нулевого, будут приведенными и, следовательно, образуют по умножению абелеву группу. Таким образом, классы вычетов по простому модулю p образуют конечное поле Галуа GF (p) из p элементов. В этом случае имеет место следующее утверждение, являющееся частным случаем теоремы Эйлера.

Теорема 2.11 (малая теорема Ферма). Если a не делится на простое число p, то $a^{p-1} \equiv 1 \pmod{p}$. Другими словами, каждый элемент поля классов вычетов по простому модулю p удовлетворяет уравнению $x^p - x = 0$.

6. Свойства функции Эйлера. Символы Лежандра и Якоби

Одним из важнейших свойств функций Эйлера является мультипликативность. Напомним, что функция $f(n)$ называется мультипликативной, если она определена для всех натуральных n, хотя бы для одного такого n отлична от нуля и для любых n_1 и n_2, таких, что НОД $(n_1, n_2) = 1$, $f(n_1 n_2) = f(n_1) f(n_2)$.

Выведем формулу для вычисления $\varphi(M)$. Пусть $n = p$ — простое число. Тогда, очевидно, $\varphi(p) = p - 1$. Пусть далее $M = p^\alpha$. Для определения $\varphi(p^\alpha)$ рассмотрим ряд чисел от 1 до p^α, который запишем в следующем виде:

$$1, 2, 3, \ldots, p_1, \ldots, 2p, \ldots, 3p, \ldots, pp, \ldots, p^{\alpha-1}p = p^\alpha.$$

Очевидно, что этот ряд содержит $p^{\alpha-1}$ чисел, которые делятся на p и, следовательно, не являются взаимно простыми с p^α. Остальные числа этого ряда взаимно простые с p^α. Их число

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1 - \frac{1}{p}\right). \tag{2.3}$$

Пусть, наконец, M — произвольное натуральное число и его каноническое разложение:

$$M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}.$$

Тогда по свойству мультипликативности

$$\varphi(M) = \varphi(p_1^{\alpha_1})\,\varphi(p_2^{\alpha_2}) \ldots \varphi(p_k^{\alpha_k}), \tag{2.4}$$

или, подставляя в (2.4) значение $\varphi(p_i^{\alpha_i})$ из (2.3), получаем

$$\varphi(M) = M\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_k}\right).$$

Пример 2.9. Пусть $M = 360$. Найдем $\varphi(360)$. Запишем разложение $360 = 2^3 \cdot 3^2 \cdot 5$. Тогда

$$\varphi(360) = 360\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) = \frac{360 \cdot 1 \cdot 2 \cdot 4}{2 \cdot 3 \cdot 5} = 96.$$

Пусть НОД $(a, M) = 1$. Рассмотрим бесконечную последовательность $a^1, a^2, a^3, a^4, a^5, \ldots$ Согласно теореме Эйлера, $a^{\varphi(M)} \equiv 1 \pmod{M}$. Здесь содержится, очевидно, следующее и более слабое утверждение: если НОД $(a, M) = 1$, то существуют такие натуральные числа γ, что

$$a^\gamma \equiv 1 \pmod{M}. \tag{2.5}$$

Наименьшее из чисел γ, удовлетворяющее выражению (2.5), называется периодом, или показателем, которому a принадлежит по

модулю M. Период обозначим через $\gamma = T(a, M)$. Если $\gamma = T(a, M)$, то числа $1 = a^0$; $a^1, a^2, \ldots, a^\gamma$ являются попарно несравнимыми по модулю M. Далее, если $a^k = 1 \pmod M$, то γ делит k. Очевидно, что $\gamma = T(a, M)$ делит $\varphi(M)$. Если период a по модулю M равен l и НОД $(k, l) = d$, то период элемента a^k по модулю M равен l/d. Наконец, если элемент x по модулю M имеет период T_1, элемент y — период T_2 и НОД $(T_1, T_2) = 1$, то xy имеет период $T_1 T_2$.

В частном случае, когда a по модулю M принадлежит показателю $\varphi(M)$, т. е. $T(a, M) = \varphi(M)$, то a называют первообразным корнем (первообразным элементом) по модулю M. Отсюда следует, что если $a \in \mathrm{GF}(p)$ является первообразным элементом, то $T(a, M) = \varphi(p) = p - 1$. Если $a^k \equiv 1 \pmod M$ и $k = T(a, M)$, то чисто формально можно написать, что $a = \sqrt[k]{1} \in Z_M$. Заметим, что в поле комплексных чисел $\sqrt[k]{1} = e^{j\frac{2\pi}{k}} \in C$ $(j = \sqrt{-1})$. Кроме того, функции $\Psi_\alpha(t) = e^{j\frac{2\pi}{k}\alpha t}$, как известно, образуют ортогональный базис и очень широко применяются при спектральном анализе. Аналогично функции вида $\Psi_\alpha(t) = a^{\alpha t}$ образуют ортогональный базис в пространстве функций, заданных на целочисленном отрезке $[0, T(a, M) - 1]$ и принимающих значение в кольце Z_M, где $T(a, M)$ — период, которому принадлежит a. Получающиеся в этом случае базисы привлекательны тем, что они позволяют избавиться от комплексных умножений на числа вида $e^{j\frac{2\pi}{k}\alpha t}$. Более того, появляется возможность выбрать a в виде степени 2, а реализация умножения на числа такого вида на ЦВМ не представляет особого труда.

Рассмотрим теперь примеры нахождения периода, которому a принадлежит по модулю M. Составим для этого ряд чисел a^1, a^2, a^3, a^4 и т. д., пока впервые не натолкнемся на такое $T(a, M)$, что $T(a, M) = 1 \pmod M$.

Пример 2.10. $a = 2$, $M = 7$. Имеем

$$2^1 = 2; \quad 2^2 = 4; \quad 2^3 = 8 \equiv 1 \pmod 7.$$

Итак, 2 принадлежит периоду 3 по модулю 7. Вместе с тем видно, что 2 не является первообразным корнем по модулю 7.

Пример 2.11. $a_1 = 3$, $a_2 = 5$, $M = 7$. Имеем

$$3^0 = 1; \quad 3^1 = 3; \quad 3^2 = 9 \equiv 2 \pmod 7;$$

$$3^3 = 6; \quad 3^4 = 4; \quad 3^5 = 5; \quad 3^6 = 1 \pmod 7;$$

$$5^0 = 1; \quad 5^1 = 5; \quad 5^2 = 4; \quad 5^3 = 6; \quad 5^4 = 2; \quad 5^5 = 3; \quad 5^6 = 1 \pmod 7.$$

Итак, 3 и 5 принадлежат одному и тому же периоду 6 и являются первообразными корнями по модулю 7 (степени 3 и 5 «пробегают» все значения от 1 до $6 = 7 - 1$). Этот пример показывает, что по одному и тому же модулю бывают разные первообразные корни.

Известно [47], что первообразные корни существуют только для целых чисел M вида $M = 2, 4, p^\alpha, 2p^\alpha$, где p — простое нечетное число и $\alpha \geqslant 1$. Более того, для каждого из этих чисел существует $\varphi(\varphi(M))$ первообразных элементов, если q — один из первообразных

элементов по модулю M, то все первообразные элементы по модулю M представляют собой числа $q^k \pmod M$, где НОД $(k, \varphi(M)) = 1$.

Пример 2.12. Минимальным положительным первообразным элементом по модулю $p=13$ является 2. Следовательно, $2^{12} \equiv 1 \pmod{13}$. Так как $\varphi(\varphi(13)) = \varphi(12) = 4$, то существует четыре первообразных корня для $p = 13$, а именно: $2^1 = 2$; $2^5 = 6$; $2^7 = 11$; $2^{11} = 7$.

Упражнение 2.7. Проверить, что 2; 2^5; 2^7 и 2^{11} действительно являются первообразными элементами по модулю 13. Построить таблицы степеней элементов (значения привести по модулю 13).

Необходимое условие существования в приведенной системе вычетов по модулю M числа a, имеющего период e, можно получить, используя определенную ниже λ функцию Кармайкла. Эта функция определяется на множестве целых чисел M следующим образом:

1) если $M = 2^n$, $n = 0, 1, 2$, то $\lambda(M) = \varphi(M)$;

2) если $M = 2^n$, $n > 2$, то $\lambda(M) = \varphi(M)/2$;

3) если $M = p^\alpha$, $\alpha > 0$, где p — простое число, то $\lambda(M) = \varphi(p^\alpha)$;

4) если $M = 2^n p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, $n \geqslant 0$, $\alpha_i > 0$, где p_i — попарно различные нечетные простые числа, то

$$\lambda(M) = \text{НОК}(\lambda(2^n), \lambda(p_1^{\alpha_1}), \ldots, \lambda(p_k^{\alpha_k})),$$

где НОК $(a_1, a_2, \ldots, a_k)$ обозначает наименьшее общее кратное чисел $a_1, a_2, \ldots, a_k$.

Из определения $\lambda(M)$ и теоремы Эйлера (см. теорему 2.10) следует, что $a^{\lambda(M)} \equiv 1 \pmod M$. Известно, что целое число $a < M$, взаимно простое с M и имеющее период e, существует тогда и только тогда, когда e является делителем $\lambda(M)$. Например, при $M = 45$ $\lambda(45) = \text{НОК}(\lambda(3^2), \lambda(5)) = \text{НОК}(6, 4) = 12$ и для каждого делителя числа $\lambda(45) = 12$ (и только для таких делителей) существует целое число, взаимно простое с M и имеющее своим периодом этот делитель.

Если НОД $(a, M) = 1$, $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, то

$$T(a, M) = \text{НОК}(T(a, p_1^{\alpha_1}), T(a, p_2^{\alpha_2}), \ldots, T(a, p_k^{\alpha_k})). \qquad (2.6)$$

Функция Кармайкла гарантирует существование первообразных элементов, а разыскать их можно, пользуясь следующей теоремой.

Теорема 2.12. Пусть $c = \varphi(M)$ и $g_1, \ldots, g_k$ различные простые делители числа c. Для того чтобы число g, взаимно простое с M, было первообразным элементом по модулю M, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений:

$$g^{c/g_1} \equiv 1 \pmod M, \ldots, g^{c/g_k} \equiv 1 \pmod M. \qquad (2.7)$$

Приведем важное для нас в дальнейшем следствие из этой теоремы. Если $M = 2^{2^l} + 1$ — простое число, то g является первообразным корнем только тогда, когда

$$g^{p-1} \equiv 1 \pmod p; \quad g^{\frac{p-1}{2}} \equiv -1 \pmod p.$$

Пример 2.13. Пусть $M = 31$. Имеем $\varphi(31) = 30 = 2 \cdot 3 \cdot 5$; $30/2 = 15$; $30/3 = 10$; $30/5 = 6$. Следовательно, для того чтобы число g было первообразным элементом по модулю 31, необходимо и достаточно, чтобы это g не удовлетворяло ни одному из сравнений

$$g^{15} \equiv 1 \pmod{31}; \quad g^{10} \equiv 1 \pmod{31}; \quad g^{6} \equiv 1 \pmod{31}.$$

Испытывая числа 2, 3, 4..., находим $2^{15} \equiv 1$; $2^{10} \equiv 1$; $2^6 \equiv 1$, $3^{15} \equiv -1$; $3^{10} \equiv 25$; $3^6 \equiv 21 \pmod{31}$, ... Отсюда видим, что 2 — не первообразный элемент, а 3 — первообразный.

При некоторых специальных видах модуля M задача отыскания первообразных корней из единицы значительно упрощается. Приведем ряд теорем.

Теорема 2.13. Первообразный корень простого числа вида $2^n + 1$ $n > 1$ есть 3.

Теорема 2.14. Первообразный корень простого числа вида $4p + 1$, где p — простое число, есть 2.

Имеют место три важных следствия теоремы 2.14.

Следствие 1. Первообразный корень простого числа вида $2p + 1$, где p вида $4n + 1$, есть 2, а при p вида $4n + 3$ есть -2.

Следствие 2. Простые нечетные делители числа $a^p \pm 1$, где p — простое нечетное число, делят $a \pm 1$ или имеют вид $2px + 1$.

Следствие 3. Простые делители числа $2^{2^n} + 1$ имеют вид $2^{n+1}x + 1$.

При отыскании первообразных корней по модулю простого числа необходимо пользоваться теоремой 2.14 и ее следствиями. Однако если $M = p^\alpha$, $2p^\alpha$ ($\alpha \geqslant 1$), то лучше воспользоваться следующими двумя теоремами.

Теорема 2.15 [47]. Пусть g — первообразный корень по модулю p. Можно указать t с условием, что u, определяемое равенством $(g + pt)^{p-1} = 1 + pu$, не делится на p. Соответствующее $g + pt$ будет первообразным корнем по модулю p^α при любом $\alpha > 1$.

Теорема 2.16 [47]. Пусть $\alpha \geqslant 1$ и g_1 — первообразный корень по модулю p^α. Нечетное из чисел g_1 и $g_1 + p^\alpha$ будет первообразным корнем по модулю $2p^\alpha$.

Пример 2.14. Пусть $M = 1681 = 41^2$. Первообразный корень по модулю 41 есть 6. Находим $6^{40} = 1 + 41(3 + 41e)$, $(60 + 41t)^{40} = 1 + 41(3 + 41e - 6^{39}t + 41T) = 1 + 41u$. Чтобы u не делилось на 41, достаточно взять $t = 0$. Поэтому в качестве первообразного корня по модулю 1681 можно взять число $6 + 41 \cdot 0 = 6$.

Пример 2.15. Пусть $M = 3362 = 2 \cdot 1681$. Тогда в качестве g нужно взять нечетное из чисел 6 и $6 + 1681$, т. е. число 1687.

При изучении колец Z_M интерес представляет алгебраическая структура мультипликативной группы этого кольца $M(Z_M)$. Произвольную мультипликативную группу обозначим через M_M, ее порядок равен числу M.

Теорема 2.17. Пусть k — целое положительное число. Тогда справедливо следующее:

1) если p — простое число, большее 2, то $M(Z_{p^k})$ — циклическая группа;

2) группы $M(Z_2)$ и $M(Z_4)$ — циклические порядков 1 и 2 соответственно, в то время как $M(Z_{2^k})$ $(k \geqslant 3)$ — прямое произведение циклической группы порядка 2^{k-2} и циклической группы порядка 2, т. е.

$$M(Z_{2^k}) \sim M \times M_{2^{m-2}}.$$

Из этой теоремы в качестве следствия получаем утверждение, о котором говорилось выше: группа $M(Z_M)$ является циклической (или, что равносильно, первообразный корень по модулю M существует) тогда и только тогда, когда целое число $M > 1$ имеет вид 2; 4; p^n или $2p^n$, где p — нечетное простое число.

Для дальнейшего полезно знать структуру не только приведенной системы вычетов $M(Z_M)$, но и структуру самого кольца Z_M. Оказывается верна следующая теорема.

Теорема 2.18. Пусть Z_M — кольцо классов вычетов по модулю M, где $M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ (p_i — различные простые числа). Тогда Z_M изоморфно кольцу $Zp_1^{\alpha_1} + Z\,p_2^{\alpha_2} + \ldots + Zp_k^{\alpha_k}$. Элементы этого кольца — k-мерные векторы, сложение и умножение определены покомпонентно.

Доказательство. Пусть отображение $f : Z_M \mapsto Zp_1^{\alpha_1} + Zp_2^{\alpha_2} + \ldots + Zp_k^{\alpha_k}$ определено следующим образом:

$$f(a) = [a \pmod{p_1^{\alpha_1}},\ a \pmod{p_2^{\alpha_2}},\ \ldots,\ a \pmod{p_k^{\alpha_k}}].$$

По мере того как a пробегает последовательность значений 0, 1, ..., $M - 1$, компонент $a \pmod{p_i^{r_i}}$ периодически принимает значения 0, 1, ..., $p_i^{r_i} - 1$, т. е. компонент $a \pmod{p_i^{r_i}}$ периодичен с периодом $p_i^{r_i}$. Так как $p_i^{r_i}$ — степени различных простых чисел, то вектор $[a \pmod{p_1^{\alpha_1}},\ a \pmod{p_2^{\alpha_2}},\ \ldots,\ a \pmod{p_k^{\alpha_k}}]$ не может повторяться дважды. Следовательно, f есть взаимооднозначное соответствие (биекция [109]). Теперь для всех $a \in Z_M$ и $b \in Z_M$

$$f(a+b) = [(a+b) \bmod p_1^{\alpha_1},\ \ldots,\ (a+b) \bmod p_k^{\alpha_k}] =$$

$$= [a \pmod{p_1^{\alpha_1}},\ \ldots,\ a \pmod{p_k^{\alpha_k}}] + [b \pmod{p_1^{\alpha_1}},\ \ldots,\ b \pmod{p_k^{\alpha_k}}] =$$

$$= f(a) + f(b).$$

Аналогично имеем $f(ab) = f(a)\,f(b)$. Таким образом, кольцо Z_M изоморфно кольцу $Zp_1^{\alpha_1} + \ldots + Zp_k^{\alpha_k}$.

В целом для математики характерен способ изучения с точностью до изоморфизма. Поэтому кольца Z_M и $Zp_1^{\alpha_1} + \ldots + Zp_k^{\alpha_k}$ представляют с точки зрения «чистой» математики один и тот же объект. Однако с точки зрения специалиста по «прикладной» математике и кибернетике — это совершенно разные объекты. Например, использование Z_M-арифметики и $Zp_1^{\alpha_1} + \ldots + Zp_k^{\alpha_k}$-арифметики при расчетах на ЦВМ приводит к совершенно различным программным и временным затратам. Далее, если мы попытаемся построить специали-

зированные устройства, работающие в этих арифметиках, то они будут обладать различной структурой, быстродействием и аппаратурными затратами.

В арифметике кольца Z_M важную роль играют еще две функции, одна из которых называется символом Лежандра, а вторая — символом Якоби. Первая определяется следующим образом. Пусть

$$x^2 \equiv a \pmod{p} \tag{2.8}$$

— квадратичное уравнение в кольце Z_p, где p — простое число. Если сравнение (2.8) является решением элемента a, то a называется квадратичным вычетом, в противном случае — квадратичным невычетом по модулю p.

Если a — квадратичный вычет по модулю p, то сравнение (2.8) имеет два решения. Пусть $x = \alpha_1 \pmod{p}$ — одно решение. Тогда вторым будет $x = -\alpha_1$, так как $\alpha_1^2 = (-\alpha_1)^2$. Это второе решение отличается от первого.

Теорема 2.19. Приведенная система вычетов по модулю p имеет $(p-1)/2$ квадратичных вычетов, сравнимых с числами

$$1^2,\ 2^2,\ \ldots,\ (p-1)^2/4 \tag{2.9}$$

и $(p-1)/2$ квадратичных невычетов.

Определение 2.11. Функция (a/p) (читается: символ a по p), задаваемая равенством $(a/p) = 1$, если a — квадратичный вычет по модулю p, и равенством $(a/p) = -1$, если a — квадратичный невычет по модулю p, называется символом Лежандра.

Теорема 2.20. При a, не делящемся на p, имеем

$$(a/p) = a^{\left(\frac{p-1}{2}\right)} \pmod{p}. \tag{2.10}$$

Доказательство. Действительно, по теореме Ферма (см. теорему 2.11)

$$a^{p-1} \equiv 1 \pmod{p};\quad (a^{\frac{p-1}{2}} - 1)(a^{\frac{p-1}{2}} + 1) \equiv 0 \pmod{p}.$$

Один и только один из сомножителей левой части последнего сравнения делится на p (оба сомножителя не могут одновременно делиться на p, в противном случае их разность 2 должна была бы делиться на p). Поэтому имеет место только одно из сравнений

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p};\quad a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \tag{2.11}$$

Но всякий квадратичный вычет a удовлетворяет при некотором x сравнению $a \equiv x^2 \pmod{p}$ и, следовательно, также получаемому из него почленным возведением в степень $(p-1)/2$ сравнению (2.11). При этом квадратичными вычетами и исчерпываются все решения сравнения (2.11), так как, будучи сравнением степени $(p-1)/2$, оно не может иметь более $(p-1)/2$ решений. Поэтому квадратичные невычеты удовлетворяют сравнению (2.11).

Пример 2.16. Имеем $2^{15} \equiv 1 \pmod{31}$. Поэтому $(2/31) = 1$ и 2 —

квадратичный вычет по модулю 31. Имеем $3^{15} \equiv -1 \pmod{31}$. Поэтому $(3/31) = -1$ и 3 — квадратичный невычет по модулю 31.

Заметим, что уравнение $x^2 = -1$ не имеет решений в поле действительных чисел, а в поле комплексных чисел его решением является мнимая единица. В конечных полях GF (p) уравнение $x^2 = -1$ может как иметь, так и не иметь решения. Все зависит от вида p. Любое натуральное число M может быть записано в одной из форм: $4n$; $4n + 1$; $4n + 2$; $4n + 3$, но первая и третья формы выражают только составные числа, а на долю всех простых и части составных остается вторая и четвертая. Так как $(p - 1)/2$ четное число, если p вида $4n + 1$, и нечетное, если p вида $4n + 3$, то отсюда следует, что -1 является квадратичным вычетом по модулю p, если p вида $4n + 1$, и квадратичным невычетом по модулю p, если p число вида $4n + 3$.

Теорема 2.21. Символ Лежандра обладает следующими свойствами:

1) $[(ab \ldots c)/p] = (a/p)(b/p) \ldots (c/p)$;

2) $(q/p) = (-1)^{\frac{p-1}{2} \cdot \frac{g-1}{2}} (p/g)$, если p, g — простые нечетные;

3) $(2/p) = (-1)^{\frac{p^2-1}{8}}$;

4) если $a \equiv a_1 \pmod{p}$, то $(a/p) = (a_1/p)$.

Полезным обобщением символа Лежандра является символ Якоби. Пусть M — нечетное, большее единицы, и $M = p_1 p_2 \ldots p_r$. Пусть далее НОД $(a, p) = 1$. Тогда символ Якоби определяется равенством

$$(a/M) = (a/p_1)(a/p_2) \ldots (a/p_2).$$

Исходя из свойств символа Лежандра, можно установить свойства и для символа Якоби.

7. Поля Галуа

Известно, что полная система вычетов по модулю простого числа p образует конечное поле порядка p, которое обозначают через GF (p) и называют простым полем Галуа. Сложение и умножение элементов поля осуществляются в виде арифметических операций по модулю p над числами $\{0, 1, 2, \ldots, p - 1\}$ или $\{-(p - 1)/2, \ldots, -1, 0, 1, \ldots, (p - 1)/2\}$.

Пример 2.17. Элементами поля GF (5) являются числа 0, 1, 2, 3, 4. Эти элементы по отношению к операции сложения по модулю 5, задаваемой табл. 2 при $M = 5$, образуют абелеву группу — аддитивную группу поля GF (5). Элементы 1, 2, 3, 4 по отношению к операции умножения по модулю 5, задаваемой табл. 6, образуют также абелеву группу — мультипликативную группу поля GF (5).

Способ построения простых полей Галуа GF (p) наводит на мысль, что, используя в $F[x]$ неприводимые полиномы (аналоги простых чисел в кольце Z), можно, вероятно, построить новые поля.

Пусть $f(x)$ — полином, принадлежащий $F[x]$ и отличающийся от нулевого. Будем говорить, что два полинома $a(x)$ и $b(x)$ сравнимы по модулю полинома $f(x)$, если оба полинома при делении на $f(x)$ дают один и тот же остаток, или полиномы $a(x)$ и $b(x)$ сравнимы по модулю $f(x)$ тогда и только тогда, когда их разность делится на $f(x)$. Это, в свою очередь, равносильно тому, что существует такой ненулевой полином $f(x)$, для которого

$$a(x) = b(x) + t(x)\, m(x).$$

Заметим, что остатки от деления любого ненулевого полинома в $F[x]$ на полином $f(x)$ также являются полиномами, степень которых меньше степени полинома $f(x)$.

Пример 2.18. Пусть

$$F[x] = R[x]; \quad f(x) = x^3 + 1;$$
$$a(x) = x^5 + x^3 + 2x^2 + x + 2;$$
$$b(x) = 0{,}1x^5 + 3x^4 + x^3 + 1{,}1x^2 + 4x + 1.$$

Тогда

$$a(x) = (x^2 + 1) f(x) + x^2 + x + 1;$$
$$b(x) = (0{,}1x^2 + 3x + 1) f(x) + x^2 + x + 1.$$

Значит,

$$a(x) \equiv b(x) = x^2 + x + 1 \pmod{(x^3 + 1)}.$$

Если $f(x) = p(x)$ — неприводимый полином, то остатки от деления ненулевых полиномов в $F(x)$ на полином $p(x)$ образуют поле относительно операции покоэффициентного сложения и операции умножения по модулю $p(x)$. Это поле обозначим через $F[x]/p(x) \times F[x]$. Аналогичная ситуация была в случае полей GF(p). Остатки от деления целых чисел на число p были числами $0, 1, \ldots, p-1$, которые и образовывали поле GF(p) относительно операций сложения и умножения по модулю p.

Пример 2.19. Пусть $F[x] = R[x]$, т. е. рассматриваем кольцо полиномов с вещественными коэффициентами. Возьмем неприводимый полином $p(x) = x^2 + 1$. Легко видеть, что этот полином не разлагается на полиномы первой степени с вещественными коэффициентами. Остатками от деления полиномов в $R[x]$ будут полиномы первой степени $cx + d$. Поскольку $x^2 + 1$ — неприводимый полином, то множество полиномов $cx + d$ должно образовывать поле. Если $f_1(x) = ax + b$ и $f_2(x) = cx + d$ — два полинома, принадлежащих этому полю, то их суммой будет полином $\varphi(x) = f_1(x) + f_2(x) = (a + c)x + (b + d)$. Произведением этих полиномов следует считать остаток от деления $(ax + b)(cx + d)$ на $p(x)$. Найдем этот остаток:

$$\begin{array}{l} (ax+b)(cx+d) = acx^2 + (bc+ad)x + bd \quad \big| \, x^2 - 1 \\ \qquad\qquad\qquad\qquad\qquad\quad +ac \qquad\quad ac \\ \hline \qquad\qquad\qquad\qquad\qquad\quad (bc+ad)x + bd - ac. \end{array}$$

Таким образом,

$$(ax + b)(cx + d) = [(bc + ad)x + (bd - ac)] \mod (x^2 + 1).$$

Теперь рассмотрим сумму и произведение двух комплексных чисел $ai + b$ и $ci + d$:

$$(ai + b)(ci + d) = (bc + ad)i + (bd - ac);$$
$$(ai + b) + (ci + d) = (a + c)i + (b + d).$$

Нетрудно видеть, что поскольку законы сложения и умножения в поле $R[x]/(x^2 + 1) \times R[x]$ полностью совпадают с соответствующими законами в поле комплексных чисел C, эти два поля изоморфны:

$$R[x]/(x^2 + 1)\, R[x] \sim C.$$

Так как коэффициентами полиномов в примере 2.18 служили действительные числа, то говорят, что поле комплексных чисел получается при расширении поля вещественных чисел присоединением к нему корня уравнения $x^2 + 1 = 0 : x = \sqrt{-1} = i$. Поскольку неприводимых полиномов более высоких степеней, чем 2, в кольце $R[x]$ не существует, единственным расширением поля вещественных чисел является поле комплексных чисел.

Иначе обстоят дела в кольце GF $(p)[x]$, т. е. в кольце полиномов, коэффициентами которого являются элементы поля Галуа GF (p). При оперировании с полиномами из этого кольца нужно всегда помнить, что коэффициенты полиномов должны складываться и перемножаться по законам поля GF (p). Пусть, например, $f_1(x) = 4x^2 + 3$; $f_2 = 3x^2 + 2$, $f_1(x)$, $f_2(x) \in$ GF $(5)[x]$. Тогда

$$f_1(x) + f_2(x) = (4x^2 + 3) + (3x^2 + 2) = (4 + 3)x^2 + 3 + 2 = 2x^2;$$
$$f_1(x) f_2(x) = (4x^2 + 3)(3x^2 + 2) = 12x^4 + 9x^2 + 8x^2 + 6 =$$
$$= 2x^4 + 4x^2 + 3x + 1 = 2x^4 + 2x^2 + 1.$$

В современной алгебре доказывается, что в кольце GF $(p)[x]$ существуют неприводимые полиномы любой степени [52]. Это означает, что можно получать любые расширения поля GF (p), которые называются гиперкомплексными полями.

Если неприводимый полином $p(x)$ имеет степень $\deg(p(x)) = n$, то поле, получающееся в результате расширения, обозначается через GF (p^n). Число элементов в таком поле равно p^n и называется составным полем Галуа.

Пример 2.20. Пусть $F(x) =$ GF $(2)[x]$. Неприводимым полиномом второй степени является $p(x) = x^2 + x + 1$. Построим поле GF (2^2), состоящее из полиномов первой степени $ax + b$; a и $b \in$ GF (2). Определим закон умножения в этом поле:

$$\begin{array}{l} (ax+b)(cx+d) = acx^2 + (bc+ad)x + bd \quad \big| \underline{x^2+x+1} \\ \underline{acx^2 + \quad acx + ac} \\ (bc + ad + ac)x + bd + ac. \end{array}$$

Таблица 13. Сложение в поле GF (2^2)

$\oplus$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

Таблица 14. Умножение в поле GF (2^2)

$\odot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Таким образом,

$$(ax+b)(cx+d) = [(bc+ad+ac)x + (bd+ax)] \mod (x^2+x+1). \tag{2.12}$$

Подставляя в выражение (2.12) вместо a и b значения $0, 1 \in$ GF (2), получаем четыре полинома 0; 1; x; $x+1$. Учитывая формулу (2.12) и помня, что коэффициенты a и b умножаются и складываются по модулю $p = 2$, получаем таблицы умножения и сложения поля GF (2^2) (табл. 13, 14).

Очень часто элементы поля GF (p^n) записывают не в виде полинома, а в виде n-мерного вектора

$$z = \begin{pmatrix} a_{n-1} \\ a_{n-2} \\ \vdots \\ a_0 \end{pmatrix} \Rightarrow z = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_0,$$

составленного из коэффициентов полинома. В примере 2.19 это будет выглядеть следующим образом. Все элементы поля GF (2^2), выражаемые через полиномы $ax + b$, запишутся в виде $\begin{pmatrix} a \\ b \end{pmatrix}$. Таким образом,

$$\text{GF}(2^2) = \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\}.$$

Заметим, что носителем поля GF (2^2) является двухмерное векторное пространство GF (2) $\times$ GF (2). Для этого поля законы сложения и умножения задаются равенствами

$$z_1 + z_2 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 \oplus a_2 \\ b_1 \oplus b_2 \end{pmatrix}; \tag{2.13}$$

$$z_1 z_2 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 \oplus b_1 b_2 \\ a_1 a_2 \oplus a_1 b_2 \oplus b_1 a_2 \end{pmatrix}. \tag{2.13а}$$

В такой записи для поля комплексных чисел имеем

$$z_1 + z_2 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 + a_2 \\ b_1 + b_2 \end{pmatrix}; \tag{2.14}$$

$$z_1 z_2 = \begin{pmatrix} a_1 \\ b_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 - b_1 b_2 \\ a_1 b_2 + b_1 a_2 \end{pmatrix}. \tag{2.14а}$$

Пример 2.21. Построим гиперкомплексное поле GF (2^3). Для этого возьмем декартову степень GF (2) × GF (2) × GF (2). Элементами этого поля будут трехмерные векторы

$$\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}.$$

Закон сложения зададим покоординатно:

$$z_1 + z_2 = \begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} + \begin{pmatrix} a_2 \\ b_2 \\ c_2 \end{pmatrix} = \begin{pmatrix} a_1 \oplus a_2 \\ b_1 \oplus b_2 \\ c_1 \oplus c_2 \end{pmatrix}, \quad a_1, a_2, b_1, b_2, c_1, c_2 \in \mathrm{GF}(2).$$

Чтобы задать умножение, поставим в соответствие каждому элементу полином второй степени $z = a + bx + cx^2$ и найдем неприводимый полином третьей степени во множестве всех полиномов с коэффициентами из поля GF (2). Таким полиномом является полином $p(x) = x^3 + x + 1$ [72]. Тогда для закона умножения будем иметь:

$$z_1 z_2 = (a_1 + b_1 x + c_1 x^2)(a_2 + b_2 x + c_2 x^2) =$$

$$= c_1 c_2 x^4 + (b_1 c_2 + c_1 b_2) x^3 + (a_2 c_1 + b_1 b_2 + a_1 c_2) x^2 + (b_1 a_2 + a_1 b_2) x + a_1 a_2 \quad \Big| \; x^3 + x + 1$$

$$\oplus \quad c_1 c_2 x^4 \qquad + c_1 c_2 x^2 \qquad + c_1 c_2 x \qquad \Big| \; c_1 c_2 x + (b_2 c_2 + c_1 b_2)$$

$$(b_1 c_2 + c_1 b_2) x^3 + (a_2 c_1 + b_1 b_2 + c_1 c_2 + a_1 c_2) x^2 + (b_1 a_2 + a_1 b_2 + c_1 c_2) x + a_1 a_2$$

$$\oplus \quad (b_1 c_2 + c_1 b_2) x^3 + \qquad\qquad (b_1 c_2 + c_1 b_2) x + (b_1 c_2 + c_1 b_2)$$

$$(a_2 c_1 + b_1 b_2 + a_1 c_2 + c_1 c_2) x^2 + (b_1 a_2 + a_1 b_2 + b_1 c_1 + c_1 b_2 + c_1 c_2) x + (a_1 a_2 + b_1 b_2 + c_1 b_2),$$

или

$$z_1 z_2 = \begin{pmatrix} a_1 \\ b_1 \\ c_1 \end{pmatrix} \begin{pmatrix} a_2 \\ b_2 \\ c_2 \end{pmatrix} = \begin{pmatrix} a_1 a_2 \oplus c_1 b_2 \oplus b_1 c_2 \\ b_1 a_2 \oplus a_1 b_2 \oplus c_1 c_2 \oplus b_1 c_2 \oplus c_1 b_2 \\ c_1 a_2 \oplus b_1 b_2 \oplus a_1 c_2 \oplus c_1 c_2 \end{pmatrix}. \tag{2.15}$$

Если векторы $\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ обозначить соответственно i_2, i_1,

1, то возможна гиперкомплексная запись элементов GF (2^3):

$$z = \begin{pmatrix} a \\ b \\ c \end{pmatrix} = a + i_1 b + i_2 c.$$

Обычно элементы i_1, i_2 называют мнимостями Галуа. Используя последнюю форму представления элементов поля Галуа и пользуясь формулой (2.15), получаем таблицы умножения и сложения в поле GF (2^3) (табл. 15, 16).

Аналогичным образом получаются и все остальные поля GF (2^n). Возможно различное обозначение элементов z этих полей: полиномиальное $z = a_0 + a_1 x + \ldots + a_{n-1} x^{n-1}$, гиперкомплексное $z = a_0 + i_1 a_1 + \ldots + i_{n-1} a_{n-1}$, векторное $z = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix}$. В последнем случае носителем поля GF (2^n) является n-мерное пространство GF (2) $\times$ $\times$ GF (2) $\times \ldots \times$ GF (2). При этом мнимые единицы Галуа имеют простое векторное представление

$$i_{n-1} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}; \ldots; \quad i_1 = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}; \quad i_0 = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Для сравнения напомним, что носителем поля комплексных чисел C является двухмерное векторное пространство $R \times R$, а все элементы этого поля имеют вид $z = i_0 a + i_1 b = \begin{pmatrix} a \\ b \end{pmatrix}$. Причем $i_0 = 1 = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $i_1 = i = \sqrt{-1} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$.

Поле порядка p^{ns} можно получить не только расширением степени ns поля GF (p), но и также расширением степени s поля GF (p). Для этого нужно взять кольцо GF (p^n) [x] полиномов с коэффициентами из поля GF (p^n), в кольце выбрать неприводимый полином степени s и все остальные полиномы складывать и умножать по модулю выбранного полинома.

Пример 2.22. Построим таблицы сложения и умножения поля GF (3^2). Элементами этого поля являются полиномы 0; 1; 2; x; $x + 1$; $x + 2$; $2x$; $2x + 1$; $2x + 2$. Таблица сложения (табл. 17) получается непосредственно сложением соответствующих коэффициентов полинома по модулю 3. Например, $(x + 1) + (x + 2) = 2x$. Для составления таблицы умножения необходимо конкретизировать неприводимый полином $p(x)$. Пусть $p(x) = x^2 - 2$. Тогда таблица умножения будет иметь вид табл. 18.

Рассуждения, аналогичные проведенным для полей GF (p) и GF (p^n), свидетельствуют, что полная система вычетов по модулю $f_s(x)$, где $f_s(x)$ — неприводимый над полем GF (p^n) полином степени s, удовлетворяет всем законам поля. Поэтому полиномы степени,

Таблица 15. **Сложение в поле GF (2^3)**

$\oplus$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x^2	$x+1$	x	1	0

Таблица 16. **Умножение в поле GF (2^3)**

$\odot$	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
0	0	0	0	0	0	0	0	0
1	0	1	x	$x+1$	x^2	x^2+1	x^2+x	x^2+x+1
x	0	x	x^2	x^2+x	$x+1$	1	x^2+x+1	x^2+1
$x+1$	0	$x+1$	x^2+x	x^2+1	x^2+x+1	x^2	1	x
x^2	0	x^2	$x+1$	x^2+x+1	x^2+x	x	x^2+1	1
x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	$x+1$	x^2+x
x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	$x+1$	x	x^2
x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	$x+1$

Таблица 17. Сложение в поле GF (3^2)

$\odot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
1	1	2	0	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$
2	2	0	1	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$
x	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$	0	1	2
$x+1$	$x+1$	$x+2$	x	$2x+1$	$2x+2$	$2x$	1	2	0
$x+2$	$x+2$	x	$x+1$	$2x+2$	$2x$	$2x+1$	2	0	1
$2x$	$2x$	$2x+1$	$2x+2$	0	1	2	x	$x+1$	$x+2$
$2x+1$	$2x+1$	$2x+2$	$2x$	1	2	0	$x+1$	$x+2$	x
$2x+2$	$2x+2$	$2x$	$2x+1$	2	0	1	$x+2$	x	$x+1$

Таблица 18. Умножение в поле GF (3^2)

$\odot$	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
0	0	0	0	0	0	0	0	0	0
1	0	1	2	x	$x+1$	$x+2$	$2x$	$2x+1$	$2x+2$
2	0	2	1	$2x$	$2x+2$	$2x+1$	x	$x+2$	$x+1$
x	0	x	$2x$	2	$x+2$	$2x+2$	1	$x+1$	$2x+1$
$x+1$	0	$x+1$	$2x+2$	$x+2$	$2x$	1	$2x+1$	2	x
$x+2$	0	$x+2$	$2x+1$	$2x+2$	1	x	$x+1$	$2x$	2
$2x$	0	$2x$	x	1	$2x+1$	$x+1$	2	$2x+2$	$x+2$
$2x+1$	0	$2x+1$	$x+2$	$x+1$	2	$2x$	$2x+2$	x	1
$2x+2$	0	$2x+2$	$x+1$	$2x+1$	x	2	$x+2$	1	$2x$

не выше $s-1$

$$R(x) = a_{s-1}x^{s-1} + a_{s-2}x^{s-2} + \cdots + a_1x + a_0, \qquad (2.16)$$

где каждое из $a_0, a_1, \ldots, a_{s-1}$ может быть любым из p^n элементов поля GF (p^n), образуют конечное поле GF $((p^n)^s)$.

Из (2.16) следует, что существует точно p^{ns} различных полиномов $R(x)$. Поэтому поле GF $((p^n)^s)$ содержит p^{ns} элементов. Поле GF $((p^n)^s)$ называют расширением степени s поля GF (p^n).

Подчеркнем, что в отличие от расширенного поля GF (p^n), где элементами были полиномы с коэффициентами из GF (p), элементы расширенного поля GF $((p^n)^s)$ — суть полиномы с коэффициентами их поля GF (p^n).

Пример 2.23. Найдем элементы поля GF $((2^2)^2)$. Элементы поля GF (2^2) — это 0; 1; a; $a+1$ (см. пример 2.19). Поэтому

$$\mathrm{GF}((2^2)^2) = \{0, 1, a, a+1, x, x+1, x+a, x+a+1, ax, ax+1,$$
$$ax+a, ax+a+1, (1+a)x, (1+a)x+1, (1+a)x+a,$$
$$(a+1)x+a+1\}.$$

С учетом того что закон сложения полиномов покомпонентный, получаем табл. 19 для закона сложения в GF $((2^2)^2)$.

В качестве неприводимого над полем GF (2^2) полинома степени $s=2$ выберем, например, полином $f = x^2 + x + i$, где i — элемент поля GF (2^2).

Найдем закон умножения. Пусть $\alpha_1x + \beta_1, \alpha_2x + \beta_2 \in \mathrm{GF}((2^2)^2)$, $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathrm{GF}(2^2)$. Тогда

$$(\alpha_1x+\beta_1)(\alpha_2x+\beta_2) = \alpha_1\alpha_2x^2 + (\beta_1\alpha_2 + \beta_2\alpha_1)x + \beta_1\beta_2;$$

$$\begin{array}{l|l} \alpha_1\alpha_2x^2 + (\beta_1\alpha_2+\beta_2\alpha_1)x + \beta_1\beta_2 & x^2+x+i \\ \alpha_1\alpha_2x^2 + \quad \alpha_1\alpha_2x + \alpha_1\alpha_2 i & \alpha_1\alpha_2 \\ \hline (\beta_1\alpha_2 + \beta_2\alpha_1 + \alpha_1\alpha_2)x + (i\alpha_1\alpha_2 + \beta_1\beta_2). & \end{array}$$

Таким образом,

$$(\alpha_1x+\beta_1)(\alpha_2x+\beta_2) =$$
$$= (\beta_1\alpha_2 + \beta_2\alpha_1 + \alpha_1\alpha_2)x + (i\alpha_1\alpha_2 + \beta_1\beta_2) \bmod (x^2+x+i).$$

Пользуясь этой формулой, получаем табл. 20 для закона умножения.

Конечные поля GF (p^n) называются полями характеристики p, а все классические поля (поле рациональных чисел, поле действительных чисел, поле комплексных чисел) — полями нулевой характеристики.

Отметим, что в некоторых свойствах поля нулевой характеристики довольно существенно отличаются от полей простой характеристики.

Теорема 2.22. В поле GF (p^n) все элементы, кратные p, равны нулю.

Пусть $n=1$. Тогда в GF (p) $p \equiv 0 \pmod p$, значит, и все кратные $kp \equiv 0 \pmod p$.

Пусть $n \neq 1$. Тогда все кратные $f(x)\, p = (a_{n-1}p)\, x^{n-1} + (a_{n-2}p)\, x^{n-2} + \ldots + a_0 p$. Но каждый коэффициент $(a_i p) \in \mathrm{GF}(p)$, значит, $a_i p \equiv 0 \pmod{p}$. Поэтому $f(x)\, p \equiv 0 \pmod{p}$.

Теорема 2.23. Если F — поле характеристики p, то для произвольных элементов a и b из F справедлива формула

$$(a + b)^p = a^p + b^p. \tag{2.17}$$

Действительно, по формуле бинома Ньютона имеем

$$(a + b)^p = a^p + c_p^1 a^{p-1} b + \ldots + c_p^{p-1} a b^{p-1} + b^p.$$

Но биномиальные коэффициенты c_p^i $(0 < i < p)$ равны $p(p-1) \ldots (p-i+1)/i!$, т. е. кратны p, а значит, равны нулю по модулю p, откуда и получается (2.17).

Теорема 2.24. В поле $\mathrm{GF}(p^n)$ для любого ненулевого элемента имеет место равенство $x^{p^n-1} = 1$.

Из теоремы 2.24 следует, что все элементы поля $\mathrm{GF}(p^n)$ имеют периоды T, являющиеся делителями $p^n - 1$, т. е. $T \mid p^n - 1$. Элемент v, имеющий максимально возможный период (это возможно в силу того, что полином $p(x)$ неприводимый и поэтому мультипликативная группа $\mathrm{MGF}(p^n)$ является циклической), называется первообразным примитивным элементом поля $\mathrm{GF}(p^n)$. Таким образом, все степени $v^0, v^1, \ldots, v^{p^n-1}$ различны и пробегают все ненулевые элементы поля $\mathrm{GF}(p^n)$, т. е.

$$\mathrm{GF}(p^n) = \{0, v, v^1, \ldots, v^{p^n-1}; \oplus, \odot\}.$$

Если v — первообразный примитивный элемент поля $\mathrm{GF}(p^n)$, то все степени v^k (где НОД $(k, p^n - 1)$) также являются первообразными примитивными элементами этого поля. Таких чисел k имеется $\varphi(p^n - 1)$. Следовательно, в поле $\mathrm{GF}(p^n)$ имеется $\varphi(p^n - 1)$ первообразных примитивных элементов.

Осталось выяснить структуру кольца $F[x]/f(x)$, где $f(x)$ — произвольный (не обязательно неприводимый) полином кольца $F[x]$. Теорема 2.18 утверждает, что кольцо Z_M изоморфно кольцу $Z_{p_1}^{\alpha_1} + Z_{p_2}^{\alpha_2} + \ldots + Z_{p_n}^{\alpha_n}$, где $M = p_1^{\alpha_1} p_1^{\alpha_2} \ldots p_n^{\alpha_n}$ — каноническое разложение числа M. Оказывается, что и в рассматриваемом случае имеет место аналогичная теорема.

Теорема 2.25. Если $f(x) = p_1^{\alpha_1}(x)\, p_2^{\alpha_2}(x) \ldots p_n^{\alpha_n}(x)$ — каноническое разложение полинома $f(x)$ на произведение степеней неприводимых полиномов, то

$$F[x]/m(x) \sim F[x]/p_1^{\alpha_1}(x) + F[x]/p_2^{\alpha_2}(x) + \cdots + F[x]/p_n^{\alpha_n}(x).$$

В заключение заметим, что в ЦОС широко распространены ТЧП со структурами быстрых алгоритмов. Эти преобразования используются при построении математических моделей систем ЦОС. С точки зрения практического применения, а также аппаратурной реализации представляет интерес изучение полного множества возможных ТЧП. С этой целью ниже рассматривается еще несколько видов конечных алгебраических систем, а именно: поля алгебраических чисел, конечное поле комплексных чисел, конечное кольцо кватернионов, не-

ассоциативное конечное кольцо чисел Кэли. Последние три системы являются аналогами известных гиперкомплексных систем, определенных над полем действительных чисел. Используя эти системы, можно строить математические модели процессов цифровой обработки многомерных сигналов.

8. Поля алгебраических чисел

Пусть α — алгебраическое число над полем рациональных чисел Q или над полем GF (p), т. е. число, которое является корнем многочлена с рациональными коэффициентами

$$g(x) = b_0x^n + b_1x^{n-1} + \cdots + b_n = 0 \qquad (2.18)$$

(коэффициенты могут быть и из поля GF (p); в дальнейшем всегда будем иметь в виду такую возможность). Используя алгебраическое число α, можно построить множество чисел вида

$$\omega = a_0 + \alpha a_1 + \alpha^2 a_2 + \cdots + \alpha^{n-1} a_{n-1}.$$

Относительно обычных операций сложения и умножения, определенных для многочленов, с учетом того что

$$\alpha_n = \frac{b_1}{b_0}\alpha^{n-1} + \frac{b_2}{b_1}\alpha^{n-2} + \cdots + \frac{b_n}{b_0},$$

множество таких чисел образует поле $Q(\alpha)$ алгебраических чисел степени n, изоморфное полю $Q[x]/p(x)\,Q[x]$. Процесс построения поля $Q(\alpha)$ называется расширением поля рациональных чисел Q с помощью алгебраического числа α.

Пример 2.24. Пусть α — корень квадратного уравнения $x^2 + 1 = 0$ ($\alpha = i = \sqrt{-1}$). Множество всех чисел

$$Q(\alpha) = \{a_0 + a_1\alpha \mid a_0,\ a_1 \in Q\}$$

образует поле комплексных рациональных чисел.

Пример 2.25. Пусть $\alpha = \sqrt[3]{2}\, e^{i\frac{2\pi}{3}}$. Это число алгебраическое, оно является корнем уравнения $x^3 - 2 = 0$. Рассмотрим все числа вида

$$\omega = a_0 + a_1\sqrt[3]{2}\, e^{i\frac{2\pi}{3}} + a_2\left(\sqrt[3]{2}\, e^{i\frac{2\pi}{3}}\right)^2 = a_0 + a_1\alpha + a_2\alpha^2.$$

Множество таких чисел образует поле $Q(\sqrt[3]{2})$.

Если $\alpha = \alpha^{(1)}, \alpha^{(2)}, \ldots, \alpha^{(n)}$ — корни многочлена $g(x)$ (очевидно, что это комплексные числа), то можно построить поля $Q(\alpha^{(1)})$, $Q(\alpha^{(2)})$, ..., $Q(\alpha^{(n)})$. Все эти поля изоморфны друг другу и полю $Q[x]/p(x)\,Q[x]$ и называются проекциями поля $Q[x]/p(x)\,Q[x]$ при отображении $g(x) \mapsto g(\alpha^{(i)})$. Проекции не нужно отождествлять друг с другом и, конечно, с полем $Q[x]/p(x)\,Q[x]$. Действительно, носителями полей $Q(\alpha^{(1)})$, $Q(\alpha^{(2)})$, ..., $Q(\alpha^{(n)})$ будут различные множества комплексных чисел, в то время как носителем поля $Q[x]/p(x)\,Q[x]$ являются полиномы. Законы сложения и умножения полей $Q[x]/p(x)\,Q[x]$ и $Q(\alpha^{(1)})$, $Q(\alpha^{(2)})$, ..., $Q(\alpha^{(n)})$ совершенно одинаковы.

Поле $Q[x]/p(x)\,Q[x]$ удобно при теоретических исследованиях, а поля $Q(\alpha^{(1)})$, $Q(\alpha^{(2)})$, ..., $Q(\alpha^{(n)})$ — при конкретных вычислениях на ЦВМ.

Целые числа поля рациональных чисел Q образуют кольцо Z. Определим среди чисел данного поля F целые элементы таким образом, чтобы они образовывали кольцо (обозначим его ENT (F) или I), содержащее единицу. Кроме того, потребуем, чтобы поле F было полем отношений кольца ENT (F), т. е. чтобы каждое число из F могло быть представлено в виде дроби a/b, $a, b \in \mathrm{ENT}(F) = I$, причем $b \neq 0$. Предположим, что это каким-то образом установлено (например, для поля Q таким кольцом является кольцо Z) и известно, какие именно числа из F будут целыми. Переходя к конечному расширению $F(\alpha)$ поля F, необходимо распространить определение целых на элементы $F(\alpha)$ так, чтобы целые из F оставались таковыми и в $F(\alpha)$. Для такой проблемы перенесения в теории чисел существует универсальное решение [22, 178].

Определение 2.12. Числа ω из $F(\alpha)$ называются целыми в $F(\alpha)$, если они удовлетворяют уравнению

$$g_1(\omega) = \omega^m + a_1\omega^{m-1} + \cdots + \omega_m = 0,$$

коэффициенты которого $a_1, \ldots, a_m$ являются целыми в F.

Ясно, что целые числа «маленького» поля F остаются целыми в $F(\alpha)$ и в этом новом смысле, т. е. будут целыми и в «большом» поле $F(\alpha)$. Исходя из данного определения, можно доказать, что целые числа поля образуют кольцо.

Теорема 2.26. В любом поле $Q(\alpha)$ существуют такие целые числа $\omega_1, \omega_2, \ldots, \omega_n$, что любое целое число $\beta \in \mathrm{ENT}(Q(\alpha))$ единственным образом представимо в виде

$$a_1\omega_1 + \cdots + a_n\omega_n,$$

где $a_1a_2, \ldots, a_n \in Z$, $\omega_1, \omega_2, \ldots, \omega_n \in \mathrm{ENT}(Q(\alpha)) = I$.

Принято говорить, что $\omega_1, \omega_2, \ldots \omega_n$ составляют фундаментальный базис поля $Q(\alpha)$. После этой теоремы естественно возникает вопрос: не будет ли фундаментальным базис $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$? Ведь любое число из поля $Q(\alpha)$ представимо в виде линейной комбинации этих чисел. Или, другими словами, если построить все числа вида

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}, \tag{2.19}$$

где $a_i \in Z$ $(i = 1, 2, \ldots, n)$, то образуют ли они все множество I? Отметим прежде всего, что числа вида (2.19) являются расширением кольца целых чисел Z с помощью алгебраического числа α. Поэтому множество таких чисел естественно обозначить $Z(\alpha)$. Оказывается, что в некоторых случаях $Z(\alpha)$ совпадает, а в некоторых случаях не совпадает со всеми целыми поля $Q(\alpha)$. Например, целые алгебраические числа поля $Q(\sqrt{-2})$ — это все числа вида $a + b\sqrt{-2}$, где a, b — целые рациональные; целые числа поля $Q(\sqrt{-3})$ — это не только числа вида $a + b\sqrt{-3}$, где $a, b \in Z$, но еще числа вида

Таблица 19. Сложение в поле GF $((2^2)^2)$

$\oplus$	0	1	a	$a+1$	x	$x+1$	$x+a$	$x+(a+1)$
0	0	1	a	$a+1$	x	$x+1$	$x+a$	$x+(a+1)$
1	1	0	$a+1$	a	$x+1$	x	$x+(a+1)$	$x+a$
a	a	$a+1$	0	1	$x+a$	$x+(a+1)$	x	$x+1$
$a+1$	$a+1$	a	1	0	$x+(a+1)$	$x+a$	$x+1$	x
x	x	$x+1$	$x+a$	$x+(a+1)$	0	1	a	$a+1$
$x+1$	$x+1$	x	$x+(a+1)$	$x+a$	1	0	$a+1$	a
$x+a$	$x+a$	$x+(a+1)$	x	$x+1$	a	$a+1$	0	1
$x+(a+1)$	$x+(a+1)$	$x+a$	$x+1$	x	$a+1$	a	1	0
ax	ax	$ax+1$	$ax+a$	$ax+(a+1)$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+(a+1)$
$ax+1$	$ax+1$	ax	$ax+(a+1)$	$ax+a$	$(a+1)x+1$	$(a+1)x$	$(a+1)x+(a+1)$	$(a+1)x+a$
$ax+a$	$ax+a$	$ax+(a+1)$	ax	$ax+1$	$(a+1)x+a$	$(a+1)x+(a+1)$	$(a+1)x$	$(a+1)x+1$
$ax+(a+1)$	$ax+(a+1)$	$ax+a$	$ax+1$	ax	$(a+1)x+(a+1)$	$(a+1)x+a$	$(a+1)x+1$	$(a+1)x$
$(a+1)x$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+(a+1)$	ax	$ax+1$	$ax+a$	$ax+(a+1)$
$(a+1)x+1$	$(a+1)x+1$	$(a+1)x$	$(a+1)x+(a+1)$	$(a+1)x+a$	$ax+1$	ax	$ax+(a+1)$	$ax+a$
$(a+1)x+a$	$(a+1)x+a$	$(a+1)x+(a+1)$	$(a+1)x$	$(a+1)x+1$	$ax+a$	$ax+(a+1)$	ax	$ax+1$
$(a+1)x+(a+1)$	$(a+1)x+(a+1)$	$(a+1)x+a$	$(a+1)x+1$	$(a+1)x$	$ax+(a+1)$	$ax+a$	$ax+1$	ax

ax	$ax+1$	$ax+a$	$ax+(a+1)$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+(a+1)$
ax	$ax+1$	$ax+a$	$ax+(a+1)$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+(a+1)$
$ax+1$	ax	$ax+(a+1)$	$ax+a$	$(a+1)x+1$	$(a+1)x$	$(a+1)x+(a+1)$	$(a+1)x+a$
$ax+a$	$ax+(a+1)$	ax	$ax+1$	$(a+1)x+a$	$(a+1)x+a+1$	$(a+1)x$	$(a+1)x+1$
$ax+(a+1)$	$ax+a$	$ax+1$	ax	$(a+1)x+(a+1)$	$(a+1)x+a$	$(a+1)x+1$	$(a+1)x$
$ax+a$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+(a+1)$	ax	$ax+1$	$ax+a$	$ax+(a+1)$
$(a+1)x+1$	$(a+1)x$	$(a+1)x+(a+1)$	$(a+1)x+a$	$ax+1$	ax	$ax+(a+1)$	$ax+a$
$(a+1)x+a$	$(a+1)x+(a+1)$	$(a+1)x$	$(a+1)x+1$	$ax+a$	$ax+(a+1)$	ax	$ax+1$
$(a+1)x+(a+1)$	$(a+1)x+a$	$(a+1)x+1$	$(a+1)x$	$ax+(a+1)$	$ax+a$	$ax+1$	ax
0	1	a	$a+1$	ax	$ax+1$	$ax+a$	$ax+(a+1)$
1	0	$a+1$	a	$ax+1$	ax	$ax+(a+1)$	$ax+a$
a	$a+1$	0	1	$ax+a$	$ax+(a+1)$	ax	$ax+1$
$a+1$	a	1	0	$ax+(a+1)$	$ax+a$	$ax+1$	ax
x	$x+1$	$x+a$	$x+(a+1)$	0	1	a	$a+1$
$x+1$	x	$x+(a+1)$	$x+a$	1	0	$a+1$	a
$x+a$	$x+(a+1)$	x	$x+1$	a	$a+1$	0	1
$x+(a+1)$	$a+x$	$x+1$	x	$a+1$	a	1	0

Таблица 20. Умножение в поле GF $((2^2)^2)$

$\odot$	0	1	a	$a+1$	x	$x+1$	$x+a$
0	0	0	0	0	0	0	0
1	0	1	a	$a+1$	x	$x+1$	$x+a$
a	0	a	$a+1$	1	ax	$ax+a$	$ax+(a+1)$
$a+1$	0	$a+1$	1	a	$(a+1)x$	$(a+1)x+$ $+(a+1)$	$(a+1)x+1$
x	0	x	ax	$(a+1)x$	$x+a$	a	$(a+1)x+a$
$x+1$	0	$x+1$	$ax+a$	$(a+1)x+$ $+(a+1)$	a	$x+(a+1)$	ax
$x+a$	0	$x+a$	$ax+(a+1)$	$(a+1)x+1$	$(a+1)x+a$	ax	$x+1$
$x+(a+1)$	0	$x+(a+1)$	$ax+1$	$(a+1)x+a$	$ax+a$	$(a+1)x+a$	$a+1$
ax	0	ax	$(a+1)x$	x	$ax+(a+1)$	$a+1$	$x+(a+1)$
$ax+1$	0	$ax+1$	$(a+1)x+a$	$x+(a+1)$	$(a+1)x+$ $+(a+1)$	$x+a$	1
$ax+a$	0	$ax+a$	$(a+1)x+$ $+(a+1)$	$x+1$	$a+1$	$ax+1$	$(a+1)x$
$ax+(a+1)$	0	$ax+(a+1)$	$(a+1)x+1$	$x+a$	$x+(a+1)$	$(a+1)x$	$ax+a$
$(a+1)x$	0	$(a+1)x$	x	ax	$(a+1)x+1$	1	$ax+1$
$(a+1)x+1$	0	$(a+1)x+1$	$x+a$	$ax+(a+1)$	$ax+1$	x	$(a+1)x+$ $+(a+1)$
$(a+1)x+a$	0	$(a+1)x+a$	$x+(a+1)$	$ax+1$	$x+1$	$ax+(a+1)$	a
$(a+1)x+$ $+(a+1)$	0	$(a+1)x+$ $+(a+1)$	$x+1$	$ax+a$	1	$(a+1)x+a$	x

$x+(a+1)$	ax	$ax+1$	$ax+a$	$ax+(a+1)$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+$ $+(a+1)$
0	0	0	0	0	0	0	0	0
$x+(a+1)$	ax	$ax+1$	$ax+a$	$ax+(a+1)$	$(a+1)x$	$(a+1)x+1$	$(a+1)x+a$	$(a+1)x+$ $+(a+1)$
$ax+1$	$(a+1)x$	$(a+1)x+a$	$(a+1)x+$ $+(a+1)$	$(a+1)x+1$	x	$x+a$	$x+(a+1)$	$x+1$
$(a+1)x+a$	x	$x+(a+1)$	$x+1$	$x+a$	ax	$ax+(a+1)$	$ax+1$	$ax+a$
$ax+a$	$ax+(a+1)$	$(a+1)x+$ $+(a+1)$	$a+1$	$ax+a$	$(a+1)x+1$	$ax+1$	$x+1$	1
$(a+1)x+1$	$a+1$	$x+a$	$ax+1$	$(a+1)x$	1	x	$ax+(a+1)$	$(a+1)x+a$
$a+1$	$x+(a+1)$	1	$(a+1)x$	$x+a$	$ax+1$	$(x+1)x+$ $+(a+1)$	a	x
x	$(a+1)x+$ $+(a+1)$	ax	$x+a$	1	$x+1$	a	$(a+1)x$	$ax+(a+1)$
$(a+1)x+$ $+(a+1)$	$(a+1)x+1$	$x+1$	1	$ax+1$	$x+a$	$(a+1)x+a$	$ax+a$	a
ax	$x+1$	$(a+1)x$	$ax+(a+1)$	a	$ax+a$	$a+1$	x	$(a+1)x+1$
$x+a$	1	$ax+(a+1)$	$(a+1)x+a$	x	a	ax	$(a+1)x+1$	$x+(a+1)$
1	$ax+1$	a	x	$(a+1)x+$ $+(a+1)$	$(a+1)x+a$	$x+1$	$a+1$	ax
$x+1$	$x+a$	$ax+a$	a	$(a+1)x+a$	$ax+(a+1)$	$x+(a+1)$	$(a+1)x+$ $+(a+1)$	$a+1$
a	$(a+1)x+a$	$a+1$	ax	$x+1$	$x+(a+1)$	$ax+a$	1	$(a+1)x$
$(a+1)x$	$ax+a$	x	$(a+1)x+1$	$a+1$	$(a+1)x+$ $+(a+1)$	1	ax	$x+a$
$ax+(a+1)$	a	$(a+1)x+1$	$x+(a+1)$	ax	$a+1$	$(a+1)x$	$x+a$	$ax+1$

$\frac{a}{2} \pm \frac{b}{2}\sqrt{-3}$, где a, b — нечетные целые. Можно все целые алгебраические числа из $Q(\sqrt{-3})$ представить также в виде $\omega = a + b\frac{1+\sqrt{-3}}{2}$, где $a, b \in Z$, т. е. в $Q(\sqrt{-3})$ фундаментальный базис состоит из 1 и $\frac{1+\sqrt{-3}}{2}$, а в $Q(\sqrt{-2})$ — из 1 и $\sqrt{-2}$.

Теорема 2.27 [22]. Пусть α — корень уравнения $x^2 + m = 0$, где m свободно от квадратов. Если $-m \equiv 2, 3 \pmod 4$, то

$$I = \mathrm{ENT}\{Q(\sqrt{-m})\} = \left\{a + \rho b \mid a,\ b \in Z,\ \rho = \frac{1}{2}(1 + \sqrt{-m})\right\}$$

— множество целых в квадратичном поле $Q(\sqrt{-m})$. Если $-m \equiv 1 \pmod 4$, то

$$I = \mathrm{ENT}\{Q(\sqrt{-m})\} = \left\{a + \rho b \mid a,\ b \in Z, \rho = \frac{1}{2}(1 - \sqrt{-m})\right\}.$$

Если необходимо перенести на кольцо I целых чисел поля $Q(\alpha)$ основы мультипликативной арифметики, свойственные кольцу Z, то тогда придется заняться теорией делимости в I, которая, как оказывается, имеет коренное отличие от мультипликативной арифметики кольца Z. Дело в том, что в I не существует однозначного разложения целых чисел на простые множители.

Пример 2.26. Рассмотрим поле $Q(\sqrt{-5})$. Так как $-5 \equiv 3 \pmod 4$, то $I = Z(\sqrt{-5}) = \{a + b\sqrt{-5} \mid a, b \in Z\}$. В этом кольце число 21 (и не только оно) допускает два существенно различных разложения на простые множители: $21 = 3 \times 7 = (1 + 2\sqrt{-5}) \times (1 - 2\sqrt{-5})$. То что числа 3; 7 и $1 \pm 2\sqrt{-5}$ простые, вытекает из следующих рассуждений. Если определить норму $N(\omega)$ целого числа $\omega = a + b\sqrt{-m}$ равенством $N(\omega) = a^2 + b^2 m$, то $N(3) = 9$, $N(7) = 49$ и $N(1 \pm 2\sqrt{-5}) = 21$. Поэтому, если бы числа 3; 7 и $1 \pm 2\sqrt{-5}$ были не простые, то из разложения $\omega = \omega_1\omega_2$ для $\omega = 3$; 7 или $1 \pm 2\sqrt{-5}$ следовало бы, что $N(\omega) = N(\omega_1)\,N(\omega_2)$, т. е. $N(\omega_i) = 3$, $N(\omega_i) = 7$, $i = 1, 2$, что невозможно, так как уравнение $x^2 + 5y^2 = 3$ (7) с $x, y \in Z$ неразрешимо. Этим доказана простота чисел 3; 7 и $1 \pm 2\sqrt{-5}$.

Казалось бы, обнаруженное явление неоднозначности разложения на простые множители в поле алгебраических чисел делает невозможным построение законченной I-арифметики. Однако Куммер показал, что, хотя I-арифметика радикально отличается от Z-арифметики, она может быть развита по образу и подобию ее [22, 178].

Основная идея заключалась в том, что если в I-арифметике разложение на простые множители неоднозначно, то отличные от нуля числа из I можно отобразить в некоторое новое множество, в котором умножение и разложение на простые множители однозначно. Тогда для всякого числа $\omega \neq 0$ его образ (ω) при этом отображении можно будет однозначно представить в виде произведения простых множи-

телей, но эти простые множители будут принадлежать не нашему кольцу, а некоторому новому множеству. Однозначность разложения должна восстановиться вследствие того, что некоторые простые числа из I отобразятся на непростые элементы нового множества, поэтому их образы будут иметь разложение на нетривиальные множители. Так, например, в кольце $I = \mathrm{ENT}(\sqrt{-5})$ для восстановления однозначности в разложении $21 = 3 \cdot 7 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5})$ должны существовать такие объекты p_1, p_2, p_3, p_4, что $3 = p_1 p_2$; $7 = p_3 p_4$; $1 + 2\sqrt{-5} = p_1 p_3$; $1 - 2\sqrt{-5} = p_3 p_4$. При этом будем иметь разложения $21 = p_1 p_2 p_3 p_4 = p_1 p_3 p_2 p_4$, которые отличаются только порядком сомножителей.

Куммер назвал эти новые объекты «идеальными» числами. Теперь их называют дивизорами. А в поле алгебраических чисел, как оказалось, дивизоры совпадают с идеалами. Действительно, если в $Q(\sqrt{-5})$ построить идеалы

$$p_1 = (3, 1 + 2\sqrt{-5}); \quad p_2 = (3, 1 - 2\sqrt{-5});$$
$$p_3 = (7, 1 + 2\sqrt{-5}); \quad p_4 = (7, 1 - 2\sqrt{-5}),$$

порождаемые двумя элементами, то будем иметь

$$p_1 p_2 = (3, 1 + 2\sqrt{-5})(3, 1 - 2\sqrt{-5}) = (3);$$
$$p_3 p_4 = (7, 1 + 2\sqrt{-5})(7, 1 - 2\sqrt{-5}) = (7).$$

Перемножив теперь главные идеалы (3) и (7), получим

$$p_1 p_2 p_3 p_4 = (3)(7) = (21).$$

Определение 2.13. Пусть A — произвольный идеал кольца $\mathrm{ENT}(Q(\alpha)) = I$. Два элемента x и y из I называются сравнимыми по модулю A ($x \equiv y \pmod{A}$) тогда и только тогда, когда $x - y$ принадлежит идеалу (дивизору) A или делится на дивизор A. Отсюда следует, что множество сравнимых элементов разбивает кольцо I на классы эквивалентных элементов. Тривиально доказывается, что эти классы образуют кольцо I/AI, называемое кольцом классов вычетов по модулю A. Если идеал A главный и порождается элементом Aa, то мы приходим к обыкновенным сравнениям по модулю некоторого целого числа A.

Теорема 2.28 [22]. Для любых взаимно простых дивизоров (идеалов) $A_1, A_2, \ldots, A_n$ и любых элементов $\beta_1, \beta_2, \ldots, \beta_n$ кольца I существует такой элемент $\xi \in I$, что

$$\xi = \beta_1 \pmod{A_1}; \quad \xi \equiv \beta_2 \pmod{A_2}; \quad \ldots; \quad \xi \equiv \beta_n \pmod{A_n}.$$

Отсюда следует китайская теорема об остатках.

Теорема 2.29 [22]. Кольцо классов вычетов I/AI (где $A = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$ — каноническое разложение идеала A) изоморфно прямой сумме классов вычетов $I/p_1^{\alpha_1}, I/p_2^{\alpha_2}, \ldots, I/p_n^{\alpha_n}$, т. е.

$$I/AI = I/p_1^{\alpha_1} + I/p_2^{\alpha_2} + \ldots + I_n/p_\alpha^n.$$

Определение 2.14. Нормой простого дивизора (идеала) p из I является степень простого целого рационального числа p^f. Число f называется степенью простого дивизора поля $Q(\alpha)$ относительно Q.

Отсюда вытекают два следствия: 1. Если $A = p$ — простой дивизор со степенью f, то

$$I/pI \sim \mathrm{GF}(p^f).$$

2. Если $A = p^n$, где p — простой дивизор со степенью f, то

$$I/Ip^n \sim Zp^f(\omega).$$

Здесь Zp^f — кольцо классов вычетов по модулю p^f.

9. Конечные гиперкомплексные системы

Простое поле Галуа GF (p) может быть расширено до конечного поля комплексных целых чисел, которое обозначим через Z_p^c или $Z[i]$, если не имеет решения в GF (p) следующее уравнение [5]: $x^2 + 1 = 0$. Это эквивалентно утверждению, что в поле GF (p) не существует корня порядка 4. Значит 4 не делит $p - 1$. Каждое целое в Z_p^c ($Z[i]$) изображается в виде $a + ib$, где $a, b \in \mathrm{GF}(p)$, $i^2 = -1$. Все арифметические операции выполняются, как и в обычной арифметике поля комплексных чисел, но учитывается то, что действительные и мнимые части определяются по mod p. Порядок поля Z_p^c равен p^2. Справедливо также равенство

$$(a + ib)^{p+1} = a^2 + b^2. \tag{2.20}$$

Это означает, что любое целое является самое большее корнем порядка $p + 1$ действительного целого числа в Z_p^c. В работе [5] рассмотрен метод нахождения комплексного целого числа и ω порядка $w = p^2 - 1$ в Z_p^c.

Из выражения (2.20) следует, что $(p + 1) \mid (p^2 - 1)$. Очевидно, что $(p^2 - 1)/(p + 1) = p - 1$. Следовательно, равенство (2.20) можно записать в виде

$$(a + ib)^{\frac{p^2-1}{p-1}} = a^2 + b^2,$$

что означает, что среди системы степеней $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{p^2-1}$ ($\varepsilon \in Z_p^c$) имеется ровно $p - 1$ действительных элементов поля Z_p^c. Корень N-ой степени из единицы существует в Z_p^c только, если $N \mid (p^2 - 1)$.

В случае если модуль является составным числом, т. е. $p = M = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, где p_i — простые, а α_i — целые числа ($i = 1, 2, \ldots, n$), получаем конечное кольцо комплексных целых чисел, которое обозначим через Z_M^c. Кольцо Z_M^c является модулем над Z_M, а поле Z_p^c — векторным пространством над GF (p).

Ниже будет показано, что для ряда задач ЦОС приходится использовать поле GF (p) с большим значением модуля p. Это увеличивает

Таблица 21. Правила умножения кватернионов

·	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

время выполнения арифметических операций по модулю p при реализации. Составное поле Галуа GF (p^v), обладая примерно таким же порядком, как поле GF (p), при значительно меньших значениях p позволяет параллельное выполнение операций над компонентами многочлена, являющегося элементом поля GF (p^v). Однако есть существенное ограничение. Операция умножения элементов поля GF (p^v) выполняется по модулю неприводимого над GF (p) многочлена, что связано с операцией деления многочленов, которая требует больших затрат оборудования и времени. В этой связи представляет интерес рассмотрение систем, являющихся алгебраическими над полем GF (p) (например, поле Z_p^c). Операция умножения в таких системах выполняется без проведения по модулю неприводимого многочлена. Возможность параллельного выполнения операций сохраняется.

Известны следующие алгебраические системы с делением, являющиеся алгебрами над полем действительных чисел: система комплексных чисел, системы кватернионов и октав [68]. Элементы системы октав называют еще числами Кэли [85]. Рассмотрим аналогичные конечные системы, являющиеся алгебрами над полем GF (p): конечное поле комплексных целых чисел; конечное кольцо кватернионов и конечное неассоциативное кольцо чисел Кэли.

Определение 2.15. Числа вида

$$h = a + ib + jc + kd \tag{2.21}$$

с законом сложения, определяемым выражением

$$(a_1 + ib_1 + jc_1 + kd_1) + (a_2 + ib_2 + jc_2 + kd_2) = (a_1 + a_2) + \\ + i(b_1 + b_2) + j(c_1 + c_2) + k(d_1 + d_2) \tag{2.22}$$

и умножением, которое осуществляется с помощью правил умножения многочленов и таблицы умножения элементов i, j, k (табл. 21), называются кватернионами [68, 85]. Из табл. 21 видно, что для умножения кватернионов не выполняется закон коммутативности, но закон ассоциативности выполняется.

Определение 2.16. Кватернион $\bar{h} = a - ib - jc - kd$ называется сопряженным кватерниону $h = a + ib + jc + kd$.

Определение 2.17. Неотрицательное действительное число $n(h) = a^2 + b^2 + c^2 + d^2 = h\bar{h} = \bar{h}h$, равное нулю только в случае, когда $h = 0$, называется нормой кватерниона h.

В работах [68, 85] показано, что справедливо следующее равенство:

$$\left(\frac{1}{n(h)}\,\bar{h}\right) h = 1, \tag{2.23}$$

из которого следует, что для всякого отличного от нуля кватерниона h существует обратный кватернион, поэтому элементы алгебры кватернионов над R образуют тело.

Теорема 2.30. Над полем GF (p) можно определить алгебру кватернионов, если следующее уравнение не имеет решения в GF (p):

$$x^2 + 1 = 0. \tag{2.24}$$

Доказательство. Любой кватернион h можно представить в виде $h = \omega_1 + j\omega_2$, где $\omega_1 = a_1 + ib_1$, $\omega_2 = a_2 + ib_2$ — комплексные целые числа, принадлежащие Z_p^c. Поле GF (p) может быть расширено до поля Z_p^c только в случае, если в нем уравнение (2.24) не имеет решения. Учитывая, что $j^2 = 1$, приходим к заключению теоремы.

Элементы алгебры кватернионов над GF (p) — это многочлены вида (2.21), сложение которых осуществляется согласно выражению (2.22) с той особенностью, что отдельные члены a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 суммируются по модулю p. Умножаются кватернионы, определенные над GF (p), как обычные многочлены с использованием табл. 21. Но опять же, отдельные произведения членов a_1, a_2, b_1, b_2, c_1, c_2, d_1, d_2 осуществляются по правилам арифметики поля GF (p), т. е. по модулю p.

Теорема 2.31. Элементы алгебры кватернионов, определенной над полем Галуа GF (p), образуют кольцо.

Доказательство. Действительно, в этом случае $n(\omega) = a^2 + b^2 + c^2 + d^2$ может принимать значение, равное нулю при ненулевых значениях $a, b, c, d \in$ GF (p). Это следует из теоремы о четырех квадратах [123], в которой доказано, что уравнение

$$m = a^2 + b^2 + c^2 + d^2,$$

где m — любое положительное число, имеет решение, в котором a, b, c, d — неотрицательные числа. Следовательно, для кватерниона $h = a + ib + jc + kd$ ($a, b, c, d \in$ GF (p)), норма которого $n(h) = a^2 + b^2 + c^2 + d^2$ равна p, не существует обратного, так как $p \equiv 0 \pmod p$ и $n(h)$ фигурирует в знаменателе выражения (2.23). Значит, в алгебре кватернионов над GF (p) существуют делители нуля и элементы ее образуют кольцо, которое обозначим через Z_p^H. Теорема доказана.

Определение 2.18. Элементы алгебры кватернионов над GF (p) (элементы кольца Z_p^H) назовем кватернионами над GF (p).

Максимальная степень корня из единицы $\sqrt[N]{1} \in Z_p^H$ будет меньше порядка кольца Z_p^H. Различные степени корня $\sqrt[N]{1} \in Z_p^H$ образуют подгруппу мультипликативной полугруппы с единицей кольца Z_p^H. Обозначим мультипликативную подгруппу кольца Z_p^H через S_p^H. В теории полугрупп [74] известна теорема, утверждающая, что для любой циклической подполугруппы $\langle a \rangle$ полугруппы S существуют два положительных целых числа, индекс r и период N элемента a, для которых

$a^{N+r} = a^r$ и

$$\langle a \rangle = \{a, a^2, \ldots, a^{N+r-1}\}.$$

Порядок подполугруппы $\langle a \rangle$ равен $N + r + 1$. Множество

$$K_\alpha = \{a^r, a^{r+1}, \ldots, a^{N+r-1}\}$$

является циклической подгруппой порядка N полугруппы S. При $r = 0$ получаем

$$K_\alpha = \{a^0, a^1, \ldots, a^{N-1}\},$$

т. е. множество K_α представляет собой систему степеней первообразного элемента a.

Получить аналитические выражения для определения порядка всех подгрупп полугруппы S_p^H — очень сложная задача. Такие задачи сложны даже для неабелевых групп [76]. Мы же имеем дело с полугруппой. Однако подобного рода перечислительные задачи можно решать с успехом при помощи вычислительных машин [53]. При небольших значениях порядка поля GF (p), над которым определяется Z_p^H, это можно сделать вручную. Например, если GF (p) = GF (3), то период любого кватерниона над этим полем равен 3 или 6 (естественно, при $a \neq 0$, $b \neq 0$, $c \neq 0$ и $d \neq 0$). Над полем GF (7) найдены элементы с периодом, равным 6 ($h = 1 + i + j + k$, $h = 2 + i + 2j + k$) и 24 ($h = 3 + 5i + 2j + k$).

Упражнение 2.8. Найти степени всех элементов кольца Z_p^H над полем GF (3).

Отметим, что теоретико-числовые свойства кватернионов изучались многими авторами (см. например, [68, 151, 152, 162, 163]). Рассматривались и вопросы применения систем кватернионов в задачах, стоящих перед вычислительной техникой [162, 163]. Однако в этих работах кватернионы исследуются над полем действительных чисел, свойства кватернионов, определенных над полями Галуа, практически не изучены.

Над полем R возможно построение восьмимерной алгебры с однозначным делением и с единицей, называемой алгеброй Кэли [68, 85 109].

Определение 2.19. Элементы алгебры Кэли, представляющие собой выражения вида

$$\gamma + he, \tag{2.25}$$

где γ и h — кватернионы; e — новый символ, называются числами Кэли.

Сложение чисел Кэли и умножение их на действительное число задаются равенствами

$$(\gamma_1 + h_1 e) + (\gamma_2) + h_2 e) = (\gamma_1 + \gamma_2) + (h_1 + h_2)\, e; \tag{2.26}$$

$$(\gamma + he)\, a = \gamma a + (ha)\, e. \tag{2.27}$$

Числа Кэли образуют восьмимерное действительное векторное пространство с базой

$$1, i, j, k, e, ie, je, ke. \tag{2.28}$$

Таблица 22. Умножение в алгебре Кэли

·	1	i	j	k	e	ie	je	ke
1	1	i	j	k	e	ie	je	ke
i	i	-1	k	$-j$	ie	$-e$	$-ke$	je
j	j	$-k$	-1	i	je	ke	$-e$	$-ie$
k	k	j	$-i$	-1	ke	$-je$	ie	$-e$
e	e	$-ie$	$-je$	$-ke$	-1	i	j	k
ie	ie	e	$-ke$	je	$-i$	-1	$-k$	j
je	je	ke	e	$-ie$	$-j$	k	-1	$-i$
ke	ke	$-je$	ie	e	$-k$	$-j$	$-i$	-1

Умножение в этом пространстве определяется равенством

$$(\gamma_1 + h_1 e)(\gamma_2 + h_2 e) = (\gamma_1\gamma_2 - h_2 h_1) + (h_2\gamma_1 + h_2\gamma_2)\, e. \qquad (2.29)$$

Правило умножения элементов базиса (2.28) задается табл. 22. Алгебра Кэли не является ни коммутативной, ни ассоциативной. Числа Кэли образуют неассоциативное тело.

Определение 2.20. Число Кэли $\bar{\xi} = \bar{\gamma} - he$ называется сопряженным числу $\xi = \gamma + he$.

Определение 2.21. Неотрицательное действительное число $h(\xi) = h(\gamma) + h(h)$, равное нулю только при $\xi = 0$, называется нормой элемента ξ.

Теорема 2.32. Над полем GF (p) можно определить алгебру Кэли, если следующее уравнение не имеет решения в GF (p):

$$x^2 + 1 = 0. \qquad (2.30)$$

Доказательство. Любое число Кэли представляется в виде (2.25). Элементы γ и h принадлежат кольцу Z_p^H, которое может быть определено, если уравнение (2.30) не имеет решений в поле GF (p). Учитывая, что $e^2 = -1$ (см. табл. 22), приходим к заключению теоремы.

Теорема 2.33. Элементы алгебры Кэли над GF (p) образуют неассоциативное кольцо.

Доказательство. Доказательство теоремы сводится к доказательству того, что при определении алгебры Кэли над полем GF (p) эта алгебра содержит делители нуля. Очевидно, что все аксиомы кольца выполняются (кроме ассоциативности операции умножения). Справедливо следующее равенство [68, 85]:

$$n(\xi_1, \xi_2) = [n(\gamma_1) + n(h_1)]\,[h(\gamma_2) + n(h_2)] = n(\xi_1)\,n(\xi_2), \quad (2.31)$$

где $\xi_1 = \gamma_1 + h_1 e$; $\xi_2 = \gamma_2 + h_2 e$; γ_1, h_1, γ_2, h_2 — кватернионы. А так как при определении алгебры Кэли над GF (p) нормы $n(\gamma_1)$, $n(h_1)$, $n(\gamma_2)$, $h(h_2)$ могут принимать нулевые значения в случае ненулевых γ_1, γ_2, h_1, h_2 (см. теорему 2.31), то и норма произведения двух элементов ξ_1 и ξ_2 алгебры Кэли над GF (p) может принимать нулевое значение при ненулевых ξ_1 и ξ_2. Следовательно, алгебра Кэли над GF (p) содержит делители нуля, и, значит, неассоциативным телом не является. Элементы этой алгебры образуют конечное неассоциативное кольцо, которое обозначим через Z_p^k. Теорема доказана.

Определение 2.22. Элементы алгебры Кэли над полем GF (p) (элементы кольца Z_p^k) назовем числами Кэли над полем Галуа GF (p).

Порядки элементов алгебры Кэли над GF (p) могут находиться перечислительными методами на ЭВМ.

10. Векторные пространства

Определим векторное пространство V над полем F как алгебраическую систему, удовлетворяющую следующим условиям:

1) пространство V является аддитивной абелевой группой;

2) для любых $x \in V$ и $\alpha \in F$ определено произведение αx, являющееся элементом пространства V;

3) если $x, y \in V$; $\alpha \in F$, то $\alpha(x + y) = \alpha x + \alpha y$;

4) если $x \in V$; $\alpha, \beta \in F$, то $(\alpha + \beta)\,x = \alpha x + \beta x$;

5) если $x \in V$; $\alpha, \beta \in F$, то $(\alpha\beta)\,x = \alpha(\beta x)$;

6) $1 \cdot x = x$ (1 — единичный элемент поля F, т. е. единичный элемент мультипликативной группы поля F).

В качестве примера векторного пространства можно привести поле F, которое рассматривается как векторное пространство над самим собой. Элементы векторного пространства называются векторами.

Упражнение 2.9. Доказать, что многочлены степени не выше m, определенные над полем F, являются векторным пространством.

Определение 2.23. Векторы $x_1, x_2, \ldots, x_m$ векторного пространства V называются линейно зависимыми, если существуют такие числа $\alpha_1, \alpha_2, \ldots, \alpha_m \in F$, не равные одновременно нулю, что

$$\alpha_1 x + \alpha_2 x_2 + \cdots + \alpha_m x_m = 0.$$

Векторы, не являющиеся линейно зависимыми, называются линейно независимыми.

Определение 2.24. Векторное пространство V называется n-мерным, если в нем можно найти n линейно независимых векторов, но больше чем n линейно независимых векторов оно не содержит.

Размерность векторного пространства — это максимальное число содержащихся в нем линейно независимых векторов. Например, размерность векторов на плоскости равна 2, размерность множества векторов в пространстве равна 3; понятно, что размерность n-мерного пространства по определению равна n; размерность поля Галуа GF (p), рассматриваемого как векторное пространство, равна 1.

Определение 2.25. Совокупность n линейно независимых векторов n-мерного векторного пространства V называется его базисом.

Теорема 2.34. Каждый вектор x линейного n-мерного пространства V можно представить, притом единственным способом, в виде линейной комбинации векторов базиса. Векторное пространство V над полем F обладает следующими свойствами:

1) $0 \cdot x = 0$ (0 в левой части равенства — единичный элемент аддитивной группы поля F; 0 в правой части равенства — элемент пространства V, являющийся единичным элементом аддитивной группы V и называемый нулевым вектором);

2) $(-1)\, x = -x$, $-1 \in F$, $x \in V$, $-x \in V$;

3) если $\alpha x = 0 \in V$, то при $\alpha \neq 0$ всегда $x = 0$.

Пусть $V_n(F)$ — множество всех последовательностей $(x_1, \ldots, x_n)$ длины n с компонентами из поля F, т. е. $V_n(F) = \{x$, таких, что $x = (x_1, \ldots, x_n)$, $x_i \in F$, $i = 1, 2, \ldots, n\}$.

Сумма и умножение определяются следующим образом:

$$x + y = (x_1 + y_1, x_2 + y_2, \ldots, x_n + y_n);$$

$$\alpha x = (\alpha x_1, \alpha x_2, \ldots, \alpha x_n),$$

где $y = (y_1, y_2, \ldots, y_n)$.

Тогда $V_n(F)$ является векторным пространством над полем F.

Упражнение 2.10. Проверить, что $V_n(F)$ — векторное пространство.

Определение 2.26. Подмножество W векторного пространства V, удовлетворяющее условиям:

1) если $w_1, w_2 \in W$, то $w_1 + w_2 \in W$;

2) для любых $\alpha \in F$ и $w \in W$ элемент $\alpha w \in W$, само является векторным пространством над полем F и называется подпространством векторного пространства V.

Понятие подпространства векторного пространства очень важно и в дальнейшем будет часто использоваться.

* * *

Таким образом, алгебраические системы можно использовать для определения преобразований, которым подвергается сигнал в процессе обработки, т. е. для построения математических моделей систем обработки. Элементы колец Z_M или полей GF (p) обычно кодируются целыми числами. Операции сложения и умножения в этих системах представляют собой операции суммы и умножения целых чисел по модулю M (по модулю p). Реализация таких операций проще по сравнению с реализацией арифметических операций поля комплексных чисел. Следовательно, использование конечных алгебраических

систем для построения математических моделей систем ЦОС позволит повысить технико-экономические показатели этих систем.

Среди многообразия конечных алгебраических систем, обладающих структурой кольца, необходимо выделить и изучить те, арифметические операции которых наиболее просто реализуются. Задача эта очень важна, так как даже для изоморфных алгебраических систем реализация арифметических операций может оказаться различной по аппаратурным затратам и быстродействию. Не менее важной является задача разработки и изучения методов реализации арифметических операций конечных алгебраических систем с помощью цифровых аппаратных средств.

ГЛАВА 3

ХАРАКТЕРЫ КОНЕЧНЫХ АБЕЛЕВЫХ ГРУПП. ОБОБЩЕННЫЕ ФУНКЦИИ И ОРТОГОНАЛЬНЫЕ ПРЕОБРАЗОВАНИЯ СИГНАЛОВ

1. Определение характеров и их основные свойства

Рассмотрим преобразование Фурье в пространстве всех функций, заданных на абелевой группе $H = H_{h_1} \dotplus H_{h_2} \dotplus \ldots \dotplus H_{h_n}$ и принимающих значения в некотором поле F, т. е. областью определения функций является группа H, областью значений — поле F. Это пространство обозначим через $L(H, F)$. Найдем сначала в $L(H, F)$ функции, являющиеся аналогами комплексных экспонент. Экспоненты $e^{i\alpha x}$ — решения функционального уравнения $f(x_1 + x_2) = f(x_1) f(x_2)$ над полем комплексных чисел. Поэтому аналогами экспонент в пространстве $L(H, F)$ будут решения функционального уравнения

$$f(x_1 \oplus x_2) = f(x_1) f(x_2), \; F \tag{3.1}$$

над полем F.

Покажем, что функции, удовлетворяющие этому уравнению и требованию $f(0) = 1$, образуют полную ортонормированную систему функций в пространстве $L(H, F)$. Обычно эти функции называют характерами группы H и обозначают $\chi(x)$.

Из равенства (3.1) следует, что числа поля F $f(x)$, соответствующие элементам $x \in H$, перемножаются аналогично тому, как складываются их оригиналы x, т. е. f — гомоморфизм группы H в поле F. Причем образ группы H при отображении $f : H \to F$ изоморфен группе H, т. е. $\operatorname{Im} f \sim H$. Таким образом, $\operatorname{Im} f$ — подгруппа мультипликативной группы поля F. Порядок этой подгруппы равен порядку группы H в силу их изоморфизма и поэтому число $[H : 1]$ должно делить порядок мультипликативной группы поля F. Если поле $F = C$, то в поле комплексных чисел существуют подгруппы любых порядков. В частности, мультипликативная подгруппа порядка $h = [H : 1]$ может быть образована всеми корнями h-й степени из единицы:

$$\varepsilon_\alpha = \sqrt[h]{1} = e^{i\frac{2\pi}{n}\alpha}, \quad \alpha = 0, 1, \ldots, h-1.$$

Действительно, это мультипликативная подгруппа порядка h и у каждого ε_α существует обратный ε_α^{-1}, являющийся корнем h-й степени. Если поле F является конечным полем Галуа GF (p), то мульти-

пликативная группа состоит из $p-1$ элементов. Поэтому в силу теоремы Лагранжа необходимо потребовать делимости $p-1$ на h. Предположим, что это выполняется, и докажем, что характеры можно определить как гомоморфизм χ в группу корней h-й степени из 1. Действительно, пусть элемент ε имеет максимальный порядок h, т. е. $\varepsilon^h = 1$. Тогда формально можно написать $\varepsilon = \sqrt[h]{1} \in \mathrm{GF}(p)$, т. е. ε является корнем степени h из 1 в поле $\mathrm{GF}(p)$, а этот корень существует в конечном поле в том случае, когда $h \mid (p-1)$. После таких предварительных соображений можно решить главную задачу: определить все решения функционального уравнения (3.1), т. е. найти все характеры группы H и исследовать их свойства.

Для начала задачу упростим и примем, что H — циклическая прямонеразложимая группа порядка $[H:1] = p_i^{\alpha_i} = h_i$. Пусть в поле F существует корень h_i-й степени. Это означает, что в поле F существует решение уравнения $x^{h_i} = 1$. Найдем все решения этого уравнения. Если обозначить корень h_i-й степени из 1 в поле F через ε_i, то, очевидно, что все решения будут иметь вид ε_i^{α} $(0 \leqslant \alpha \leqslant h_i - 1)$. Действительно, $(\varepsilon_i^{\alpha})^{h_i} = (\varepsilon_i)^{h_i \alpha} = 1$. Каждому решению можно поставить во взаимнооднозначное соответствие характер группы H, т. е. функцию вида $\chi_{\alpha}(x) = \varepsilon^{\alpha x}$, где $x \in H = \{0, 1, \ldots, h_i - 1, \oplus\}$. Действительно, в этом случае удовлетворяются все свойства характеров

$$\chi_{\alpha}(x \oplus y) = \chi_{\alpha}(x)\,\chi_{\alpha}(y), \quad \chi_{\alpha}(0) = 1, \quad F.$$

Поскольку α изменяется в пределах от 0 до $h_i - 1$, то число характеров равно числу элементов группы.

Рассмотрим общий случай, когда группа H равна прямой сумме подгрупп предыдущего вида $H = H_{h_1} \dotplus H_{h_2} \dotplus \ldots \dotplus H_{h_n}$, где $[H:1] = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$; $h_1, h_2, \ldots, h_i, \ldots, h_n$ — порядки подгрупп H_{h_i}; p_i $(i = 1, 2, \ldots, n)$ — простые числа (не обязательно все разные).

Любой элемент группы H, $x \in H$, имеет вид n-ки (n-ка — это набор из n элементов):

$$x = (x_1, x_2, \ldots, x_n), \quad x_i \in H_i.$$

Сложение в H определяется следующим образом:

$$Z = (x \oplus y) = (x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) = \\ = (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n), \tag{3.2}$$

где $x_i \oplus y_i = z_i \pmod{h_i}$.

Так как группы H_{h_i} и $0 \dotplus 0 \dotplus \ldots \dotplus H_{h_i} \dotplus \ldots \dotplus 0$ изоморфны, то элемент $x_i \in H_i$ можно отождествить с элементом $(0, 0, \ldots, x_i, \ldots, 0)$. Тогда произвольный элемент $x = (x_1, x_2, \ldots, x_n)$ можно представить как сумму

$$x = (x_1, x_2, \ldots, x_n) = (x_1, 0, \ldots, 0) \oplus (0, x_2, \ldots, 0) \oplus \\ \oplus (0, 0, \ldots, x_n) = \sum_{i=1}^{n} x_i.$$

Поэтому для всех характеров группы $H = H_{h_1} \dotplus H_{h_2} \dotplus \ldots \dotplus H_{h_n}$ должно выполняться равенство

$$\chi(x) = \chi\left(\sum_{i=1}^{n} x_i\right) = \chi(x_1)\,\chi(x_2)\,\ldots\,\chi(x_n).$$

Это означает, что все характеры группы H исчерпываются функциями вида

$$\chi_\alpha(x) = \varepsilon_1^{\alpha_1 x_1}\varepsilon_2^{\alpha_2 x_2}\ldots\varepsilon_n^{\alpha_n x_n} = \chi_{\alpha_1}(x_1)\,\chi_{\alpha_2}(x_2)\,\ldots\,\chi_{\alpha_n}(x_n), \qquad (3.3)$$

где $\varepsilon_i = \sqrt[h_i]{1}$.

Вводя n-ки $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, имеем

$$\chi_\alpha(x) = \chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \varepsilon_1^{\alpha_1 x_1}\varepsilon_2^{\alpha_2 x_2}\ldots\varepsilon_n^{\alpha_n x_n}.$$

Число разных характеров такого вида $h = h_1 h_2 \ldots h_n$. И в этом случае число характеров равно порядку группы $[H : 1] = h_1 h_2 \ldots h_n$. Если все $\alpha_1 = \alpha_2 = \ldots = \alpha_n$, то характер называется единичным $\chi_0(x) \equiv 1$.

Используя равенство (3.3), можно написать

$$\chi_\alpha(x)\,\chi_\beta(x) = \prod_{i=1}^{n}\varepsilon_i^{\alpha_i x_i}\prod_{i=1}^{n}\varepsilon_i^{\beta_i x_i} = \prod_{i=1}^{n}\varepsilon_i^{(\alpha_i \oplus \beta_i)x_i} = \prod_{i=1}^{n}\varepsilon_i^{\gamma_i x_i} = \chi_\gamma(x),$$

где $\alpha_i \oplus \beta_i = \gamma_i \pmod{h_i}$, $i = 1, 2, \ldots, n$.

Таким образом, на множестве n-ок $(\alpha_1, \alpha_2, \ldots, \alpha_n) = \alpha$ можно рассматривать групповую структуру с законом покомпонентного сложения. Нетрудно видеть, что при этом получается коммутативная группа, изоморфная группе H, которую обозначим H^* и назовем двойственной по отношению к H.

В пространстве $L(H, C)$ можно просто и наглядно интерпретировать характеры в виде многомерных дискретных экспоненциальных функций. Предположим, что изучается функция $f(x_1, x_2, \ldots, x_n)$ от n целочисленных переменных $x_i \in Z$. Примем, что эти функции периодичны по первой координате x_1 с периодом h_1, по второй координате x_2 с периодом h_2, по третьей —с периодом h_3 и т. д., т. е. $f(x_1 + h_1; x_2 + h_2; \ldots; x_n + h_n) = f(x_1, x_2, \ldots, x_n)$. Тогда можно ограничиться изучением поведения этих функций на n-мерном целочисленном параллелепипеде со сторонами длины $h_1, h_2, \ldots, h_n$. Назовем его h-брусом, где $h = (h_1, h_2, \ldots, h_n)$. В случае, когда $h_1 = h_2 = \ldots = h_n$, получается, очевидно, n-куб. Тогда любую такую периодическую функцию можно разложить в многомерный дискретный ряд Фурье:

$$f(x_1, x_2, \ldots, x_n) =$$

$$= \sum_{\alpha_1}\sum_{\alpha_2}\ldots\sum_{\alpha_n} S(\alpha_1, \alpha_2, \ldots, \alpha_n)\, e^{i\frac{2\pi}{h_1}\alpha_1 x_1}\ldots e^{i\frac{2\pi}{h_n}\alpha_n x_n},$$

где

$$S(\alpha_1, \alpha_2, \ldots, \alpha_n) =$$

$$= \sum_{x_1}\sum_{x_2}\ldots\sum_{x_n} f(x_1, x_2, \ldots, x_n)\, e^{-i\frac{2\pi}{h_1}\alpha_1 x_1}\ldots e^{-i\frac{2\pi}{h_n}\alpha_n x_n}.$$

Таким образом, h функций

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \varepsilon_1^{\alpha_1 x_1}\varepsilon_2^{\alpha_2 x_2} \ldots \varepsilon_n^{\alpha_n x_n}$$

также определены на h-брусе $[0, h, -1] \times [0, h_2 - 1] \times \ldots \times [0, h_n - 1]$. Здесь $\varepsilon_j^{hj} = \sqrt{1} = e^{i\frac{2\pi}{h_j}}$. Два множества точек $\{x\} = \{(x_1, x_2, \ldots, x_n)\}$, $\{\alpha\} = \{(\alpha_1, \alpha_2, \ldots, \alpha_n)\}$, образующих подобные брусы, обозначим соответственно H и H^*. Введем на этих множествах операции сложения:

$$z = (x \oplus y) = (x_1, x_2, \ldots, x_n) \oplus (y_1, y_2, \ldots, y_n) =$$
$$= (x_1 \oplus y_1, x_2 \oplus y_2, \ldots, x_n \oplus y_n) = (z_1, z_2, \ldots, z_n);$$
$$\gamma = (\alpha \oplus \beta) = (\alpha_1, \alpha_2, \ldots, \alpha_n) \oplus (\beta_1, \beta_2, \ldots, \beta_n) =$$
$$= (\alpha_1 \oplus \beta_1, \alpha_2 \oplus \beta_2, \ldots, \alpha_n \oplus \beta_n) = (\gamma_1, \gamma_2, \ldots, \gamma_n),$$

где $z_i = x_i \oplus y_i \pmod{h_i}$; $\gamma_i = \alpha_i \oplus \beta_i \pmod{H_i}$.

Тогда относительно этих операций множества H и H^* превращаются в группы, а после замены ε_i на $e^{-i\frac{2\pi}{h_i}}$ из многомерных комплексно-экспоненциальных функций получается выражение (3.3) для характеров:

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \varepsilon_1^{\alpha_1 x_1}\varepsilon_2^{\alpha_2 x_2} \ldots \varepsilon_n^{\alpha_n x_n}. \qquad (3.4)$$

Их естественной областью определения являются группы H, H^* или h-брусы. Нам бы хотелось иметь функции с подобными свойствами, но определенными на целочисленной оси времени Z. Достичь этого можно вложением группы H в дискретную ось времени. О том, как это можно осуществить, будет изложено ниже. Сейчас мы опишем некоторые свойства характеров, которые понадобятся при изучении ортогональных преобразований.

Первым и основным свойством характеров, которое непосредственно следует из определения, является свойство инвариантности относительно группового сдвига:

$$\chi_\alpha(x \oplus x_{сд}) = \chi_\alpha(x_{сд})\,\chi_\alpha(x).$$

Второе, не менее важное, свойство — мультипликативность характеров. Это свойство означает, что произведение двух характеров всегда дает новый характер:

$$\chi_\alpha(x)\,\chi_\beta(x) = \chi_{\alpha\oplus\beta}(x).$$

Поскольку все ε_i являются корнями h_i-й степени из 1, то

$$\chi_\alpha(x)\,\overline{\chi}_\alpha(x) = \chi_\alpha(x \ominus x) = \chi_\alpha(0) = 1.$$

В связи с этим для сопряженного характера $\overline{\chi}_\alpha(x)$ введем следующее обозначение:

$$\overline{\chi}_\alpha(x) = \chi_{\ominus\alpha}(x) = \chi_{h\ominus\alpha}(x) = \chi_\alpha(\ominus x) = \chi_\alpha(h \ominus x),$$

где $h \ominus \alpha = (h_1 \ominus \alpha_1, \ldots, h_n \ominus \alpha_n)$; $h \ominus x = (h_1 \ominus x_1, \ldots, h_n \ominus x_n)$; $\ominus$ — операция вычитания по модулю h_i.

Из аналитического выражения для $\chi_\alpha(x)$ следует свойство симметричности характеров $\chi_\alpha(x) = \chi_x(\alpha)$. Нетрудно видеть, что относительно операции умножения характеры образуют группу. Установим теперь некоторые соотношения между значениями характеров. Для единичного характера имеем $\sum\limits_{x \in H} \chi_0(x) = h$. Пусть характер $\chi_\alpha(x)$ не является единичным, так что $\chi_\alpha(z) \neq 1$ для некоторого $z \in H$. Если x пробегает все элементы из группы H, то $z \oplus x$ также пробегает все элементы из H. Полагая $S = \sum\limits_{x \in H} \chi_\alpha(x)$, имеем

$$S = \sum_{x \in H} \chi_\alpha(z \oplus x)\, \chi_\alpha(z)\, S.$$

Поскольку $\chi_\alpha(z) \neq 1$, полученное равенство возможно лишь при $S = 0$. Поэтому

$$\sum_{x \in H} \chi_\alpha(x) = \begin{cases} h, & \chi_\alpha(x) = \chi_0(x); \\ 0, & \chi_\alpha(x) \neq \chi_0(x). \end{cases} \tag{3.5}$$

Далее значение любого характера $\chi_\alpha(x)$ при $x = 0$ равно единице, поэтому $\sum\limits_{\alpha \in H^*} \chi_\alpha(0) = h$. Положим, $T = \sum\limits_{\alpha \in H} \chi_\alpha(x)$. Пусть для некоторого $\beta \in H^*$ имеем $\chi_\beta(x) \neq 1$. Если α пробегает все H^*, то и $\beta \oplus \alpha$ пробегает H^*. Поэтому

$$T = \sum_{\alpha \in H} \chi_{\alpha \oplus \beta}(x) = \chi_\beta(x)\, T,$$

а так как $\chi_\beta(x) \neq 1$, то $T = 0$. Этим доказана формула

$$\sum_{\alpha \in H^*} \chi_\alpha(x) = \begin{cases} h, & x = 0; \\ 0, & x \neq 0. \end{cases} \tag{3.6}$$

Теперь на характеры $\chi_\alpha(x)$ можно смотреть и как на систему функций $\{\chi_\alpha(x)\}$, $\alpha = 0, 1, \ldots, h-1$ в пространстве $L(H, F)$, и как на систему $\{\chi_\alpha(x)\}$, $x = 0, 1, \ldots, h-1$ в пространстве $L(H^*, F)$. Оказывается, что эти системы функций образуют, каждая в своем пространстве, ортонормированные базисы [22]. Докажем это.

В пространствах $L(H, F)$ и $L(H^*, F)$ введем скалярные умножения:

$$\langle \varphi(x) \mid \Psi(x) \rangle_{L(H,F)} = \frac{1}{h} \sum_{x \in H} \varphi(x)\, \overline{\Psi}(x); \tag{3.7}$$

$$\langle \varphi(\alpha) \mid \Psi(\alpha) \rangle_{L(H^*,F)} = \frac{1}{h} \sum_{\alpha \in H^*} \varphi(\alpha)\, \overline{\Psi}(\alpha). \tag{3.8}$$

Тогда имеет место следующая теорема.

Теорема 3.1. Пусть $\{\chi_\alpha(x)\}$ ($\alpha \in H^*$, $x \in H$) — характеры группы H. Тогда они образуют ортонормированный базис в пространствах $L(H, F)$ и $L(H^*, F)$ относительно скалярных произведений (3.7) и (3.8).

Доказательство. Докажем сначала ортонормированность, а потом полноту. Так как

$$\langle \chi_\alpha(x) \mid \chi_\beta(x)\rangle_{L(H,F)} = \frac{1}{h}\sum_{x\in H}\chi_\alpha(x)\,\overline{\chi}_\beta(x) = \frac{1}{h}\sum_{x\in H}\chi_{\beta\ominus\alpha}(x),$$

то, используя (3.5), получаем

$$\langle \chi_\alpha(x) \mid \chi_\beta(x)\rangle_{L(H,F)} = \delta_{\alpha\beta}.$$

Аналогично имеем

$$\langle \chi_{\alpha(x)} \mid \chi_\beta(x)\rangle_{L(H^*,F)} = \delta_{xy}.$$

Таким образом, в пространствах $L(H, F)$ и $L(H^*, F)$ мы построили по h ортонормированных функций. Поскольку эти пространства h-мерные, то эти системы полны.

Из этой теоремы следует, что произвольную функцию можно разложить в ряд

$$f(x) = \sum_{\alpha\in H^*} S_f(\alpha)\,\chi_\alpha(x) = D^{-1}\{S(\alpha)\}, \tag{3.9}$$

где

$$S_f(\alpha) = \frac{1}{h}\sum_{\alpha\in H} f(x)\,\overline{\chi}_\alpha(x) = D\{f(x)\}. \tag{3.10}$$

Этими преобразованиями устанавливается взаимооднозначное соответствие между пространствами $L(H, F)$ и $L(H^*, F)$:

$$L(H,F) \xrightarrow{D} L(H^*,F) \xrightarrow{D^{-1}} L(H,F); \quad f(x) \xrightarrow{D} S_f(\alpha) \xrightarrow{D^{-1}} f(x).$$

Это означает, что оператор D переводит функции $f(x)$ в функции $S_f(\alpha) \in L(H^*, F)$, а оператор D^{-1} действует обратно. Пару этих преобразований называют [92] обратным и прямым преобразованиями Фурье на абелевой группе H.

Рассмотрим теперь более подробно условие существования корней $(h_1, h_2, \ldots, h_n)$-й степеней в поле F. Пусть $q = \text{НОК}(h_1, h_2, \ldots, h_n)$ и $\varepsilon = \sqrt[q]{1}$. Тогда каждый корень q-й степени является корнем h_i-й степени. Действительно, $q = h_i l_i$ для некоторого l_i. Поэтому $\varepsilon^{q} = (\varepsilon^{l_i})^{h_i}$. Кроме того, поскольку каждый корень из 1 степени q можно представить в виде произведения $\varepsilon_1\varepsilon_2 \ldots \varepsilon_n$, достаточно требовать существования корня q-й степени. Если он существует, то существуют корни $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n$ и можно проводить гармонический анализ функций из $L(H, F)$.

Пример 3.1. Пусть $H = H_2 \times H_3 \times H_4$. Тогда $q = \text{НОК}(2, 3, 4) = 12$. Если $\sqrt[12]{1} \in F$, то существуют и корни 2-й, 3-й и 4-й степени.

Упражнение 3.1. Принять $F = \text{GF}(13)$ (см. пример 3.1) и $\sqrt[12]{1} = 2 \in \text{GF}(13)$. Проверить, что существуют корни 2-й, 3-й и 4-й степени. Найти их.

2. χ-Функции, обобщенные функции Радемахера и Хаара

Естественной областью определения характеров является абелева группа. Желательно иметь функции со свойствами характеров, определенные на конечном отрезке или вещественной, или целочисленной оси. Для этого, очевидно, необходимо каким-либо способом вложить абелеву группу в этот отрезок. Осуществим это вложение следующим образом. Каждому элементу $x = (x_1, x_2, \ldots, x_n)$ группы $H = H_1 \times H_2 \times \ldots \times H_n$ можно поставить в соответствие n-разрядное число x^*. Без ограничения общности x_n можно считать младшим, а x_1 — старшим разрядами числа x^* в системе счисления со смешанными основаниями $\langle h_1, h_2, \ldots, h_n\rangle$. Тем самым устанавливается следующее взаимооднозначное соответствие между элементами группы и целыми числами отрезка $\Omega = [0, h-1]$:

$$x \to x^* = x_n + x_{n-1}h_n + x_{n-2}h_nh_{n-1} + \cdots + x_1h_nh_{n-1}\ldots h_2 = \\ = x_n + \sum_{i=1}^{n-1} x_ih_nh_{n-1}\ldots h_{i+1}. \qquad (3.11)$$

С учетом введенного соответствия каждый характер может быть представлен решетчатой функцией $\chi_\alpha(x^*)$, определенной в точках $0, 1, \ldots, h-1$ отрезка $\Omega = [0, h-1]$.

Группу H^* также отобразим в отрезок $\Omega^* = [0, h-1]$. При этом каждый мультииндекс α отобразится в целое число:

$$\alpha \to \alpha^* = \alpha_n + \sum_{i=1}^{n-1} \alpha_ih_nh_{n-1}\ldots h_{i+1}. \qquad (3.12)$$

Определение 3.1. Характеры $\chi_\alpha(x)$, определенные на конечном отрезке, назовем χ-функциями.

Пример 3.2. Пусть $H = H_2 + H_2 + H_2$. Тогда элементы этой группы отобразятся в отрезок $[0,7]$ следующим образом:

$$(0,0,0) \mapsto 0;\quad (0,0,1) \mapsto 1;\quad (0,1,0) \mapsto (0,1,1) \mapsto 3;$$
$$(1,0,0) \mapsto 4;\quad (1,0,1) \mapsto 5;\quad (1,1,0) \mapsto (1,1,1) \mapsto 7.$$

При этом характеры группы H переходят в функции Уолша:

$$\chi_0(x): 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1\ \ 1;$$
$$\chi_1(x): 1\ -1\ \ 1\ -1\ \ 1\ -1\ \ 1\ -1;$$
$$\chi_2(x): 1\ \ 1\ -1\ -1\ \ 1\ \ 1\ -1\ -1;$$
$$\chi_3(x): 1\ -1\ -1\ \ 1\ \ 1\ -1\ -1\ \ 1;$$
$$\chi_4(x): 1\ \ 1\ \ 1\ \ 1\ -1\ -1\ -1\ -1;$$
$$\chi_5(x): 1\ -1\ \ 1\ -1\ -1\ \ 1\ -1\ \ 1;$$
$$\chi_6(x): 1\ \ 1\ -1\ -1\ -1\ -1\ \ 1\ \ 1;$$
$$\chi_7(x): 1\ -1\ -1\ \ 1\ -1\ \ 1\ \ 1\ -1.$$

Пример 3.3. Пусть $H = H_2 \dotplus H_3$. Элементы этой группы отобразятся в отрезок [0, 5] следующим образом:

$$(0, 0) \mapsto 0; \quad (0, 1) \mapsto 1; \quad (0, 2) \mapsto 2;$$
$$(1, 0) \mapsto 3; \quad (1, 1) \mapsto 4; \quad (1, 2) \mapsto 5.$$

Аналогичное отображение имеет место и для группы $H^* = H_2^* + H_3^*$. При этом χ-функции группы $H_2 + H_3$ на отрезке [0, 5] будут иметь следующий вид:

$$\chi_0(x): 1\ 1\ 1\ 1\ 1\ 1; \quad \chi_3(x): 1\ 1\ 1\ -1\ -1\ -1;$$
$$\chi_1(x): 1\ \varepsilon\ \varepsilon^2\ 1\ \varepsilon\ \varepsilon^2; \quad \chi_4(x): 1\ \varepsilon\ \varepsilon^2\ -1\ -\varepsilon\ -\varepsilon^2;$$
$$\chi_2(x): 1\ \varepsilon^2\ \varepsilon\ 1\ \varepsilon^2\ \varepsilon; \quad \chi_5(x): 1\ \varepsilon^2\ \varepsilon\ -1\ -\varepsilon^2\ -\varepsilon.$$

Очень часто будут использоваться характеры, определенные на отрезке $[0, h]$ или $[0, 1]$ вещественной оси. Поэтому доопределим характеры $\chi_\alpha(x)$ до кусочно-постоянных функций

$$\chi_\alpha(x) = \chi_\alpha(x^*), \quad x \in [x^*, x^* + 1], \quad x \in \boldsymbol{R}, \ x^* \in \boldsymbol{Z}.$$

В дальнейшем под переменной x будем подразумевать $x \in H$ или $x \in [0, h] \subset \boldsymbol{R}$, или $x \in [0, h-1] \subset \boldsymbol{Z}$, а из текста будет ясно, о каком случае идет речь.

Про χ-функции будем говорить, что они типа HF. Многообразие базисов χ-функций определяется многообразием групп H и полей F. В дальнейшем область значений, которые могут принимать характеры, можно расширить до колец K более сложной природы. Таким образом, можно классифицировать базисы, составленные из характеров конечных абелевых групп, по типу группы H и типу кольца K.

Такие широко известные базисы, как базис Уолша (базис типа $(H_2 \dotplus H_2 \dotplus \ldots \dotplus H_2)$, C)

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = (-1)^{\sum_{i=1}^{n} \alpha_i x_i};$$

базис Крестенсона (базис типа $(H_p + H_p + \ldots + H_p)$, C)

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \exp\left(i \frac{2\pi}{p} \sum_{i=1}^{n} \alpha_i x_i\right);$$

базис Фурье (базис типа H_N, C)

$$\chi_\alpha(x) = \exp\left(i \frac{2\pi}{N} \alpha x\right);$$

базис Рейдера (базис типа H_{2^n}, GF (q))

$$\chi_\alpha(x) = 2^{\alpha x}, \ 2 = \sqrt[2^n]{1} \in \mathrm{GF}(q);$$

базис Виленкина — Крестенсона (базис типа $(H_m + H_m + \ldots + H_m)$, C, где m — произвольное целое число)

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \exp\left(i \frac{2\pi}{m} \sum_{i=1}^{n} \alpha_i x_i\right);$$

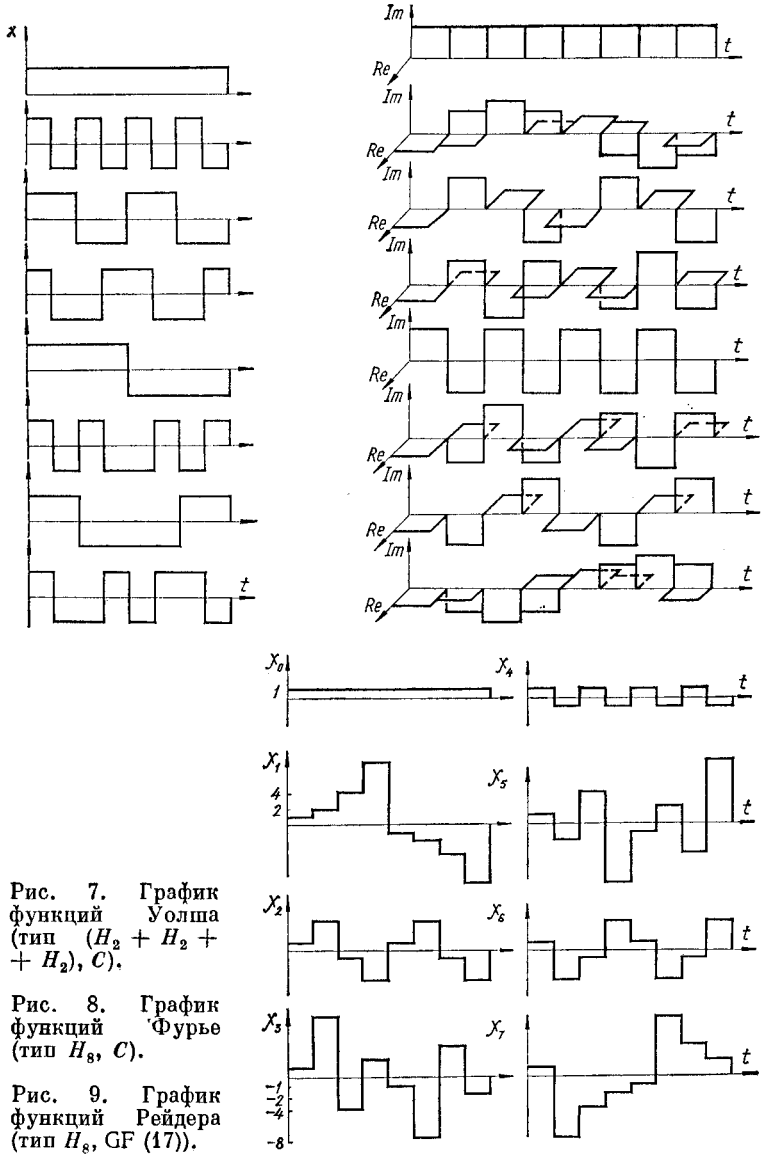


Рис. 7. График функций Уолша (тип $(H_2 + H_2 + H_2), C$).

Рис. 8. График функций Фурье (тип H_8, C).

Рис. 9. График функций Рейдера (тип H_8, GF (17)).

базис Понтрягина — Виленкина — Крестенсона (базис типа $(H_{h_1} \dotplus H_{h_2} \dotplus \ldots \dotplus H_{h_n})$, где $h_1, h_2, \ldots, h_n$ — произвольные целые числа)

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \varepsilon^{\alpha_1 x_1}\varepsilon^{\alpha_2 x_2} \ldots \varepsilon_n^{\alpha_n x_n}$$

и т. д., являются частными случаями базисов χ-функций типа *НК* (рис. 7—11).

Переход к полуинтервалу [0, 1] тривиален:

$$x = \frac{1}{h}\left[x_n + \sum_{i=1}^{n-1} x_i h_n h_{n-1} \ldots h_{i+1}\right].$$

Рассмотрим еще одну форму представления χ-функций. Для этого введем функции $R_i(x) = \varepsilon_i^{x_i}$, которые назовем обобщенными функциями Радемахера. Они являются частным случаем характеров и совпадают с теми из них, номера α которых в системе со смешанными основаниями содержат один ненулевой и один равный единице разряд. Действительно, при $\alpha_i = 1$, $\alpha_j = 0$, $i \neq j$, получаем

$$\chi_{0\ldots\alpha_i\ldots 0}(x) = R_i(x) = \varepsilon_i^{x_i}.$$

Таким образом, характеры, а значит, и χ-функции можно представить в виде произведения степеней n обобщенных функций Радемахера:

$$\chi_\alpha(x) = \chi_{\alpha_1\alpha_2\ldots\alpha_n}(x_1, x_2, \ldots, x_n) = \prod_{i=1}^{n} [R_i(x_i)]^{\alpha_i}.$$

Если переменная x пробегает значения 0, 1, 2, ..., $h-1$, то любой ее разряд изменяется периодически в пределах от 0 до $h_i - 1$ с периодом $h_n h_{n-1} \ldots h_{n-i}$. Отсюда следует, что функция Радемахера $R_i(x)$ — это периодическая функция, у которой на интервале h

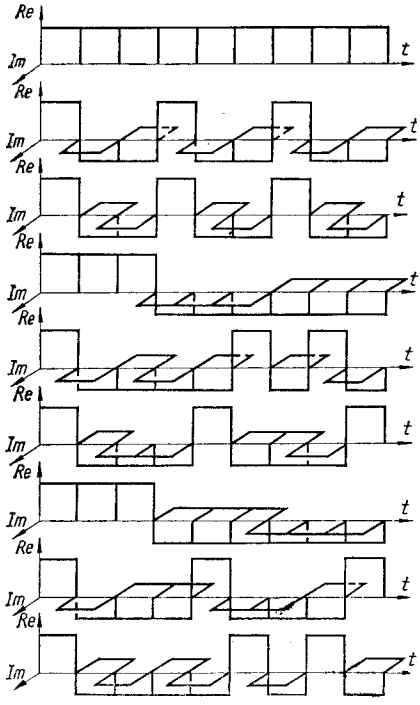


Рис. 10. График функций Крестенсона (тип $(H_3 + H_3)$, C).

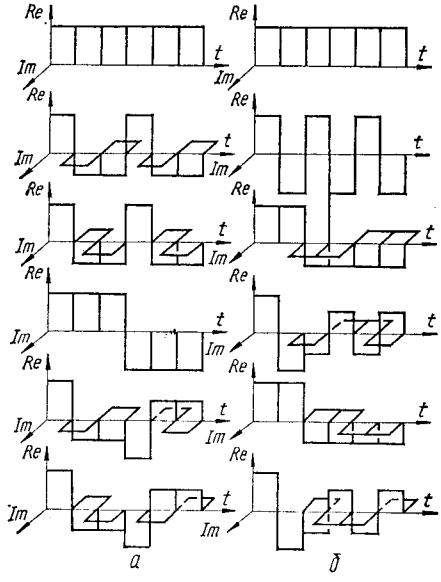


Рис. 11. График функций Понтрягина — Виленкина — Крестенсона типа $(H_2 + H_3)$, C (*а*) и типа $(H_3 + H_2)$, C (*б*).

укладывается $\prod_{m=1}^{i} h_m$ периодов. При $h_1 = h_2 = \ldots = h_n = 2$ обобщенная функция Радемахера является действительной функцией и совпадает с функцией Радемахера — Уолша.

В дальнейшем будут часто использоваться матричные представления системы Х-функций. Поскольку любая система Х-функций состоит из характеров и определена в h точках, она может быть представлена матрицей размера $h \times h$. Эту матрицу обозначим через H_h, где индекс h указывает порядок матрицы. Чередование функций $\chi_\alpha(x)$ в системе или расположение строк в матрице H_h может быть, вообще говоря, различным. Один из возможных способов упорядочения строк в матрице H_h определяется отображением (3.12).

Пример 3.4. Матрица H_6 для Х-функций группы $H_2 \times H_3$ имеет вид

$$H_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 & 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon & 1 & \varepsilon^2 & \varepsilon \\ 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \varepsilon & \varepsilon^2 & -1 & -\varepsilon & -\varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon & -1 & -\varepsilon^2 & -\varepsilon \end{bmatrix}. \tag{3.13}$$

Такая же матрица для Х-функций группы H_6:

$$H_6 = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 & \varepsilon^3 & \varepsilon^4 & \varepsilon^5 \\ 1 & \varepsilon^2 & \varepsilon^4 & 1 & \varepsilon^2 & \varepsilon^4 \\ 1 & \varepsilon^3 & 1 & \varepsilon^3 & 1 & \varepsilon^3 \\ 1 & \varepsilon^4 & \varepsilon^2 & 1 & \varepsilon^4 & \varepsilon^2 \\ 1 & \varepsilon^5 & \varepsilon^4 & \varepsilon^3 & \varepsilon^2 & \varepsilon \end{bmatrix}. \tag{3.14}$$

Очевидно, что теория характеров конечных абелевых групп имеет непосредственное приложение в ЦОС. Действительно, в области определения E_N цифрового сигнала $x(n)$ можно рассматривать абелеву группу H, равную прямому произведению своих подгрупп: $H = H_1 \times H_2 \times \ldots \times H_n$. Группа H — циклическая группа порядка $[H : 1] = N = q_1 q_2 \ldots q_n$, где $q_i = p_i^{\alpha_i}$ — порядок подгруппы H_i; p_i — простые числа, не обязательно все разные; $r_i = 0, 1, 2, \ldots$; $i = 1, 2, \ldots, n$. Любой элемент $n \in H$ имеет вид $n = (n_1, n_2, \ldots, n_m)$, $n_i \in H_i$. Групповая операция определяется выражением (3.2). Значения сигнал $x(n)$ принимает в некотором кольце K. Задавая вид группы H и кольцо K, в котором может принимать значение цифровой сигнал $x(n)$, мы тем самым задаем вид базиса, состоящего из характеров группы H.

Пример 3.5. Пусть $N = 6$. В области определения цифрового сигнала $x(n)$ будем рассматривать абелеву группу H порядка $[H : 1] = 6$. В качестве групповой операции выступает операция сложения по модулю 6. Выражение для характеров имеет вид

$$\chi_\alpha(n) = \varepsilon\alpha_n \pmod 6. \tag{3.15}$$

Матрица характеров задается выражением (3.14). В данном случае $0 \leqslant \alpha \leqslant 5$, $0 \leqslant n \leqslant 5$. Если $\varepsilon \in C$, то получаем систему дискретных экспоненциальных функций, приведенную в табл. 23, $\varepsilon = e^{i\frac{\pi}{3}\alpha_n}$. Пусть теперь $\varepsilon \in \mathrm{GF}(p)$. Значение p выбирается исходя из условия $q \mid (p-1)$, где $q = 6$ — показатель группы H. Наименьший порядок поля Галуа GF (p), над которым можно определить систему характеров группы H, равен 7, т. е. $p = 7$. В качестве первообразного элемента ε выбирается первообразный корень из единицы, принадлежащий полю GF (7). Нетрудно убедиться, что таким корнем является элемент поля GF (7), равный 3. Результаты построения системы характеров приведены в табл. 24.

Пример 3.6. Возьмем, как и в предыдущем примере, $N = 6$, но в области определения сигнала будем рассматривать абелеву группу H, равную прямому произведению своих подгрупп H_2 и H_3 : $H = H_2 \times H_3$, $[H_2 : 1] = 2$, $[H_3 : 1] = 3$. Система характеров в этом случае определяется выражением

$$\chi_{\alpha_1\alpha_2}(n_1, n_2) = \varepsilon_1^{\alpha_1 n_1}\varepsilon_2^{\alpha_2 n_2}, \tag{3.16}$$

где $0 \leqslant \alpha_1 \leqslant 1$, $0 \leqslant n_1 \leqslant 1$; $0 \leqslant \alpha_2 \leqslant 2$, $0 \leqslant n_2 \leqslant 2$.

Если $\varepsilon_1, \varepsilon_2 \in C$, то получаем систему функций Виленкина — Крестенсона. Результаты построений согласно (3.16) сведены в табл. 25 и 26, в которых $\varepsilon_1 = e^{i\pi\alpha_1 n}$, $\varepsilon_2 = e^{i\frac{2\pi}{3}\alpha_2 n_2}$. Пусть теперь $\varepsilon_1, \varepsilon_2 \in \mathrm{GF}(p)$. Тогда $q = \text{НОК}(2, 3) = 6$. Значит, условия выбора порядка поля Галуа те же, что и в примере 3.5. Система характеров группы $H_6 = H_2 \times H_3$, определенных над полем GF (7), приведена в табл. 27 ($\varepsilon_1 = 6$, $\varepsilon_2 = 2$).

Упражнение 3.2. Построить систему характеров группы H, рассматриваемой в области определения цифрового сигнала $x(n)$ на интервале $N = 6$, причем $H = H_3 \times H_2$. Построить характеры над полем C и GF (p).

Произвольную решетчатую функцию, принимающую значения в поле F и определенную на конечном интервале $[0, h-1]$, можно разложить в ряд

$$f(x) = \sum_{\alpha=0}^{h-1} S(\alpha)\chi_\alpha(x) = HS(\alpha), \tag{3.17}$$

где

$$S(\alpha) = \frac{1}{h}\sum_{x=0}^{h-1} f(x)\chi_\alpha^{-1}(x) = H^{-1}f(x). \tag{3.18}$$

Таблица 23. Дискретные экспоненциальные функции при $N = 6$

α	n					
	0	1	2	3	4	5
0	1	1	1	1	1	1
1	1	$e^{i\frac{\pi}{3}}$	$e^{i\frac{2\pi}{3}}$	-1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{5}{3}\pi}$
2	1	$e^{i\frac{2\pi}{3}}$	$e^{i\frac{4}{3}\pi}$	1	$e^{i\frac{2\pi}{3}}$	$e^{i\frac{4}{3}\pi}$
3	1	-1	1	-1	1	-1
4	1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{2}{3}\pi}$	1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{2}{3}\pi}$
5	1	$e^{i\frac{5}{3}\pi}$	$e^{i\frac{4}{3}\pi}$	-1	$e^{i\frac{2}{3}\pi}$	$e^{i\frac{\pi}{3}}$

Таблица 24. Система характеров группы G порядка 6 над полем $GF(7)$

α	n					
	0	1	2	3	4	5
0	1	1	1	1	1	1
1	1	3	2	6	4	5
2	1	2	4	1	2	4
3	1	6	1	6	1	6
4	1	4	2	1	4	2
5	1	5	4	6	2	3

Таблица 25. Система характеров группы G порядка 6 и структуры $2 \cdot 3$

α_1	α_2	$n_1 = 0$			$n_1 = 1$		
		n_2			n_2		
		0	1	2	0	1	2
0	0	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$
	1	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^1$	$\varepsilon_1^0\varepsilon_2^2$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^1$	$\varepsilon_1^0\varepsilon_2^1$
	2	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^2$	$\varepsilon_1^0\varepsilon_2^1$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^2$	$\varepsilon_1^0\varepsilon_2^1$
1	0	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^1\varepsilon_2^0$	$\varepsilon_1^1\varepsilon_2^0$	$\varepsilon_1^1\varepsilon_2^0$
	1	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^1$	$\varepsilon_1^0\varepsilon_2^2$	$\varepsilon_1^1\varepsilon_2^0$	$\varepsilon_1^1\varepsilon_2^1$	$\varepsilon_1^1\varepsilon_2^2$
	2	$\varepsilon_1^0\varepsilon_2^0$	$\varepsilon_1^0\varepsilon_2^2$	$\varepsilon_1^0\varepsilon_2^1$	$\varepsilon_1^1\varepsilon_2^0$	$\varepsilon_1^1\varepsilon_2^2$	$\varepsilon_1^1\varepsilon_2^1$

Таблица 26. **Система базисных функций Виленкина — Крестенсона при $N = 6$ и структуре группы $2 \cdot 3$**

α_1	α_2	$n_1 = 0$			$n_1 = 1$		
		n_2			n_2		
		0	1	2	0	1	
0	0	1	1	1	1	1	1
	1	1	$e^{i\frac{2}{3}\pi}$	$e^{i\frac{4}{3}\pi}$	1	$e^{i\frac{2}{3}\pi}$	$e^{i\frac{4}{3}\pi}$
	2	1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{2}{3}\pi}$	1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{2}{3}\pi}$
1	0	1	1	1	−1	−1	−1
	1	1	$e^{i\frac{2}{3}\pi}$	$e^{i\frac{4}{3}\pi}$	−1	$e^{i\frac{5}{3}\pi}$	$e^{i\frac{\pi}{3}}$
	2	1	$e^{i\frac{4}{3}\pi}$	$e^{i\frac{2}{3}\pi}$	−1	$e^{i\frac{\pi}{3}}$	$e^{i\frac{5}{3}\pi}$

Таблица 27. **Система характеров группы G порядка 6 и структуры $2 \cdot 3$ над полем GF (7)**

α_1	α_2	$n_1 = 0$			$n_1 = 1$		
		n_2			n_2		
		0	1	2	0	1	2
0	0	1	1	1	1	1	1
	1	1	2	4	1	2	4
	2	1	4	2	1	4	2
1	0	1	1	1	6	6	6
	1	1	2	4	6	5	3
	2	1	4	2	6	3	5

Пару этих преобразований назовем соответственно обратным и прямым дискретным Х-преобразованиями. Функцию $S(\alpha)$ назовем Х-спектром (или Х-изображением) функции $f(x)$. Условно этот факт будем изображать следующим образом: $S(\alpha) \div f(x)$.

Каждый из коэффициентов $S(\alpha)$ разложения (3.17) учитывает поведение функции во всех точках ее задания. Однако в ряде случаев оказывается более удобным в качестве базисов применять такие системы функций, для которых коэффициенты разложения учитывают поведение исходной функции лишь в нескольких близко расположенных точках. Такого рода системами функций являются, например, функции Хаара — Уолша и Хаара — Крестенсона [88,

155]. Естественным обобщением этих функций являются χ-функции Хаара, которые можно построить, используя определение χ-функции Радемахера, следующим образом:

$$K_{0,0}^{0} = 1; \quad K_{\alpha_i,i}^{q_i}(x) = \begin{cases} R_i^{\alpha_i}(x) = \chi_{0\ldots\alpha_i\ldots0}(x), \\ x \in [(g_i - 1)\, h_n \ldots h_{n-i}, \\ \qquad g_i h_n \ldots h_{n-i}]; \\ 0 \text{ в остальных случаях,} \end{cases}$$

где $g_i = 1, 2, \ldots, h_0, h_1, \ldots, h_{i-1}$; $g_0 = 1$; $\alpha_i = 1,2, \ldots, h_{i-1}$, $i = 0, 1, \ldots, n-1$.

χ-Функции Хаара при $h_i = 2$ совпадают с функциями Хаара — Уолша, а при $h_i = p$, $i = 1, 2, \ldots, n-1$ (где p — простое) — с функциями Хаара — Крестенсона. Здесь для удобства нумерации χ-функций Хаара принята нумерация разрядов от 0 до $n-1$, а не от 1 до n (рис. 12).

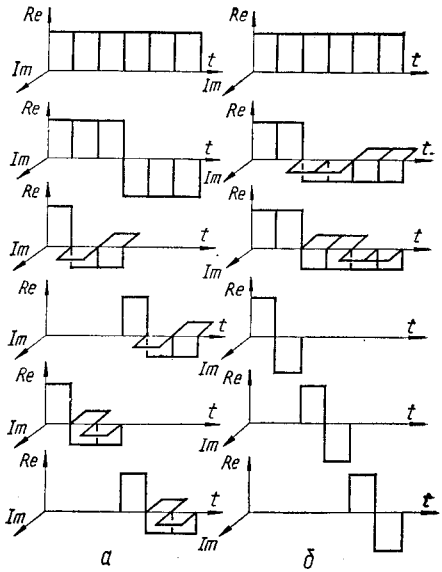


Рис. 12. Графическое изображение χ-функции Хаара для групп $H_6 = H_2 \dotplus H_3$ (*а*) и $H_6 = H_3 \dotplus H_2$ (*б*).

Из определения χ-функций Хаара немедленно следует, во-первых, их ортогональность

$$\sum_{x=0}^{h-1} K_{\alpha_i,i}^{g_i}(x)\, K_{\alpha_j,j}^{g_i}(x) = \begin{cases} h_0 h_1 \ldots h_{i-1}, \ \alpha_i = \alpha_j, \quad i \neq j; \ g_i = g_j; \\ 0 \text{ в остальных случаях;} \end{cases}$$

во-вторых, тот факт, что число χ-функций Хаара равно h. Таким образом, эти функции образуют полный ортонормированный базис в пространстве $L(H, F)$. Однако в отличие от χ-функций χ-функции Хаара не замкнуты относительно умножения, т. е. не обладают свойством мультипликативности.

3. Основные свойства и быстрые алгоритмы χ-преобразований

Отметим важнейшие свойства χ-преобразований, так как спектры по этим преобразованиям широко применяются при анализе и синтезе линейных систем. Рассматриваемые свойства будут использоваться в дальнейшем.

Теорема 3.2 (теорема линейности). Пусть $f(x) = \sum_{k=1}^{n} C_k f_k(x)$.

Тогда $S(\alpha) = \sum_{k=1}^{n} S_k(\alpha)$.

Теорема 3.3. Для сдвинутых оригинала $f(x \ominus s)$ и изображения $S(\alpha \ominus \omega)$ имеют место равенства

$$S_{f(x\ominus s)}(\alpha) = \overline{\chi}_\alpha(s) S_{f(x)}(\alpha); \quad S_{f(x)}(\alpha \ominus \omega) = S_{f(x)\overline{\chi}_\omega(x)}(\alpha).$$

Доказательство

$$S_{f(x\ominus s)}(\alpha) = h^{-1} \sum_x f(x \ominus s) \overline{\chi}_\alpha(x) = h^{-1} \sum_y f(x) \overline{\chi}_\alpha(y \ominus s) =$$

$$= \overline{\chi}_\alpha(s) S_{f(x)}(\alpha);$$

$$S_{f(x)}(\alpha \ominus \omega) = \sum_x f(x) \chi_{\alpha\ominus\omega}(x) = \sum_x [f(x) \overline{\chi}_\omega(x)] \chi_\alpha(x) = S_{f(x)\overline{\chi}_\omega(x)}(\alpha).$$

Определение 3.2. Разностью функции $f(x)$ в направлении a называется функция

$$\Delta_a f(x) = f(x \oplus a) - f(x).$$

Теорема 3.4. Разность функции $f(x)$ имеет изображение

$$S_\Delta(\alpha) = [\chi_\alpha(a) - 1] S_f(\alpha).$$

Доказательство

$$S_\Delta(\alpha) = h^{-1} \sum_x [f(x \oplus a) - f(x)] \chi_\alpha(x) = \chi_\alpha(a) S_f(\alpha) - S_f(\alpha) =$$

$$= [\chi_\alpha(a) - 1] S_f(\alpha).$$

Разности более высокого порядка определяются следующим образом:

$$\Delta^h_{a_1 a_2 \ldots a_n} = \Delta_{a_n} \Delta_{a_{n-1}} (\ldots (\Delta_{a_1} f(x)) \ldots).$$

Нетрудно видеть, что

$$S_{\Delta^n}(\alpha) = \left\{ \prod_{i=1}^n [\chi_\alpha(a_i) - 1] \right\} S_f(\alpha),$$

и если $a_1 = a_2 = \ldots = a_n$, то $S_{\Delta^n}(\alpha) = [\chi(\alpha) - 1]^n S_f(\alpha)$.

Определение 3.3. Если $f_1(x), f_2(x) \in L(H, \mathrm{K})$, то функция

$$\delta_{1,2}(\tau) = h^{-1} \sum_x f_1(x) \bar{f}_2(x \ominus \tau)$$

называется *НК*-взаимной корреляционной функцией (или просто *НК*-ВКФ) сигналов $f_1(x)$ и $f_2(x)$. Если $f_1(x) = f_2(x)$, то $b(\tau)$ является *НК*-автокорреляционной функцией сигнала $f(x)$ (*НК*-АКФ).

Теорема 3.5. χ-Преобразование переводит *НК*-ВКФ в произведение спектров $S_{1,2}(\alpha) = S_1(\alpha) \overline{S}_2(\alpha)$.

Доказательство

$$S_{1,2}(\alpha) = h^{-1} \sum_\tau b_{1,2}(\tau) \overline{\chi}_\alpha(\tau) = h^{-1} \sum_\tau h^{-1} \sum_x f_1(x) f_2(x \ominus \tau) \times \overline{\chi}_\alpha(x) \times$$

$$\times \chi_\alpha(x) = h^{-1} \sum_x f_1(x) \overline{\chi}_\alpha(x) h^{-1} \overline{\sum_\tau f_2(x \ominus \tau) \chi_\alpha(x - \tau)} = S_1(\alpha) \overline{S}_2(\alpha).$$

Для *НК*-АКФ будем иметь $b(\tau) \div |S(\alpha)|^2 = G(\alpha)$.

Определение 3.4. Если $f(x)$, $h(x) \in L(H, K)$, то функция

$$y(x) = h^{-1} \sum_{\tau} h(x - \tau) f(\tau)$$

называется HK-сверткой сигналов $h(x)$, $f(x)$.

Теорема 3.6. χ-Преобразование переводит HK-свертку в произведение спектров $S_y(\alpha) = S_h(\alpha) S_f(\alpha)$.

Доказательство аналогично доказательству теоремы 3.4.

Отметим, что функцию $G(\alpha) = |S(\alpha)|^2$ по аналогии с преобразованием Фурье естественно назвать HK-энергетическим спектром. Очевидно, $b(\tau)$ и $G(\alpha)$ связаны парой χ-преобразований

$$G(\alpha) = h^{-1} \sum_{\tau} b(\tau) \overline{\chi}_{\alpha}(\tau); \quad b(\tau) = \sum_{\alpha} G(\alpha) \chi_{\alpha}(\tau),$$

которые следует трактовать как теорему Винера — Хинчина в χ-базисе.

Теорема 3.7. Энергетический спектр инвариантен относительно H-сдвигов.

Доказательство

$$S_{f(x \ominus \tau)}(\alpha) = \overline{\chi}_{\alpha}(\tau) S_{f(x)}(\alpha), \; G_{f(x-\tau)}(\alpha) =$$

$$= \overline{\chi}_{\alpha}(\tau) S_{f(x)}(\alpha) \chi_{\alpha}(\tau) \overline{S_{f(x)}(\alpha)} = S_{f(x)}(\alpha) S_{f(x)}(\alpha) = G_{f(x)}(\alpha).$$

Эта теорема является естественным обобщением аналогичной теоремы для обычных сдвигов и базиса Фурье.

χ-Преобразование является обобщением обширного класса ортогональных преобразований, которые используются при анализе и синтезе сигналов и систем. Построение алгоритмов эффективного вычисления таких преобразований — определенная проблема. Вычисление непосредственно по выражениям (3.17) и (3.18) требует выполнения значительного числа операций умножения и сложения в поле F, которое пропорционально квадрату числа, представляющего размер матрицы преобразований. Лучшие оценки получаются при использовании так называемых быстрых алгоритмов, которые существуют для многих частных случаев χ-преобразований. Однако даже в этом случае объем вычислений является препятствием для эффективного решения многих задач. Особенно задач, при решении которых необходимо вычисление многомерных χ-преобразований. Например, задачи цифровой обработки многозональных изображений [103]. Поэтому делаются попытки дальнейшего уменьшения объема вычислений при реализации ортогональных преобразований. Например, χ-преобразования могут заменяться упрощенными преобразованиями со сходными свойствами [73, 90].

Кроме того, как отмечалось в первой главе, объем вычислений зависит от поля, над которым определяются χ-преобразования. С этой точки зрения привлекательными являются преобразования, определенные над конечным полем или над конечным кольцом. Такой подход позволяет добиться дальнейшего уменьшения объема вычислений, в то время как для некоторых видов χ-преобразований (в

частности, для преобразования Фурье) получены предельные оценки [45, 46, 57, 77, 78], показывающие, что возможности уменьшения объема вычислений построением быстрых алгоритмов исчерпаны.

Предпримем попытку получить быстрые алгоритмы в общем случае для χ-преобразований. С этой целью каждому выражению $\chi_{\alpha_i}(x_i)$ поставим в соответствие матрицу $\hat{H}_{h_i} = [\varepsilon^{\alpha_i x_i}]$ порядка h_i. Тогда выражению $\chi_\alpha(x) = \chi_{\alpha,\ldots,\alpha_n}(x_1, \ldots, x_n)$ будет соответствовать матрица $\hat{H}_h$ порядка h, получающаяся как результат тензорного (прямого) произведения матриц $\hat{H}_{h_i}$

$$\hat{H}_h = \hat{H}_{h_1} \otimes \hat{H}_{h_2} \otimes \cdots \otimes \hat{H}_{h_n}.$$

Например, пусть $\hat{H}_6 = \hat{H}_2 + \hat{H}_3$ и

$$\hat{H}_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}; \quad \hat{H}_3 = \begin{bmatrix} 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon \end{bmatrix}, \quad \varepsilon = \sqrt[3]{1}.$$

Тогда

$$\hat{H}_6 = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \varepsilon & \varepsilon^2 & 1 & \varepsilon & \varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon & 1 & \varepsilon^2 & \varepsilon \\ \hline 1 & 1 & 1 & -1 & -1 & -1 \\ 1 & \varepsilon & \varepsilon^2 & -1 & -\varepsilon & -\varepsilon^2 \\ 1 & \varepsilon^2 & \varepsilon & -1 & -\varepsilon^2 & -\varepsilon \end{array}\right].$$

Для факторизации матрицы $\hat{H}_h$ воспользуемся следующим свойством тензорного произведения:

$$A_1 A_2 \otimes B_1 B_2 = (A_1 \otimes B_1)(A_2 \otimes B_2),$$

где операторы с одинаковыми индексами действуют в одном общем для них пространстве. Тогда можно записать

$$\hat{H}_h = (\hat{H}_{h_1} \otimes I_{h_2} \otimes \cdots \otimes I_{h_n})(I_{h_1} \otimes \hat{H}_{h_2} \otimes \cdots \otimes I_{h_n}) \cdots \otimes$$

$$\otimes (I_{h_1} \otimes I_{h_2} \otimes \cdots \otimes \hat{H}_{h_n}) = \prod_{i=1}^{n} T_i, \qquad (3.19)$$

где $T_i = I_{h_1} \otimes I_{h_2} \otimes \cdots \otimes \hat{H}_{h_i} \otimes \cdots \otimes I_{h_n}$.

Например, если $H_8 = H_2 + H_2 + H_2$, то

$$\hat{H}_8 = (I_2 \otimes I_2 \otimes \hat{H}_2)(I_2 \otimes \hat{H}_2 \otimes I_2)(\hat{H}_2 \otimes I_2 \otimes I_2) = T_3 T_2 T_1,$$

где

$$T_3 = \left[\begin{array}{cc|cc|cc|cc} 1 & 1 & & & & & & \\ 1 & -1 & & & & & & \\ \hline & & 1 & 1 & & & & \\ & & 1 & -1 & & & & \\ \hline & & & & 1 & 1 & & \\ & & & & 1 & -1 & & \\ \hline & & & & & & 1 & 1 \\ & & & & & & 1 & -1 \end{array}\right]; \quad T_2 = \left[\begin{array}{cc|cc|cc|cc} 1 & 1 & & & & & & \\ & & 1 & 1 & & & & \\ 1 & -1 & & & & & & \\ & & 1 & -1 & & & & \\ \hline & & & & 1 & 1 & & \\ & & & & & & 1 & 1 \\ & & & & 1 & -1 & & \\ & & & & & & 1 & -1 \end{array}\right]; \quad T_1 = \left[\begin{array}{cc|cc|cc|cc} 1 & & & & 1 & & & \\ & 1 & & & & 1 & & \\ & & 1 & & & & 1 & \\ & & & 1 & & & & 1 \\ \hline 1 & & & & -1 & & & \\ & 1 & & & & -1 & & \\ & & 1 & & & & -1 & \\ & & & 1 & & & & -1 \end{array}\right].$$

Если $H_6 = H_2 + H_3$, то $\hat{H}_6 = (I_2 \otimes \hat{H}_3)(\hat{H}_2 \otimes I_3)$, где

$$T_2 = \left[\begin{array}{ccc|ccc} 1 & 1 & 1 & & & \\ 1 & \varepsilon & \varepsilon^2 & & & \\ 1 & \varepsilon^2 & \varepsilon & & & \\ \hline & & & 1 & 1 & 1 \\ & & & 1 & \varepsilon & \varepsilon^2 \\ & & & 1 & \varepsilon^2 & \varepsilon \end{array}\right]; \quad T_1 = \left[\begin{array}{ccc|ccc} 1 & & & 1 & & \\ & 1 & & & 1 & \\ & & 1 & & & 1 \\ \hline 1 & & & -1 & & \\ & 1 & & & -1 & \\ & & 1 & & & -1 \end{array}\right].$$

Если $H_9 = H_3 + H_3$, то $\hat{H}_9 = (I_3 \otimes \hat{H}_3)(\hat{H}_3 \otimes I_3) = T_2 T_1$, где

$$T_2 = \left[\begin{array}{ccc|ccc|ccc} 1 & 1 & 1 & & & & & & \\ 1 & \varepsilon & \varepsilon^2 & & & & & & \\ 1 & \varepsilon^2 & \varepsilon & & & & & & \\ \hline & & & 1 & 1 & 1 & & & \\ & & & 1 & \varepsilon & \varepsilon^2 & & & \\ & & & 1 & \varepsilon^2 & \varepsilon & & & \\ \hline & & & & & & 1 & 1 & 1 \\ & & & & & & 1 & \varepsilon & \varepsilon^2 \\ & & & & & & 1 & \varepsilon^2 & \varepsilon \end{array}\right]; \quad T_1 = \left[\begin{array}{ccc|ccc|ccc} 1 & & & 1 & & & 1 & & \\ & 1 & & & 1 & & & 1 & \\ & & 1 & & & 1 & & & 1 \\ \hline 1 & & & \varepsilon & & & \varepsilon^2 & & \\ & 1 & & & \varepsilon & & & \varepsilon^2 & \\ & & 1 & & & \varepsilon & & & \varepsilon^2 \\ \hline 1 & & & \varepsilon^2 & & & \varepsilon & & \\ & 1 & & & \varepsilon^2 & & & \varepsilon & \\ & & 1 & & & \varepsilon^2 & & & \varepsilon \end{array}\right].$$

Выражение (3.19) представляет собой алгоритм быстрого χ-преобразования. Перепишем его в следующем виде:

$$\hat{H}_h = \prod_{i=1}^{n} (I_{h_1} \otimes I_{h_2} \otimes \cdots \otimes \hat{H}_{h_i} \otimes \cdots \otimes I_{h_n}) \qquad (3.20)$$

и подсчитаем количество арифметических операций, требующихся для вычисления спектра с использованием выражения (3.20).

Так как строка матрицы T_i содержит h_i ненулевых элементов, а в каждой матрице h строк, то для вычисления спектра с использованием быстрого алгоритма необходимо $4h \sum_{i=1}^{n} h^i$ операций умножения и сложения действительных чисел. При прямом вычислении спектра (без представления матрицы $\hat{H}_h$ в виде слабозаполненных матриц) эта величина равна $4h^2$. В результате получаем коэффициент

ускорения вычислений: КУВ $=4h^2 \Big/ 4h \sum_{i=1}^{n} h_i = \prod_{i=1}^{n} h_i \Big/ \sum_{i=1}^{n} h_i$.

При построении алгоритмов быстрого преобразования Фурье оказывается, что каждую матрицу $T_i = I_{h_1} \otimes \ldots \otimes \hat{H}_{h_i} \otimes \ldots \otimes I_{h_n}$ можно также факторизовать на произведение более слабозаполненных матриц, что позволит еще больше увеличить значение КУВ.

Наряду с факторизацией матрицы в форме (3.20) в ЦОС распространен метод Гуда [57]. Поясним его сначала на примере групп $H_2 + H_2 + \ldots + H_2$ и $H_m + H_m + \ldots + H_m$. Для этого введем матрицу P_2 «идеального» перемешивания, переставляющую отсчеты сигнала $x(n) = x_0x_1 \ldots x_{2^{n-1}-1}x_{2^{n-1}} \ldots x_{2^n-1}$ следующим образом:

$$P_2[x_0x_1 \ldots x_{2^{n-1}-1}x_{2^{n-1}}x_{2^{n-1}+1} \ldots x_{2^n-1}]' =$$

$$= [x_0x_{2^{n-1}}x_1x_{2^{n-1}+1} \ldots x_{2^{n-1}-1}x_{2^n-1}], \qquad (3.21)$$

где штрихом обозначена операция транспонирования.

Например, если $n = 3$, то

$$\begin{bmatrix} 1 & & & & & & & \\ & & 1 & & & & & \\ & 1 & & & & & & \\ & & & 1 & & & & \\ & & & & 1 & & & \\ & & 1 & & & & & \\ & & & & & 1 & & \\ & & & & & & & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} = \begin{bmatrix} x_0 \\ x_4 \\ x_1 \\ x_5 \\ x_2 \\ x_6 \\ x_3 \\ x_7 \end{bmatrix}.$$

По сути, P_2 — матричное представление перестановки

$$\pi = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 0 & 4 & 1 & 5 & 2 & 6 & 3 & 7 \end{pmatrix},$$

т. е. весь массив $x_0x_1 \ldots x_{2^{n-1}} \ldots x_{2^n-1}$ делится пополам на две части. Затем за первым элементом первой половины ставится первый элемент второй половины, после чего приставляется второй элемент первой половины, за которым немедленно следует второй элемент второй половины и т. д.:

$$x_0 \; \underset{\downarrow}{x_{2^{n-1}}} \; x_1 \; \underset{\downarrow}{x_{2^{n-1}+1}} \; x_2 \ldots x_{2^{n-1}-1} \; \underset{\downarrow}{x_{2^n-1}}.$$

Будем говорить о таком перемешивании как о двоичном.

В перестановке P_2 запишем все числа в двоичной форме:

$$\pi = \begin{pmatrix} (0\,0\,0) & (0\,0\,1) & (0\,1\,0) & (0\,1\,1) & (1\,0\,0) & (1\,0\,1) & (1\,1\,0) & (1\,1\,1) \\ (0\,0\,0) & (1\,0\,0) & (0\,0\,1) & (1\,0\,1) & (0\,1\,0) & (1\,1\,0) & (0\,1\,1) & (1\,1\,1) \end{pmatrix}, \qquad (3.22)$$

где $(s_1s_2s_3)$ — двоичное представление числа s.

Теперь нетрудно заметить, что двоичные числа в нижней строке перестановки π отличаются от двоичных чисел верхней строки тем, что разряды циклически переставлены на одну позицию $(s_1, s_2, s_3) \to (s_3, s_2, s_1)$. Этот результат верен и для общего случая. Действительно, рассмотрим ряд индексов в правой части равенства (3.21):

$$\underbrace{0,\ 0+2^{n-1}}, \underbrace{1,\ 1+2^{n-1}}, \ldots, \underbrace{2^{n-1}-1,\ 2^{n-1}-1+2^{n-1}}. \qquad (3.23)$$

Из (3.23) видно, что каждая пара отмеченных чисел в двоичной записи имеет одинаковые разряды, кроме первого, который равен нулю у левого члена пары и единице у правого: $(0, s_1, s_2, \ldots, s_{n-1})$, $(1, s_1, s_2, \ldots, s_{n-1})$, т. е. двоичное представление чисел ряда (3.23) имеет вид

$$(s_n, s_1, s_2, \ldots, s_{n-1}).$$

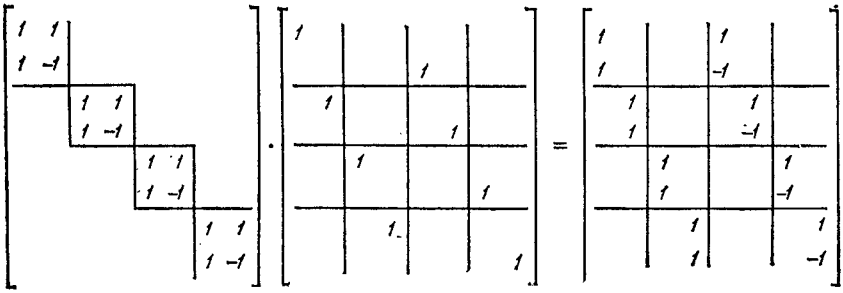
Значит, перестановка π или ее матричное представление P_2 осуществляется циклическим сдвигом $(s_1 s_2 \ldots s_n) \to (s_n s_1 \ldots s_{n-1})$ разрядов у индексов s отсчетов x_s. Отсюда получаем следующее свойство двоичного перемешивания: $P^n = I$. Тогда для каждого сомножителя быстрого χ-преобразования на группе $H = H_2 \dotplus H_2 \dotplus \ldots \dotplus H_2$, обозначая $T_1 = H_2 \otimes I_2 \otimes \ldots \otimes I_2$, будем иметь

$$\left.\begin{aligned}
&P_2 T_1 P_2^{-1} = P_2 (H_2 \otimes I_2 \otimes I_2 \otimes \cdots \otimes I_2) P_2^{-1} = \\
&= I_2 \otimes H_2 \otimes I_2 \otimes \cdots \otimes I_2 = T_2; \\
&P_2^2 T_1 P_2^{-2} = P_2^2 (H_2 \otimes I_2 \otimes I_2 \otimes \cdots \otimes I_2) P_2^{-2} = \\
&= I_2 \otimes I_2 \otimes H_2 \otimes \cdots \otimes I_2 = T_3; \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&P_2^{(n-1)} T_1 P_2^{(n-1)} = P_2^{(n-1)} (H_2 \otimes I_2 \otimes I_2 \otimes \cdots \otimes I_2) P_2^{-(n-1)} = \\
&= I_2 \otimes I_2 \otimes I_2 \otimes \cdots \otimes H_2 = T_n.
\end{aligned}\right\} \qquad (3.24)$$

Подстановка (3.24) в $\hat{H}_{2^n} = \prod_{i=1}^{n} T_i$ дает

$$\hat{H}_{2^n} = T_1 (P_2 T_1 P_2^{-1}) (P_2^2 T_1 P_2^{-2}) \ldots (P_2^{n-1} T_1 P_2^{-n+1}) = (T_1 P)^n,$$

где $T_1 R$ имеет следующий вид (при $n = 3$):



Рассмотрим теперь следующий случай: $H = H_m \dotplus H_m \dotplus \ldots$ $\ldots \dotplus H_m$. Для него введем m-ичную перемешивающую матрицу

$$P_m x(s_1 s_2 \ldots s_n) = x(s_n s_1 s_2 \ldots s_{n-1}).$$

Например, для группы $H_9 = H_3 \dotplus H_3$ она имеет вид

$$P_3 = \left[\begin{array}{ccc|ccc|ccc} 1 & & & & & & & & \\ & & & 1 & & & & & \\ & & & & & & 1 & & \\ \hline & 1 & & & & & & & \\ & & & & 1 & & & & \\ & & & & & & & 1 & \\ \hline & & 1 & & & & & & \\ & & & & & 1 & & & \\ & & & & & & & & 1 \end{array}\right].$$

Данное перемешивание осуществляется следующим образом. Весь массив $x_0 x_1 x_2 \ldots x_{3^n-1}$ делится на три части, например для $n = 2$ имеем

$$x_0 x_1 x_2 \,|\, x_3 x_4 x_5 \,|\, x_6 x_7 x_8.$$

Затем к первому элементу первой части приписываются первые элементы остальных частей. Потом идет второй элемент второй части, к которому приписываются вторые элементы остальных частей и т. д.:

$$\begin{array}{ccccccccc} & & x_6 & & x_7 & & x_8 \\ & x_3 & \downarrow & & \downarrow & & \downarrow \\ x_0 & \downarrow & \downarrow & x_1 & \downarrow & x_2 & \downarrow & \downarrow \end{array}.$$

Теперь нетрудно понять, что для слабозаполненных матриц имеют место равенства $P_m^i T_1 P_m^{-i} = T_i$, $i = 1, 2, \ldots, m$. Поэтому

$$\hat{H}_{m^n} = T_1 P_m T_1 P_m^{-1} P_m^2 T_1 P_m^{-2} \ldots P_m^{n-1} T_1 P_m^{-n+1} = (T_1 P_m)^n,$$

где $T_1 P_m$ имеет следующий вид (при $n = 2$, $m = 3$):

$$T_1 P_3 = \left[\begin{array}{ccc|ccc|ccc} 1 & & & 1 & & & 1 & & \\ 1 & & & \varepsilon & & & \varepsilon^2 & & \\ 1 & & & \varepsilon^2 & & & \varepsilon & & \\ \hline & 1 & & & 1 & & & 1 & \\ & 1 & & & \varepsilon & & & \varepsilon^2 & \\ & 1 & & & \varepsilon^2 & & & \varepsilon & \\ \hline & & 1 & & & 1 & & & 1 \\ & & 1 & & & \varepsilon & & & \varepsilon^2 \\ & & 1 & & & \varepsilon^2 & & & \varepsilon \end{array}\right].$$

Перейдем теперь к общему случаю, когда $H = H_{h_1} \dotplus H_{h_2} \dotplus \ldots$ $\ldots \dotplus H_{h_n}$. Введем в рассмотрение матрицы перемешивания $P_{h_1}, P_{h_2}, \ldots$ $\ldots, P_{h_n}$. Ясно, что $P_{h_1} P_{h_2} \ldots P_{h_n} = I$. Нетрудно проверить также, что эти матрицы коммутируют между собой. Согласно формуле (3.20) для быстрого χ-преобразования на группе H_h имеем

$$\hat{H}_h = \prod_{i=1}^{n} T_i = T_1 T_2 \ldots T_n = T_1 (P_{h_1} P_{h_2} \ldots P_{h_n}) T_2 (P_{h_1} P_{h_2} \ldots$$
$$\ldots P_{h_n}) T_3 \ldots (P_{h_1} P_{h_2} \ldots P_{h_n}) T_n (P_{h_1} P_{h_2} \ldots P_{h_n}). \qquad (3.25)$$

Так как матрицы P_{h_1}, P_{h_2}, ..., P_{h_n} коммутируют, то их можно внутри (3.25) представлять так, как нам это удобно. Например,

$$\hat{H}_h = (T_1 P_{h_1}) (P_{h_2} \ldots P_{h_n} T_2 P_{h_1}) P_{h_2} (P_{h_3} \ldots P_{h_n} T_3 P_{h_1} P_{h_2}) P_{h_3} \ldots$$
$$\ldots (P_{h_n} T_n P_{h_1} P_{h_2} \ldots P_{h_{n-1}}) P_{h_n} =$$
$$= T_1 P_{h_1} (P_{h_1}^{-1} T_2 P_{h_1}) P_{h_2} (P_{h_2}^{-1} P_{h_1}^{-1} T_3 P_{h_1} P_{h_2}) \ldots$$
$$\ldots (P_{h_{n-1}}^{-1} P_{h_{n-2}}^{-1} \ldots P_{h_1}^{-1} T_{h_m} P_{h_1} P_{h_2} \ldots P_{h_{n-1}}) P_{h_m}.$$

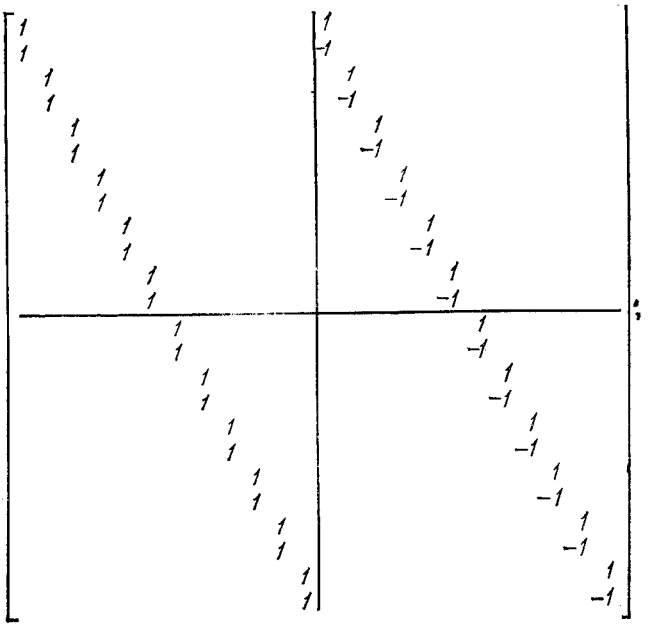
Поскольку

$$P_{h_1}^{-1} T_2 P_{h_2} = T_2, \; P_{h_2}^{-1} P_{h_1}^{-1} T_3 P_{h_1} P_{h_2} = T_3, \ldots$$
$$\ldots, \; P_{h_{n-1}} P_{h_{n-2}} \ldots P_{h_1}^{-1} T_{h_1} P_{h_1} \ldots P_{h_{n-2}} P_{hn-1} = T_{h_n},$$

то

$$\hat{H}_h = (T_1 P_{h_1}) (T_2 P_{h_2}) \ldots (T_n P_{h_n}). \qquad (3.26)$$

Обозначая $T_i P_{h_i} = G_i$, получаем быстрое Х-преобразование по методу Гуда: $\hat{H}_h = G_1 G_2 \ldots G_n$. Так, например, для группы $H_{24} = H_2 + H_3 + H_4$ это дает

$G_1 =$  ;

$$G_2 = \left[\begin{array}{ccc|ccc|ccc}
1 & & & 1 & & & 1 & & \\
1 & & & \varepsilon & & & \varepsilon^2 & & \\
1 & & & \varepsilon^2 & & & \varepsilon & & \\
 & 1 & & & 1 & & & 1 & \\
 & 1 & & & \varepsilon & & & \varepsilon^2 & \\
 & 1 & & & \varepsilon^2 & & & \varepsilon & \\
 & & 1 & & & 1 & & & 1 \\
 & & 1 & & & \varepsilon & & & \varepsilon^2 \\
 & & 1 & & & \varepsilon^2 & & & \varepsilon \\
\hline
1 & & & 1 & & & 1 & & \\
1 & & & \varepsilon & & & \varepsilon^2 & & \\
1 & & & \varepsilon^2 & & & \varepsilon & & \\
 & 1 & & & 1 & & & 1 & \\
 & 1 & & & \varepsilon & & & \varepsilon^2 & \\
 & 1 & & & \varepsilon^2 & & & \varepsilon & \\
 & & 1 & & & 1 & & & 1 \\
 & & 1 & & & \varepsilon & & & \varepsilon^2 \\
 & & 1 & & & \varepsilon^2 & & & \varepsilon \\
\hline
1 & & & 1 & & & 1 & & \\
1 & & & \varepsilon & & & \varepsilon^2 & & \\
1 & & & \varepsilon^2 & & & \varepsilon & & \\
 & 1 & & & 1 & & & 1 & \\
 & 1 & & & \varepsilon & & & \varepsilon^2 & \\
 & 1 & & & \varepsilon^2 & & & \varepsilon & \\
 & & 1 & & & 1 & & & 1 \\
 & & 1 & & & \varepsilon & & & \varepsilon^2 \\
 & & 1 & & & \varepsilon^2 & & & \varepsilon
\end{array}\right];$$

где $\varepsilon = \sqrt[3]{1}$; $\gamma = \sqrt[4]{1}$.

В заключение приведем выражения для быстрых преобразований Уолша и Крестенсона:

$$\hat{H}_{2^n} = \prod_{i=1}^{n} [I_{2^{i-1}} \otimes H_2 \otimes I_{2^{n-i}}]; \quad \hat{H}_{p^n} = \prod_{i=1}^{n} [I_{p^{i-1}} \otimes \hat{H}_p \otimes I_{p^{n-i}}],$$

или по методу Гуда

$$\hat{H}_{2^n} = (G_2)^n; \quad \hat{H}_{p^n} = (G_p)^n.$$

* * *

Таким образом, χ-преобразования являются аппаратом для проведения обобщенного гармонического анализа цифровых сигналов, заданных на конечной абелевой группе и принимающих значения в некотором поле F. Введение χ-преобразований позволяет с

$$G_3 = \left[\begin{array}{cccc|cccc|cccc|cccc}
1 & & & & 1 & & & & 1 & & & & 1 & & & \\
1 & & & & \gamma & & & & \gamma^2 & & & & \gamma^3 & & & \\
1 & & & & \gamma^2 & & & & 1 & & & & \gamma^2 & & & \\
1 & & & & \gamma^3 & & & & \gamma^2 & & & & \gamma & & & \\
 & 1 & & & & 1 & & & & 1 & & & & 1 & & \\
 & 1 & & & & \gamma & & & & \gamma^2 & & & & \gamma^3 & & \\
 & 1 & & & & \gamma^2 & & & & 1 & & & & \gamma^2 & & \\
 & 1 & & & & \gamma^3 & & & & \gamma^2 & & & & \gamma & & \\
 & & 1 & & & & 1 & & & & 1 & & & & 1 & \\
 & & 1 & & & & \gamma & & & & \gamma^2 & & & & \gamma^3 & \\
 & & 1 & & & & \gamma^2 & & & & 1 & & & & \gamma^2 & \\
 & & 1 & & & & \gamma^3 & & & & \gamma^2 & & & & \gamma & \\
 & & & 1 & & & & 1 & & & & 1 & & & & 1 \\
 & & & 1 & & & & \gamma & & & & \gamma^2 & & & & \gamma^3 \\
 & & & 1 & & & & \gamma^2 & & & & 1 & & & & \gamma^2 \\
 & & & 1 & & & & \gamma^3 & & & & \gamma^2 & & & & \gamma
\end{array}\right],$$

единых позиций подходить к выбору базисных функций, по которым производится разложение цифрового сигнала. Эти преобразования вычисляются по быстрым алгоритмам, которые в общем случае можно рассматривать как исходные для построения быстрых алгоритмов частных случаев Х-преобразований. Вычисление по быстрым алгоритмам по сравнению с вычислениями непосредственно по формулам Х-преобразований требует реализации значительно меньшего числа вычислительных операций. Дальнейшее снижение объема вычислений может быть достигнуто за счет выбора поля F с просто реализуемыми арифметическими операциями.

ГЛАВА 4

ТЕОРЕТИКО-ЧИСЛОВЫЕ ПРЕОБРАЗОВАНИЯ

1. Преобразования Фурье — Галуа

При анализе сигналов и систем особое место занимают ортогональные преобразования благодаря свойству, заключающемуся в том, что координаты разлагаемых произвольных функций в пространстве ортогональных функций вычисляются наиболее просто [48, 155]. С появлением ЦВМ возрос интерес к изучению цифровых ортогональных преобразований. Такие преобразования и функции, определенные над полем комплексных чисел, изучены достаточно хорошо [12, 126, 155, 160, 172]. Области использования их весьма обширные: обработка речевых сигналов [135], обработка изображений [112, 129, 130, 148], отбор признаков при распознавании образов [12, 63, 113, 161] и др. Поэтому в работах, связанных с использованием конечных колец и полей в целях ЦОС, в первую очередь исследовался вопрос о возможности определения над этими алгебраическими системами ортогональных преобразований, аналогичных изученным [189, 190, 199, 201, 204, 214]. В этой связи сначала займемся изучением и описанием ортогональных преобразований, определенных над конечным полем или над конечным кольцом.

Пусть GF (p) — конечное поле Галуа; G_N — циклическая группа порядка N; $\varepsilon = \sqrt[N]{1} \in \mathrm{GF}(p)$. Тогда χ-преобразования сигнала $x(n)$ в пространстве $L(G_N, \mathrm{GF}(p))$

$$S(\alpha) = \sum_{n=0}^{N-1} x(n)\,\varepsilon^{\alpha n}, \quad x(n) = N^{-1} \sum_{\alpha=0}^{N-1} S(\alpha)\,\varepsilon^{-\alpha n} \tag{4.1}$$

будем называть преобразованиями Фурье — Галуа (ПФГ). Подобные преобразования впервые были предложены Р. Г. Фараджевым и Я. З. Цыпкиным в работах [165—167].

χ-Преобразования сигнала $x(n)$, определенные в пространстве $L(G_N, Z_M)$, называют теоретико-числовыми преобразованиями (ТЧП) [2, 211]. Рассмотрим свойства и особенности ТЧП и ПФГ, связанные с использованием их для решения задач ЦОС и с реализацией с помощью ЦВМ. С этой точки зрения важной является задача выбора первообразного корня из единицы $\varepsilon = \sqrt[N]{1}$ с заданным значением N

и выбора значения модуля M (или p), позволяющих снизить объем вычислений при реализации.

Так как функции $\chi_\alpha(n) = \varepsilon^{\alpha n}$ — характеры циклической группы G_N, то ПФГ переводит периодические корреляцию и свертку в произведение спектров, а именно: если

$$c(n) = \sum_{\tau=0}^{N-1} h(n \ominus \tau)\, x(\tau); \quad b(\tau) = \sum_{n=0}^{N-1} x_1(n)\, x_2(n-\tau),$$

то

$$S_c(\alpha) = S_n(\alpha)\, S_x(\alpha); \quad S_b(\alpha) = S_1(\alpha)\, S_2(N-\alpha),$$

где $S_c(\alpha)$, $S_b(\alpha)$, $S_n(\alpha)$, $S_x(\alpha)$, $S_1(\alpha)$, $S_2(\alpha)$ — спектры соответственно функций $c(n)$, $b(\tau)$, $h(n)$, $x(n)$, $x_1(n)$, $x_2(n)$.

Следовательно, если $\varepsilon \in \mathrm{GF}(p)$ может быть найдено таким, что операция умножения на степени ε достаточно просто осуществима на ЦВМ, свертку и корреляцию можно вычислить через спектры соответствующих функций. Очевидно, что ε желательно выбирать в виде степени двойки, так как в этом случае умножение на $\varepsilon^{\alpha n}$ сводится к операции сдвига кодового слова в арифметическом устройстве ЦВМ. Именно в этом случае можно получить выигрыш в быстродействии, поскольку вместо умножения на комплексные числа $\varepsilon^{\alpha n} = \exp\left(i\,\frac{2\pi}{N}\,\alpha n\right)$, которые требуют наибольших затрат времени при использовании быстрого преобразования Фурье, появляются обычные сдвиги кодового слова.

Отметим, что ПФГ действует в пространстве $L(G_N, \mathrm{GF}(p))$, в то время как физические сигналы, дискретизированные по времени, принадлежат пространству $L(G_T, C)$ или $L(G_T, R)$ (рассматриваем конечный интервал времени T). Однако при обработке сигналов $x(t)$ на ЦВМ происходит их квантование по уровню. Поэтому выборочные значения $x(n)$ сигналов $x(t)$ можно рассматривать как функции, заданные на группе G_N и принимающие значения в некотором поле $\mathrm{GF}(p)$, или, более общо, в некотором конечном коммутативном кольце Z_M: $x(n) = G_n \to Z_M$. Именно это обстоятельство дает возможность воспользоваться гармоническим анализом над кольцами Z_M и выбирать базис в виде $\chi_\alpha(n) = 2^{\alpha n}$, где $2 = \sqrt[N]{1} \in Z_M$.

Свойства ПФГ изоморфны свойствам преобразований Фурье. В частности, ПФГ (или ТЧП) можно вычислять по быстрым алгоритмам, аналогичным быстрым алгоритмам, применяемым при вычислении преобразования Фурье [202, 209]. ТЧП и ПФГ по своей структуре наилучшим образом реализуются с использованием цифровой элементной базы. Объем вычислений при реализации существенным образом зависит от выбора параметров ε и M. Эти параметры, очевидно, следует выбирать, исходя из следующих соображений:

как отмечалось, ε желательно иметь в виде степени двойки, так как в этом случае умножение на степени ε при вычислении ПФГ заменяется сдвигами кодовых слов и приведением сдвинутых кодовых слов по модулю M (или по модулю p);

значения M или p должны быть такими, чтобы арифметические операции по модулю M (или модулю p) можно было просто реализовать с высоким быстродействием.

Остановимся пока на простых числах $M = p$. Среди них наиболее полно удовлетворяют последнему из приведенных требований числа Мерсенна $p = 2^q - 1$, где q — простое число, и числа Ферма $F_n = 2^{2^n} + 1$, где n — любое целое число.

ТЧП и ПФГ с применением чисел Мерсенна получили название ТЧП Мерсенна [202, 205, 208]. Рассмотрим их более подробно. Числа Мерсенна являются простыми не для всех простых q. В 1664 г. Мерсенн для $q \leqslant 257$ указал все p, которые он считал простыми числами. Исследования в этой области показали, что в пяти случаях Мерсенн ошибся. Оказалось, что p являются простыми числами для q, равного 2; 3; 5; 7; 13; 19; 31; 61; 89; 107; 127, и составными для всех остальных $q < 257$. До 1750 г. строго математически была доказана простота чисел Мерсенна при $q \leqslant 19$. В 1750 г. Леонард Эйлер установил, что число $M_{31} = 2^{31} - 1$ является простым. Эйлерово число M_{31} оставалось самым большим из известных простых чисел более ста лет. В 1876 г. французский математик Лукас установил, что 39-значное (в десятичной системе счисления) число

$$M_{127} = 170\,141\,183\,469\,469\,231\,731\,687\,303\,715\,884\,105\,727 = 2^{127} - 1$$

является простым числом.

Первые 11 чисел Мерсенна были вычислены с помощью только карандаша. Появление вычислительных машин позволило продолжить поиски. Среди чисел Мерсенна с $127 < q \leqslant 257$ не оказалось простых. С помощью ЦВМ SWAC (Калифорния) летом 1952 г. Д. Х. Ленегр нашел новые простые числа Мерсенна M_{521}, M_{607}, M_{1279}, M_{2203}, M_{2281}. Между M_{127} и M_{521} лежит 66 составных M_q. Вообще говоря, разложения на множители M_q, о которых известно, что они составные, не найдено.

Дальнейшие поиски также увенчались успехом. Ризель (1958 г.) показал, что $q = 3217$ дает простое число Мерсенна, а Гурвиц (1962 г.) нашел еще два таких значения: $q = 4253$ и $q = 4423$. Огромного успеха добился Гиллельс (1964 г.), который нашел простые числа Мерсенна, соответствующие значениям $q = 9689$; $q = 9941$; $q = 11\,213$. Совсем недавно получены [198, 200] еще четыре простых числа Мерсенна с $q = 19\,937$; $q = 21\,701$; $q = 23\,209$; $q = 44\,497$.

Таким образом, к настоящему времени известно 27 простых чисел Мерсенна, которые получаются для q, равного 2; 3; 5; 7; 11; 13; 17; 19; 31; 61; 89; 107; 127; 521; 607; 1279; 2203; 2281; 3217; 4253; 9689; 9941; 11213; 19 937; 21 701; 23 209; 44 497.

Последнее 27-е число Мерсенна получено в 1979 г. с помощью ЦВМ CRAY-1.

Найдем период числа 2 по модулю чисел Мерсенна, последовательно возводя двойку в степень. Ясно, что $2^k < 2^q - 1$ для $k < q$. Но $2^q \equiv 1 \pmod{2^q - 1}$, поэтому $N_{\max}(2) = q$. Аналогично получаем $N_{\max}(-2) = 2q$, т. е. максимальная длина интервала определения $N_{\max}$ сигнала $x(n)$ равна $2q$ при выборе $\varepsilon = -2$. При других значе-

Таблица 28. Степени элементов поля *GF* (17)

t	2^t	3^t	4^t	6^t	t	2^t	3^t	4^t	6^t
0	1	1	1	1	9	2	14	4	11
1	2	3	4	6	10	4	8	16	15
2	4	9	16	2	11	8	7	13	5
3	8	10	13	12	12	16	4	1	13
4	16	13	1	4	13	15	12	4	10
5	15	5	4	7	14	13	2	16	9
6	13	15	16	8	15	9	6	13	3
7	9	11	13	14	16	1	1	1	1
8	1	16	1	16					

ниях ε возможна большая величина $N_{\max}$ (вплоть до $N = p - 1$), но при вычислении ПФГ или ТЧП необходима более сложная реализация умножений значений сигнала $x(n)$ на степени первообразного корня ε. Отметим, что числа Мерсенна широко применяются в комплексных ТЧП над полем GF (p^2), $p = 2^q - 1$. В этом поле порядок мультипликативной группы равен $(2^q - 1)^2 - 1 = 2^q(2^q - 1)$. Поэтому возможны ТЧП с $N = 2^q$, так как $N \mid 2^q(2^q - 1)$.

Рассмотрим теперь числа Ферма. Первые несколько чисел Ферма следующие: $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$. Эти числа простые, а числа $F_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$, $F_6 \approx \approx 1{,}84 \cdot 10^{19} = 274\,177 \cdot 67\,280\,421\,310\,721$ — составные.

ТЧП с применением чисел Ферма в качестве модулей называют преобразованиями Ферма (ТЧПФ). Так как числа Ферма $F_0 - F_4$ простые, то $N_{\max}(F_t) = 2^{2^t} = 2^b$, где $b = 2^t$, следовательно, существуют ТЧПФ для любого объема $N = 2^m$, $m \leqslant b$. Для этих простых чисел Ферма целое 3 является корнем из единицы порядка $2b$, допускающим наибольший возможный объем преобразований. Целое 2 имеет порядок $N = 2b = 2^{t+1}$. Если ε принимается равным 2 или степени 2, то ТЧПФ называется теоретико-числовым преобразованием Рейдера (ТЧПР) [4, 213].

Пример 4.1. Рассмотрим число Ферма $F_2 = p = 17$. Найдем степени некоторых элементов поля GF (17), которые можно принять в качестве первообразных элементов. Результаты сведены в табл. 28. Как видно, элементы 3 и 6 являются примитивными корнями, которые образуют все ненулевые элементы поля GF (17). Элемент 2 имеет порядок 8, элемент 4 — порядок 4. Заметим, что $6^2 \equiv \equiv 2 \pmod{17}$, т. е. $\sqrt{2} = 6 \pmod{17}$.

Первообразный элемент ε, имеющий порядок $4b$ в $\mathrm{GF}(F_t)$, задается выражениями

$$\varepsilon = 2^{b/4}(1 + 2^{-b/2}) \quad \text{или} \quad \varepsilon = 2^{b/4}(1 - 2^{b/2}).$$

Докажем это утверждение для произвольного кольца Z_M нечетного порядка. Пусть α — некоторый обратимый элемент в кольце Z_M. Составим сумму $\alpha + \alpha^{-1} = \varepsilon$. Возведем ее в квадрат:

$$\varepsilon^2 = (\alpha + \alpha^{-1})^2 = \alpha^2 + \alpha^{-2} + 2.$$

Если α выбрать таким образом, чтобы $\alpha^2 + \alpha^{-2} = 0$, то ε и есть искомый элемент. Выясним теперь, что представляет собой элемент α. Из уравнения $\alpha^2 + \alpha^{-2} = 0$ следует, что $\alpha^4 + 1 = 0$, т. е. что $\alpha^4 = -1$ и $\alpha^8 = 1$; другими словами, если α — корень восьмой степени из 1, то $\varepsilon = \alpha + \alpha^{-1} = \sqrt{2}$. Пусть теперь $M = F_t = 2^{2^t} + 1$ $(t \geqslant 2)$. Тогда $2^{2^{t+1}} = 2^{2b} \equiv 1 \pmod{F_t}$ и $\alpha = \sqrt[8]{1} = 2^{2^t-2}$, откуда

$$\alpha^{-1} = 1/2^{2^t-2} = 2^{2^{t+1}}/2^{2^t-2} = 2^{2^{t+1}} - 2^{t-2};$$

$$\varepsilon = \sqrt{2} = \alpha + \alpha^{-1} = 2^{2^t-2} + 2^{2^{t+1}} - 2^{t-2}.$$

Так как $2^{2^t-2} = 2^{b/4}$; $2^{2^{t+1}} = 2^{2b}$, то

$$\varepsilon = 2^{b/4} + 2^{2b-b/4} = 2^{b/4}(1 + 2^{2b-b/2}).$$

Отсюда можно получить два выражения для ε. Учитывая, что $2^{2b} \equiv 1 \pmod{2^b + 1}$, находим первое выражение:

$$\varepsilon = 2^{b/4}(1 + 2^{-b/2}).$$

Кроме того, поскольку $2^{2b} = 2^b \cdot 2^b = -2^b$ и $2^{2b-b/2} = -2^{b/2}$, имеем второе выражение

$$\varepsilon = 2^{b/4}(1 - 2^{b/2}).$$

Непосредственно проверка показывает, что $\varepsilon^2 = 2$. Действительно,

$$\varepsilon^2 = [2^{b/4}(1 + 2^{-b/2})]^2 = 2^{b/2}(1 + 2^{-b} + 2^{-b/2+1}) =$$

$$= 2^{b/2} \cdot 2^{-b/2+1} \equiv 2 \bmod (2^b + 1).$$

Поэтому $\varepsilon^2 = 2$. Далее,

$$\varepsilon^2 = [2^{b/4}(1 - 2^{b/2})]^2 = 2^{b/2}(1 + 2^b - 2^{b/2+1}) =$$

$$= -2^{b/2} \cdot 2^{b/2+1} = -2^{b+1} \equiv 2 \bmod (2^b + 1).$$

Любая нечетная степень $\sqrt{2}$ будет также порядка $4b = 2^{t+2}$. При возведении $\sqrt{2}$ в степень 2^{t+2-m} получается ε порядка 2^m, $m \leqslant t + 2$. Таким образом, сформированное утверждение доказано.

Как видно, ТЧП по модулю ТЧПФ с простым или составным модулем может иметь в качестве первообразного элемента ε число 2 или степень 2 для $N_{\max} = 2^b = 2^{t+1}$. В силу этого возможно вычисление ТЧПФ по быстрым алгоритмам, аналогичным быстрым алго-

ритмам преобразования Фурье с прореживанием по времени и с прореживанием по частоте [4, 12, 115, 134, 202].

Если применяется $\varepsilon = \sqrt{2}$, то можно осуществить преобразование последовательности длиной $N_{\max} = 4b = 2^{t+2}$, но в этом случае один из этапов алгоритма будет требовать двух сдвигов, так как $\sqrt{2} = 2^{b/4}\,(2^{b-2} - 1)$. При $\varepsilon = \sqrt{2}$ длина $N_{\max} = 4b$ является максимально возможной для F_5 и F_6.

Сравним ТЧПФ и ТЧП по модулю чисел Мерсенна (ТЧПМ). ТЧПФ с ε, равным 2 или степени 2, можно определить для интервала $N_{\max 1} \simeq 2N_{\max 2}$, где $N_{\max 2}$ — интервал определения сигнала $x(n)$, для которого возможно построение ТЧПМ с $\varepsilon = 2$ (в этом случае $F_t = 2^{2^t} + 1$, $M = 2^q - 1$, причем $q = 2^t - 1$). Однако, выбрав $\varepsilon = -2$, при построении ТЧПМ можно увеличить $N_{\max 2}$ в два раза. Умножение на отрицательные степени 2 соответствует циклическому сдвигу и инверсии кодового слова. Вообще арифметика по модулю чисел Мерсенна проще в реализации по сравнению с арифметикой по модулю чисел Ферма. В частности, проще реализуются умножения на степени 2 даже при выборе $\varepsilon = -2$.

Упражнение 4.1. Показать, что умножение на степени 2 в кольце по модулю $M = 2^n - 1$ сводится к циклическому сдвигу двоичного числа — множимого. Представить умножение на степени 2 в кольце по модулю $F = 2^n + 1$ в виде двух операций: циклического сдвига числа — множимого и вычитания циклически сдвинутых m старших разрядов от числа, получившегося в результате сдвига и отбрасывания m старших разрядов (множитель равен 2^m).

Несмотря на более простую аппаратурную реализацию, практическое применение ТЧПМ ограничено. Это связано с тем, что при выборе ε, равным 2 или степени 2, получалось $N_{\max}$, равное простому числу. Для таких значений N не были известны быстрые алгоритмы. Положение в корне изменилось после нахождения быстрых алгоритмов преобразования Фурье для случая, когда N — простое число [46, 77, 203]. Аналогичные алгоритмы можно использовать и при вычислении ТЧПМ. В связи с этим интерес к ТЧПМ значительно возрос.

2. χ-Преобразования над прямыми суммами полей Галуа

При решении многих практических задач необходимо проводить обработку многомерных цифровых сигналов. Кроме того, ряд задач обработки одномерных сигналов с целью повышения эффективности реализации удобно свести к обработке многомерных сигналов [182]. Поэтому важно рассмотрение многомерных χ-преобразований.

Отправной точкой при дальнейших исследованиях будет существование изоморфизма, порождаемого одной простой теоремой теории чисел, называемой китайской теоремой об остатках. Напомним ее. Если $m = p_1 p_2 \ldots p_n = \prod_{i=1}^{n} p_i$ и p_i — различные простые числа,

то кольцо Z_M классов вычетов по модулю m изоморфно прямой сумме $\mathrm{GF}(p_1) \dotplus \mathrm{GF}(p_2) \dotplus \ldots \dotplus \mathrm{GF}(p_n)$ конечных полей $\mathrm{GF}(p_i)$:

$$Z_m \sim \mathrm{GF}(p_1) \dotplus \mathrm{GF}(p_2) \dotplus \cdots \dotplus \mathrm{GF}(p_n). \tag{4.2}$$

Изоморфизм задается как отображение

$$\Psi_1 : a \mapsto (a_1, a_2, \ldots, a_n),$$

где $a \in Z_m$, $a_i \equiv a(\mathrm{mod} p_i)$, $i = 1,2,\ldots, n$ [207].

Обратный изоморфизм задается отображением

$$\Psi^{-1} : (a_1, a_2, \ldots, a_n) \mapsto a, \tag{4.3}$$

где

$$a = M_1 M_1^{-1} a_1 + \cdots + M_n M_n^{-1} a_n,$$

$$M_i = m/p_i; \quad M_i^{-1} = (M_i \bmod p_i)^{-1} \bmod p_i. \tag{4.4}$$

Оба представления $(a_1, a_2, \ldots, a_n)$ и a элементов Z_m с математической точки зрения эквивалентны. Однако с точки зрения простоты аппаратурной реализации они различны. Как указывалось, аппаратурная реализация проще при представлении элементов кольца Z_m в виде n-ки $(a_1, a_2,\ldots, a_n)$. Действительно, для представления чисел кольца Z_m необходимо $\log_k m$ разрядов (при $k = 2$ $\log_2 m$ разрядов). При использовании первого представления уменьшается разрядная сетка арифметического устройства. Кроме того, появляется возможность повысить быстродействие вычислений. Покажем это на примере ТЧП.

Пусть N делит $p_i - 1$ для всех $i = 1, 2,\ldots, n$. Тогда существует примитивный корень ε_i из единицы в $\mathrm{GF}(p_i)$ для $i = 1, 2,\ldots, n$. Элемент

$$\Psi^{-1}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = \varepsilon$$

соответствует примитивному корню N-й степени из единицы в Z_m. Отсюда следует, что на N точках существуют прямое и обратное ТЧП над Z_m:

$$S(\alpha) = \sum_{n=0}^{N-1} x(n)\, \varepsilon^{-\alpha n}, \quad x(n) = N^{-1} \sum_{\alpha=0}^{N-1} S(\alpha)\, \varepsilon^{\alpha n}. \tag{4.5}$$

Применяя к паре уравнений (4.5) преобразование Ψ, получаем

$$\Psi[S(\alpha)] = \sum_{n=0}^{N-1} \Psi[x(n)]\, \Psi[\varepsilon^{-\alpha n}]; \quad \Psi[x(n)] = N^{-1} \sum_{\alpha=0}^{N-1} \Psi[S(\alpha)]\, \Psi[\varepsilon^{\alpha n}],$$

т. е.

$$(S_1(\alpha), \ldots, S_n(\alpha)) = \left(\sum_{n=0}^{N-1} x_1(n)\, \varepsilon_1^{-\alpha n}, \ldots, \sum_{n=0}^{N-1} x_n(n)\, \varepsilon_n^{-\alpha n} \right);$$

$$(x_1(n), \ldots, x_n(n)) = \left(N^{-1} \sum_{\alpha=0}^{N-1} S_1(\alpha)\, \varepsilon_1^{\alpha n}, \ldots, N^{-1} \sum_{\alpha=0}^{N-1} S_n(\alpha)\, \varepsilon_n^{\alpha n} \right).$$

Приравнивая соответствующие координаты, находим n пар преобразований:

$$\left.\begin{aligned}
&S_1(\alpha) = \sum_{n=0}^{N-1} x_1(n)\,\varepsilon_1^{-\alpha n}, \quad x_1(n) = N^{-1}\sum_{\alpha=0}^{N-1} S_1(\alpha)\,\varepsilon_1^{\alpha n} \pmod{p_1};\\
&S_2(\alpha) = \sum_{n=0}^{N-1} x_2(n)\,\varepsilon_2^{-\alpha n}, \quad x_2(n) = N^{-1}\sum_{\alpha=0}^{N-1} S_2(\alpha)\,\varepsilon_2^{\alpha n} \pmod{p_2};\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&S_n(\alpha) = \sum_{n=0}^{N-1} x_n(n)\,\varepsilon_n^{-\alpha n}, \quad x_n(n) = N^{-1}\sum_{\alpha=0}^{N-1} S_n(\alpha)\,\varepsilon_n^{\alpha n} \pmod{p_n}.
\end{aligned}\right| \qquad (4.6)$$

Таким образом, если требуется вычислить n преобразований (4.6), то эти преобразования могут быть вычислены независимо n раз или однократно над кольцом Z_m по формулам (4.5). Если все ε_i — степени 2, то при независимых вычислениях спектров $S_i(\alpha)$ потребуется $nN\log_2 N$ операций, а совместные вычисления по формуле (4.5) потребуют всего $N\log_2 N$ операций, поскольку операцию, задаваемую выражением (4.3), можно аппаратурно совместить с операцией аналого-цифрового преобразования, а умножения на степени 2, как в полях $\mathrm{GF}(p_i)$, так и в кольце, требуют одного и того же времени. В этом случае схема совместных вычислений по формуле (4.5) более быстродействующая. Однако если ε и ε_i не являются степенями двойки, то умножения на степени ε (см. выражение (4.5)) занимают приблизительно такое же время, как и n умножений на степени ε_i в выражении (4.6). Это связано с тем, что длина разрядной сетки для представления элементов кольца Z_m приблизительно равна суммарной длине разрядных сеток, представляющих элементы полей $\mathrm{GF}(p_i)$. Основное преимущество $\mathrm{GF}(p_1) \dotplus \mathrm{GF}(p_2) \dotplus \ldots \dotplus \mathrm{GF}(p_m)$-арифметики — возможность организации параллельных вычислений и, следовательно, значительного повышения быстродействия арифметического устройства. Это особенно касается случая, когда ε_i и ε не являются степенями 2. Заметим, что хотя выбор $\varepsilon = 2$ или степени 2 желателен, но не всегда возможен на практике из-за малых объемов ТЧП $N_{\max}$.

Упражнение 4.2. Изобразить в виде графика функции Ψ_1 и Ψ^{-1} (функция Ψ_1^{-1} задана выражением (4.3)).

Естественным обобщением ТЧП над прямой суммой полей Галуа являются ТЧП над произвольным кольцом Z_m, т. е. преобразования в базисе характеров $\chi_\alpha(n)$ циклической группы G_N над кольцом Z_m. По определению характеры $\chi_\alpha(n)$ — это функции, отображающие группу G_N в мультипликативную группу MZ_m, которая состоит из $\varphi(m) = m\prod_{i=1}^{r}(1 - g_i^{-1})$ элементов, где $m = g_1 g_2, \ldots, g_r$ — простые числа в каноническом разложении числа $m = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_r^{\alpha_r}$. По теореме Эйлера любой элемент $a \in M(Z_m)$ удовлетворяет равенству $a^{\varphi(m)} \equiv 1 (\mathrm{mod} m)$. Поэтому любой элемент $a \in M(Z_m)$ является корнем $\varphi(m)$-й степени из единицы. Если α — первообразный корень степе-

ни $\varphi(m)$ (т. е. степени α пробегают всю группу $M(Z_m)$), то любой корень ε степени N из единицы будет иметь следующий вид: $\varepsilon = \alpha^{\varphi(m)/N}$. В общем случае, если ε — корень порядка N, то ε^k является корнем порядка N/k, если $k \mid N$, и порядка N, если N и k взаимно просты. Это означает, что корней порядка N ровно $\varphi(N)$ и из них можно выбрать такой, который в максимальной степени удовлетворяет требованиям, диктуемым объемом вычислений и необходимым значением $N_{\max}$.

Напомним еще, что если $m = g_1^{\alpha_1} g_2^{\alpha_2} \ldots g_r^{\alpha_r}$ — каноническое разложение модуля кольца Z_m, то оно изоморфно кольцу $Z_{g_1^{\alpha_1}} \dotplus \dotplus Z_{g_2^{\alpha_2}} \dotplus \ldots \dotplus Z_{g_r^{\alpha_r}}$. Этот изоморфизм задается отображением

$$a \to [a \pmod{g_1^{\alpha_1}},\ a \pmod{g_2^{\alpha_2}},\ \ldots,\ a \pmod{g_r^{\alpha_r}}].$$

Пусть теперь число ε является корнем N-й степени в Z_m, т. е. является N-периодическим. Тогда оно должно быть N-периодическим и в каждом $Zg_i^{\alpha_i}$, т. е.

$$\varepsilon^N \equiv 1 \pmod{g_i^{\alpha_i}}, \quad i = 1, 2, \ldots, r. \tag{4.7}$$

Кроме того, из формулы (4.5) следует, что N должно принадлежать мультипликативной группе кольца Z_m, $M(Z_m)$, так как на N придется делить значения спектральных коэффициентов. Значит, во-первых, НОК $(m, N) = 1$ и, во-вторых, N должно делить $\varphi(g_i^{\alpha_i}) = g_i^{\alpha_i - 1}(g_i - 1)$ (так как ε N-периодично в $Zg_i^{\alpha_i}$). Следовательно, N должно быть взаимно простым с m (или с g_i; а значит, и с $g_i^{\alpha_i - 1}$) и в то же время должно делить $g_i - 1$. Отсюда следует, что

$$N \mid \text{НОД}(g_1 - 1, g_2 - 1, \ldots, g_r - 1).$$

Очевидно, что максимальное значение, которое может принимать N, равно НОД $(g_1 - 1, g_2 - 1, \ldots, g_r - 1)$, т. е.

$$N_{\max}(m) = \text{НОД}(g_1 - 1, g_2 - 1, \ldots, g_r - 1).$$

Таким образом, доказана следующая теорема.

Теорема 4.1 [214]. ТЧП в пространстве $L(G_N, Z_m)$ существует тогда и только тогда, когда $N \mid$НОД $(g_1 - 1, g_2 - 1, \ldots, g_n - 1)$ и НОК $(N, m) = 1$.

Простейшей Z_m-арифметикой с точки зрения ЦВМ является арифметика по модулю $m = 2^k$, но при m, четном $N_{\max} = 1$, т. е. в этой арифметике нет преобразований, которые оказались бы пригодными. Следовательно, m должно быть нечетным. Второй простейший случай — арифметика по модулю $m = 2^k - 1$ и $m = 2^k + 1$.

3. ТЧП над конечным полем целых комплексных чисел

Комплексным ТЧП называется χ-преобразование цифрового сигнала $\chi(n)$ в пространстве $L(G_N, Z_p^c)$. Такое преобразование применимо к комплексным целочисленным сигналам

$z(n) = x(n) + iy(n)$. Заметим, что конечное поле целых комплексных чисел Z_p^c изоморфно полю $GF(p^2)$. Более того, поле $GF(p^2)$ совпадает с Z_p^c, если в качестве неприводимого полинома выбрать полином $p(x) = x^2 + 1$. Как указывалось, простое поле Галуа $GF(p)$ можно расширить до поля Z_p^c, если уравнение $x^2 + 1 = 0$ не имеет решения в $GF(p)$. Это означает, что -1 является квадратичным невычетом. Рассмотрим случай, когда p — простое число Мерсенна вида $M = 2^q - 1$, где g равно 2; 3; 5; 13; 17; 19; 31; 61 и $p = 2^{2^t} + 1$ — число Ферма (t равно 0; 1; 2; 3; 4).

Для определения того, является ли -1 квадратичным вычетом или нет, воспользуемся символом Лежандра:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{если } a \text{ — квадратичный вычет по mod } p; \\ -1, & \text{если } a \text{ — квадратичный невычет по mod } p. \end{cases}$$

Для чисел Мерсенна имеем

$$(-1/p) = (-1)^{(p-1)/2} = (-1)^{(2q-2)/2} = (-1)^{2q-1} = -1,$$

Для чисел Ферма

$$\left(\frac{1}{p}\right) = (-1)^{(p-1)/2} = (-1)^{2^{2t}/2} = 1.$$

Таким образом, полином $x^2 + 1$ неприводим над полем $GF(2^q - 1)$ и приводим над полем $GF(2^{2^t} + 1)$. Это дает возможность построить комплексные поля $GF(p^2)$ только над конечными полями Галуа $GF(2^q - 1)$ [111], что означает невозможность использования для определения поля Z_p^c чисел Ферма.

Порядок $N_{\max}$ мультипликативной группы M $GF(p^2)$ равен $N_{\max} = 2^{q+1}(2^{q-1} - 1)$. Так как это число содержит множитель $2^{q+1} = N$, то может существовать корень $\sqrt[N]{1} = \varepsilon$ и можно построить характеры циклической группы G_N над полем $GF(p^2)$. Поскольку делителями числа 2^{q+1} могут быть числа вида 2^k, где $1 \leqslant k \leqslant q + 1$, можно воспользоваться обычным алгоритмом быстрого преобразования Фурье.

Пусть α — примитивный элемент из $GF(p^2)$. Тогда образующая (генератор) мультипликативной группы MGF из 2^{q+1} элементов задается выражением

$$\varepsilon = \alpha^{2^{q+1-N}(2^{q-1} - 1)}.$$

Для нахождения конкретных значений ε полезны следующие теоремы, доказанные в [198, 210].

Теорема 4.2. Если p — простое число Мерсенна и $N = 2^k$, где $1 \leqslant k \leqslant q + 1$, то $\varepsilon = a + ib$ является примитивным элементом порядка N из $GF(p^2)$ тогда и только тогда, когда

$$\varepsilon^{N/2} = (a + ib)^{N/2} \equiv -1 \pmod{p}.$$

Доказательство. Если $\varepsilon^N \equiv 1 \pmod{p}$, то $\varepsilon^{N/2} = \pm 1 \pmod{p}$. По предположению порядком ε является N, поэтому

$\varepsilon^{N/2} \not\equiv 1 (\mathrm{mod}\ p)$. Отсюда

$$\varepsilon^{N/2} = (a + ib)^{N/2} = -1 (\mathrm{mod}\ p). \tag{4.8}$$

Пусть N не является наименьшим положительным числом, для которого это справедливо. Тогда существует $l = 2^n = N_1$, $n < k$, такое, что $\varepsilon^l \equiv 1 (\mathrm{mod}\ p)$. Допустим, $n = \text{НОД}\ (N_1,\ l)$. Тогда $N_x + l_y = n$ для некоторых x, y и

$$\varepsilon^n = \varepsilon^{Nx+ly} = (\varepsilon^N)^x (\varepsilon^l)^y = 1^x \cdot 1^y = 1.$$

Так как $n < N$, то n делит $N/2$. Поэтому $\varepsilon^{N/2} \equiv 1 (\mathrm{mod}\ p)$, что противоречит (4.8). Значит, теорема доказана.

Теорема 4.3. Для простых чисел Мерсенна ($p > 3$) первым квадратичным невычетом по модулю p в последовательности 1, 2, 3,... ..., $p - 1$ является 3.

Доказательство. Рассмотрим последовательность 1, 2, 3,..., $p - 1$. Последовательно проверяем числа в этом ряду до тех пор, пока не обнаружим первый квадратичный невычет:

$$\left(\frac{2}{2^q - 1}\right) = (-1)^{[(2^q-1)^2-1]/8} = (-1)^{2q+1(2^{q-1}-1)/8} = 1;$$

$$\left(\frac{3}{2^q - 1}\right) = \left(\frac{(2^q - 1) \bmod 3}{3}\right)(-1)^{(3-1)/2} = \left(\frac{1}{3}\right)(-1) = -1.$$

Для нахождения примитивного элемента ε в $\mathrm{GF}(p^2)$ можно использовать следующую процедуру. Допустим, элемент $\varepsilon = a + ib$ является элементом порядка 2^{q+1} в $\mathrm{GF}(p^2)$. Тогда

$$(a + ib)^{2q} = (a + ib)\,(a + ib)^{2^{q-1}}.$$

По теореме бинома

$$(a + ib)^{2^{q-1}} = \sum_{i=0}^{2^{q-1}} \binom{2^{q-1}}{i} a^{2^{q-1}-i} b^i.$$

Поскольку все биноминальные коэффициенты делятся на $2^q - 1$,

$$(a + ib)^{2^q} \equiv (a + ib)\,(a + i^{2^{q-1}} b) \bmod p.$$

Однако $i^{2^{q-1}} \equiv -i (\mathrm{mod}\ p)$. Следовательно,

$$(a + ib)^{2q} = (a^2 + b^2) \bmod p.$$

Согласно теореме 4.2, из этого следует, что

$$(a + ib)^{2q} = a^2 + b^2 = -1 (\mathrm{mod}\ p). \tag{4.9}$$

Допустим $X \equiv a^2 (\mathrm{mod}\ p)$ и пусть $Y = -b^2 (\mathrm{mod}\ p)$. Тогда (4.9) примет вид

$$X + 1 \equiv Y \bmod p. \tag{4.10}$$

Согласно (4.10) X является квадратичным вычетом. Для Y имеем

$$(Y/p) = (-b^2/p) = (-1/p)\,(b^2/p) = (-1/p) = (-1)^{(2^{q-1}-1)/2} = -1.$$

Таким образом, $Y = X + 1$ является квадратичным невычетом.

Следовательно, один путь выбора чисел X и Y заключается в том, чтобы в качестве X и Y выбирать два последовательных числа из ряда целых 1, 2, 3, ..., $2^q - 2$, так что первое число X является, а второе число не является квадратом. С помощью теоремы 4.2 можно прийти к выводу, что для $p > 3$ $Y = 3$ не является, а предыдущий элемент является квадратом. Таким образом, этого достаточно, чтобы предположить, что

$$a^2 \equiv X \equiv 2 \bmod (2^q - 1); \qquad (4.11)$$
$$b^2 \equiv -X - 1 \equiv -Y \equiv -3 \bmod (2^q - 1).$$

Решение этой системы уравнений предложено в [198] и заключается в следующем. Так как $\left(\frac{2}{2^q - 1}\right) \equiv 1$, то с помощью теоремы Эйлера находим, что $2^{(p-1)/2} \equiv 1 \bmod p$. Умножив обе части сравнения на 2, получим

$$2^{(2^q-2)/2+1} = 2^{2^q-1} \equiv 2 \bmod p. \qquad (4.12)$$

Следовательно, $(2^{2^q-2})^2 = 2 \bmod (2^q - 1)$. Таким образом, решением (4.11) является

$$a = \pm 2^{2^q-2} \bmod (2^q - 1). \qquad (4.13)$$

Используя этот метод для (4.12), находим

$$b = \pm (-3)^{2^q-2} \bmod (2^q - 1).$$

В мультипликативной группе MGF поля GF(p^2) всегда существует примитивный элемент $\varepsilon = a + ib$ порядка N, для которого

$$(a + ib)^{N/2} = -1 \bmod p. \qquad (4.14)$$

Возведем обе части (4.14) в j-ю степень:

$$[(a + ib)^{N/2}]^j = (-1)^j \pmod p.$$

Элемент $[(a + ib)^{N/2}]^j$ будет примитивным элементом тогда и только тогда, когда j — нечетное число. Подобные элементы различны и включают все примитивные элементы порядка N. Другими словами, если $a + ib$ — примитивный элемент в циклической подгруппе MGF из GF(p^2), тогда $(a + ib)^j$ также является примитивным элементом для $j = 1, 3, 5, \ldots$. Мы рассмотрели случай, когда ε — элемент порядка 2^{q+1}. Если N делит 2^{q+1}, то $\alpha = \varepsilon^{\frac{2^{q+1}}{N}}$ является элементом порядка N. Теорема доказана.

Для того чтобы выполнить умножения на степени $\varepsilon = a + ib$, в арифметическом устройстве желательно представить q-битовые слова a и b минимальной суммой из степеней двойки. Тогда ε^{n+1} по ε^n может быть получено с помощью умножения ε^n на ε по mod p посредством рекурсивного использования минимального числа сдвигов двоичных разрядов и сложений.

Пример 4.2. [198]. Найдем все примитивные элементы, определенные как сумма степеней 2 в подгруппе MGF из $GF(p^2)$, где $p = 2^5 - 1 = 31$, $q = 5$, $N = 2^3 = 8$.

Прежде всего определим элемент порядка $2^{q+1} = 2^6 = 64$ в $GF(31^2)$. По утверждению теоремы 4.2, если $\varepsilon = a + ib$ — примитивный элемент порядка 2^6 в MGF из $GF(31^2)$, то

$$(a + ib)^{32} = -1 \pmod{31}. \tag{4.15}$$

Учитывая (4.9), получаем

$$a^2 + b^2 = -1 \pmod{31}. \tag{4.16}$$

С помощью (4.13) имеем

$$a \equiv 2^{2^5-2} \equiv 2^8 \equiv 8 \bmod 31; \quad b \equiv (-3)^{2^5-2} \equiv 20 \bmod 31.$$

Таким образом, 64 является таким наименьшим положительным целым, что $(8 + i20)^{64} \equiv 1 \bmod 31$. Элемент порядка $2^{q+1}/N = 8$ имеет вид $(8 + i20)^8 = (24 + i4) \bmod 31$.

Четыре примитивных элемента в подгруппе M_8 из MGF будут иметь следующий вид:

$$(27 + i4) = (2^5 - 2^2 - 2^0) + i2^2 \pmod{31};$$

$$(27 + i4)^3 = (4 + i4) = 2^2 + i2^2 \pmod{31};$$

$$(27 + i4)^5 = (4 + i27) = 2^2 + i(2^5 - 2^2 - 2^0) \pmod{31};$$

$$(27 + i4)^7 = (27 + i27) = (2^5 - 2^2 - 2^0) + i(2^5 - 2^2 - 2^0) \pmod{31}.$$

Отсюда следует, что $\varepsilon = 4 + i4$ имеет наименьшее число членов степени 2. Этот примитивный элемент является таким, что умножение на степени ε из $MGF(31^2)$ дает наименьшее количество арифметических операций. Такие ε названы в работе [198] простейшими примитивными элементами.

Нетрудно подсчитать, что общее количество операций умножения, необходимых для выполнения быстрого комплексного ТЧП, равно величине $N \log_2 N$, т. е. такое же, как и в обычном быстром преобразовании Фурье над полем комплексных чисел. Правда, здесь имеется возможность несколько снизить эту величину за счет использования простейших примитивных элементов. Подобный алгоритм описан в работе [209]. Оказалось, что N должно иметь вид $2^k q$, где $1 \leqslant k \leqslant q + 1$.

Покажем, что это действительно так. Порядок мультипликативной группы MGF (p^2) равен $t = 2^{q+1}(2^{q-1} - 1)$. Так как $2^k \mid 2^{q+1}$, необходимо показать, что $q \mid 2^{q-1} - 1$. По теореме Ферма $2^{q-1} \equiv 1 \pmod{q}$. Значит, $2^{q-1} - 1 \equiv 0 \pmod{q}$, т. е. $q \mid 2^{q-1} - 1$. Таким образом, $2^{q+1}(2^{q-1} - 1)$ имеет множители вида $N = 2^{q+1}q$. Это означает, что можно определить характеры группы $G_{2^k q}$, где $1 \leqslant k \leqslant q + 1$. Найдем корень $\sqrt[2^k q]{1} = \varepsilon$. Для этого допустим, что известен примитивный элемент $\theta = a + ib$ порядка $2^{q+1}(2^{q-1} - 1)$. Тогда

для него должно быть

$$\theta^{2q+1}(2^{q-1}-1)/2 \equiv -1 \pmod{p};$$

$$\varepsilon = \theta^{2q+1-k(2^{q-1}-1)/q}.$$

Естественно, что ε^j являются примитивными порядка T элементами в MGF (p^2) для всех j, взаимно простых с $2^{q+1-k}(2^{q-1}-1)$. Пусть теперь $T = N_1 N_2 \ldots N_n$ — разложение числа $T = 2^k q$, где $N_i = 2, 2^2, 2^3$ для $i = 1, 2, \ldots, n-1$ и $N_n = 8q$. Покажем, что каждый $\varepsilon_i = \sqrt[N_i]{1}$ является степенью 2 по модулю p для $i = 1, 2, \ldots, n$. Пусть $\varepsilon = \sqrt[T]{1}$. Тогда

$$\varepsilon^{T/2} \equiv -1 \pmod{p}. \tag{4.17}$$

Однако

$$(1+i)^{4q} \equiv (-4)^q \equiv -1 \pmod{p}, \tag{4.18}$$

где $p = 2^q - 1$. Поэтому $1 + i$ является элементом порядка $8q$. Объединяя (4.17) и (4.18), получаем

$$\varepsilon^{T/8q} \equiv 1 + i \pmod{p}. \tag{4.19}$$

Заметим, что четные степени $\varepsilon^{T/8q}$ являются степенями $2i$ по mod p, т. е. $(\varepsilon^{T/8q})^2 = \varepsilon^{T/4q} = 2i \pmod{p}$, $\varepsilon^{T/2q} = (2i)^2 \pmod{p}$, $(\varepsilon^{T/8q})^6 = (\varepsilon^{T/4q})^3 = (2i)^3$ и т. д. Из (4.17) следует, что

$$\varepsilon^{T/4} \equiv \pm i \pmod{p}. \tag{4.20}$$

Таким образом, степени $\varepsilon^{T/4}$ являются числами i, $-i$, 1, -1.

Так как $(1 \pm i)^2 = \pm 2i$, то, умножая обе части этого равенства на единицу, которую можно представить в виде 2^{q-1}, получаем

$$2^{(q-1)/2}(1 \pm i) = \sqrt{\pm 2i}. \tag{4.21}$$

Поэтому

$$\varepsilon^{T/8} = 2^{(q-1)/2}(1 \pm i). \tag{4.22}$$

Используя (4.17), (4.20), (4.21), (4.22), имеем

$$\varepsilon^{T/2} = \sqrt[2]{1} = -1; \quad \varepsilon^{T/4} = \sqrt[4]{1} = \pm i; \quad \varepsilon^{T/8} = \sqrt[8]{1} = 2^{(q-1)/2}(1 \pm i);$$

$$\varepsilon^{T/8q} = \sqrt[8q]{1} = 1 + i.$$

Таким образом, умножения на $\varepsilon = \sqrt[N_i]{1}$ для N_i, равных 2; 4; 8; $8q$, могут быть выполнены просто с помощью циклических сдвигов вместо умножений. Следовательно, в быстром ТЧП каждое N_i-точечное ТЧП может быть выполнено без комплексных умножений. Однако фазовые вращатели, связывающие эти N_i-точечные ТЧП, будут иметь нетривиальные множители, снижающие в целом быстродействие комплексного ТЧП.

Рассмотрим метод вычисления первообразного примитивного элемента. По определению элемент $\varepsilon = a + ib$, имеющий максималь-

но возможный период, равный p^2-1, называется первообразным примитивным элементом. Для него должны быть справедливы сравнения

$$(a+ib)^{p^2-1} \equiv 1 \pmod{p}; \tag{4.23}$$

$$(a+ib)^{(p^2-1)/2} \equiv -1 \pmod{p}. \tag{4.24}$$

Распишем левую часть (4.23) следующим образом:

$$[(a+ib)^{p+1}]^{p-1} = [(a+ib)^p (a+ib)]^{p-1}.$$

Но $(a+ib)^p = a + i^p b$, $i^p = -i$. Тогда

$$(a+ib)^{p^2-1} = (a^2+b^2)^{p-1} \equiv 1 \pmod{p}.$$

Аналогично

$$(a^2+b^2)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Это значит, что задача нахождения первообразного примитивного элемента $(a+ib) \in \mathrm{GF}(p^2)$ поля $\mathrm{GF}(p^2)$ сведена к определению такого же элемента, т. е. первообразного примитивного $\sqrt[p-1]{1} \in \mathrm{GF}(p)$ поля $\mathrm{GF}(p)$.

Теорема 4.4. Пусть $c \in \mathrm{GF}(q)$. Тогда существуют такие $a, b \in \mathrm{GF}(q)$, что $c = a^2 + b^2$.

Доказательство. Если $q = 2^m$, то $c^{2^m} = c$ и поэтому $c = (c^{2^{m-1}})^2 + 0^2$. Если q — нечетное, то $\mathrm{GF}(q)$ можно разбить на два подмножества:

$$\mathrm{GF}(q) = \{0, a_1, a_2, \ldots, a_{(q-1)/2}\} \cup \{-a_1, -a_2, \ldots, -a_{(q-1)/2}\} \neq \phi.$$

Поэтому в поле $\mathrm{GF}(q)$ существуют все $(q+1)/2$ квадратов, а именно $\{0, a_1^2, a_2^2, \ldots, a_{(q-1)/2}^2\}$. Из этого следует, что существует также $(q+1)/2$ элементов формы $c - b^2$ для фиксированного $c \in \mathrm{GF}(q)$. Поэтому

$$\{a^2 \mid a \in \mathrm{GF}(q)\} \cap \{(c - b^2) \mid b \in \mathrm{GF}(q)\} \neq \phi.$$

Значит, найдется такая пара a, b для заданного c, что $a^2 + b^2 = c$.

Теорема 4.5 [210]. Если 3 является примитивным элементом в $\mathrm{GF}(p)$, где $p = 2^q - 1$, то сравнение $a^2 + b^2 \equiv 3 \pmod{p}$ имеет решение

$$a = 2^{(q-1)/2} + 1, \quad b = 2^{(q-1)/2} - 1.$$

В том случае, когда примитивный элемент имеет другое численное значение, необходимо решать уравнение $a^2 + b^2 = c$. В табл. 29 для примера приведены примитивные элементы в $\mathrm{GF}(p^2)$ и в $\mathrm{GF}(p)$.

В заключение приведем еще один алгоритм определения примитивного элемента в поле $\mathrm{GF}(p^2)$. До сих пор рассматривались поля, порожденные неприводимым полиномом $x^2 + 1 = 0$. Однако, поскольку этот полином не является примитивным, степени его корня не накрывают всю мультипликативную группу поля $\mathrm{GF}(p^2)$.

Таблица 29. **Примитивные элементы в поле GF (p^2) и GF (p)**

q	$g = 2^q - 1$	Примитивный элемент	$a^2+b^2 \pmod p$	Примитивный элемент в GF (p^2)
3	7	3	3^2+1^2	$3+1\cdot i$
5	31	3	5^2+3^2	$5+3\cdot i$
7	127	3	9^2+7^2	$5+7\cdot i$
13	32 767	17	4^2+1^2	$4+1\cdot i$
17	131 071	3	257^2+255^2	$257+255\cdot i$
19	542 287	3	513^2+511^2	$513+511\cdot i$
31	2 147 483 647	53	7^2+2^2	$7+2\cdot i$

Если $\varepsilon = a + ib$ — примитивный корень, то он должен быть корнем неприводимого примитивного полинома. Найдем этот полином. Пусть ε удовлетворяет полиному

$$x^2 + mx + n = 0. \tag{4.25}$$

Подставляя вместо x элемент $\varepsilon = a + ib$, получаем

$$a^2 - b^2 + ma + i(2ab + mb) = 0,$$

откуда $m = -2a$; $n = a^2 + b^2$ или

$$a = -m/2; \quad b = \sqrt{n - m^2/4}. \tag{4.26}$$

Решая эти уравнения совместно, находим вид уравнения (4.25):

$$x^2 - 2ax + (a^2 + b^2) = 0.$$

Если известен хоть один примитивный неприводимый полином (4.25), то из него можно определить числа a и b, т. е. искомый элемент $\varepsilon = a + ib$.

4. Χ-Преобразования над прямой суммой полей Галуа GF (p^2) и над конечными гиперкомплексными системами

Воспользуемся результатами китайской теоремы об остатках для определения Χ-преобразований над прямой суммой комплексных полей GF(p^2). Используемый метод аналогичен методу определения Χ-преобразований над прямыми суммами простых полей Галуа (см. параграф 2 настоящей главы).

Пусть Z_m — кольцо классов вычетов по модулю m. Значение m имеет каноническое разложение $m = p_1 p_2 \ldots p_n$, где p_i ($i = 1, 2, \ldots, n$) — простые числа. Пусть полином $x^2 + 1$ неприводим над кольцом Z_m. Построим кольцо $Z_m[x]/x^2 + 1$. Если i — корень уравнения $x^2 + 1 = 0$, то кольцо $Z_m[x]/x^2 + 1$ изоморфно кольцу $Z_m[i]$. Первое кольцо

состоит из полиномов первой степени $\{ax + b \mid a,b \in Z_m\}$, все операции в котором происходят по модулю $x^2 + 1$, второе кольцо состоит из элементов $\{ai + b \mid a,\ b \in Z_m\}$, все операции в котором осуществляются с учетом того, что $i^2 = -1$. Для нас более удобной будет интерпретация кольца $Z_m[x]/x^2 + 1$ как кольца $Z_m[i]$. В этом случае говорят, что кольцо $Z_m[i]$ получается расширением кольца Z_m присоединением к нему корня i неприводимого полинома $x^2 + 1$.

Теорема 4.6. Кольцо $Z_m[i]$ изоморфно прямой сумме комплексных полей Галуа $\mathrm{GF}(p_i^2)$, т. е.

$$Z_m[i] \sim \mathrm{GF}(p_1^2) \dotplus \mathrm{GF}(p_2^2) \dotplus \cdots \dotplus \mathrm{GF}(p_n^2),$$

если $x^2 + 1$ неприводим над каждым полем $\mathrm{GF}(p_i^2)$, $i = 1, 2,\ldots, n$.

Доказательство. Пусть $a + ib \in Z_m[i]$. Определим отображение

$$\Psi : a + ib \mapsto (a_1 + ib_1 \pmod{p_1},\ a_2 + ib_2 \pmod{p_2},\ \ldots$$
$$\ldots,\ a_n + ib_n \pmod{p_n}).$$

Так как $x^2 + 1$ неприводим над каждым полем $\mathrm{GF}(p_i^2)$, $i = 1, 2,\ldots, n$, то остаток $a_k + ib_k$ принадлежит $\mathrm{GF}(p_k^2)$ для всех $k = 1, 2,\ldots, n$. Следовательно, Ψ является отображением кольца $Z_m[i]$ в прямую сумму полей $\mathrm{GF}(p_i^2)$:

$$\Psi : Z_m[i] \mapsto \mathrm{GF}(p_1^2) \dotplus \mathrm{GF}(p_2^2) \dotplus \cdots \dotplus \mathrm{GF}(p_n^2).$$

Если $z_1 = a^1 + ib^1$ и $z_2 = a^2 + ib^2$ — произвольные элементы в $Z_m[i]$, то

$$\Psi(z_1 + z_2) = \Psi((a^1 + a^2) + i(b^1 + b^2)) = ([(a^1 + a^2) + i(b^1 + b^2)] \bmod p_1;$$
$$[(a^1 + a^2) + i(b^1 + b^2)] \bmod p_2,\ \ldots,\ [(a^1 + a^2) + i(b^1 + b^2)] \bmod p_n) =$$
$$= ((a^1 + ib^1) \bmod p_2 + (a^2 + ib^2) \bmod p_1,\ (a^1 + ib^1) \bmod p_2 +$$
$$+ (a^2 + ib^2) \bmod p_2,\ \ldots,\ (a^n + ib^n) \bmod p_n + (a^2 + ib^2) \bmod p_n) =$$
$$= (a^1 + ib^1 \pmod{p_1},\ a^1 + ib^1 \pmod{p_2},\ \ldots,\ a^1 + ib^1 \pmod{p_n}) +$$
$$+ (a^2 + ib^2 \pmod{p_1},\ (a^2 + ib^2) \bmod p_2,\ \ldots,\ (a^2 + ib^2) \bmod p_n) =$$
$$= \Psi(z_1) + \Psi(z_2).$$

Аналогично доказывается равенство $\Psi(z_1\ z_2) = \Psi(z_1)\Psi(z_2)$. Таким образом, отображение Ψ является гомоморфизмом. Если ограничить отображение Ψ только на действительную часть (или мнимую), то оно перейдет в изоморфизм $\Psi_{\text{ог}}$, связывающий Z_m и $\mathrm{GF}(p_1) \dotplus \mathrm{GF}(p_0) \dotplus \ldots \dotplus \mathrm{GF}(p_n)$. Это доказывает, что Ψ также является изоморфизмом.

Теорема 4.7. Пусть N делит $p_i^2 - 1$ для всех $i = 1,2,\ldots, n$. Тогда существует χ-преобразование в пространстве всех функций, заданных на циклической группе G_N и принимающих значения в кольце $Z_m[i]$.

Доказательство. Так как N делит $p_i^2 - 1$ для всех $i = 1, 2,\ldots, n$, то во всех полях $\mathrm{GF}(p_i^2)$ существуют примитивные кор-

ни ε_i из единицы. Поэтому элемент $\Psi^{-1}(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n) = \varepsilon$ соответствует примитивному корню N-й степени из единицы в $Z_m[i]$ и наоборот. Отсюда следует, что на N точках существуют прямое и обратное χ-преобразования над $Z_m[i]$:

$$S(\alpha) = \sum_{n=0}^{N-1} x(n)\,\varepsilon^{-\alpha n}, \quad x(n) = N^{-1} \sum_{\alpha=0}^{N-1} S(\alpha)\,\varepsilon^{\alpha n}, Z_m[i]. \qquad (4.27)$$

Существование обратного N^{-1} в $Z_m[i]$ гарантируется тем, что $(N, p_i) = 1$, $i = 1, 2, \ldots, n$. Отсюда следует, что и НОК $(N, m) = 1$, т. е. N принадлежит мультипликативной группе кольца Z_m, а значит, и мультипликативной группе кольца $Z_m[i]$.

Согласно теореме 4.7, N-точечное χ-преобразование может быть непосредственно использовано для вычисления спектра $S(\alpha)$. Однако такое непосредственное вычисление может потребовать длину слова бо́льшую, чем у ЦВМ. Этого можно избежать, применяя к паре уравнений (4.27) преобразование Ψ:

$$\left.\begin{aligned} S_1(\alpha) &= \sum_{n=0}^{N-1} x_1(n)\,\varepsilon_1^{-\alpha n}, \quad x_1(n) = N^{-1} \sum_{\alpha=0}^{N-1} S_1(\alpha)\,\varepsilon_1^{\alpha n}, \ \mathrm{GF}(p_1^2); \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ S_n(\alpha) &= \sum_{n=0}^{N-1} x_1(n)\,\varepsilon_1^{-\alpha n}, \quad x_1(n) = N^{-1} \sum_{\alpha=0}^{N-1} S_1(\alpha)\,\varepsilon_1^{\alpha n}, \ \mathrm{GF}(p_n^2). \end{aligned}\right\} \qquad (4.28)$$

При этом сумматор должен иметь такую длину разрядной сетки, при которой он позволяет суммировать числа с числом разрядов, не превышающим $\lfloor \log(\max p_i) \rfloor$, что значительно меньше, чем в том случае, когда требуется суммировать числа, каждое из которых представляется с помощью $\lfloor \log m \rfloor$ разрядов.

По аналогии с χ-преобразованиями, определяемыми над конечным полем целых комплексных чисел, определяются преобразования над конечным кольцом кватернионов Z_p^H и конечным неассоциативным кольцом чисел Кэли Z_p^k.

Определение 4.1. χ-Преобразование в пространстве $L(G_N, Z_p^H)$, матрица $\chi_\alpha(n)$ которого образуется с помощью элемента $h = a + ib + jc + kd$, назовем ТЧП над конечным кольцом кватернионов.

Очевидно, что при $c = 0$ и $d = 0$, или при $l = 0$ и $d = 0$, или при $b = 0$ и $c = 0$ ТЧП над Z_p^H совпадают с ТЧП Z_p^c, т. е. с комплексными ТЧП.

Определение 4.2. χ-Преобразование в пространстве $L(G_N Z_p^k)$, матрица $\chi_\alpha(n)$ которого образуется с помощью числа Кэли $\xi = \gamma + he$, называется ТЧП над конечным неассоциативным кольцом чисел Кэли.

Если $h = 0$, то ТЧП над Z_p^k совпадает с ТЧП над Z_p^H.

С помощью введенных ТЧП над Z_p^H и Z_p^k можно вести обработку сигналов, задаваемых последовательностями комплексных и гиперкомплексных чисел.

Упражнение 4.3. Найти степени первообразного элемента ε вида $\varepsilon_1 = a + ib + jc$ ($\varepsilon_1 \in Z_7^H$). Сопоставить со степенями элемента $\varepsilon_2 = a + ib + jc + kd$ ($\varepsilon_2 \in Z_7^H$).

Точно так же, как комплексное ТЧП, ТЧП над Z_p^H и Z_p^k можно определить при выборе в качестве модуля p простого числа Мерсенна и нельзя модуль выбирать равным числу Ферма. Основной трудностью при определении ТЧП над Z_p^H и Z_p^k является выбор первообразного корня из единицы $\sqrt[N]{1} \in Z_p^H$ и $\sqrt[N]{1} \in Z_p^k$ заданного порядка N в связи с отсутствием эффективных методов нахождения таких корней. Практически первообразные элементы в Z_p^H и Z_p^k можно найти с помощью перечислительных методов на ЭВМ. В этой связи ТЧП над Z_p^H и Z_p^k представляют определенный интерес. Главное достоинство этих преобразований заключается в том, что операция умножения элементов колец Z_p^H и Z_p^c выполняется проще по сравнению с выполнением операции умножения элементов поля $\mathrm{GF}(p^4)$ и $\mathrm{GF}(p^8)$. Заметим, что при выборе в качестве неприводимого полинома многочлена $y = x^2 + 1$ Z_p^H совпадает с $\mathrm{GF}(p_4)$, а Z_p^k — с $\mathrm{GF}(p^8)$. Это объясняется тем, что операция в $\mathrm{GF}(p^4)$ и $\mathrm{GF}(p^8)$ выполняется по модулю неприводимого многочлена, что связано с операцией деления многочленов, и реализуется с определенными трудностями [42, 69, 70].

Выше описывались различные разновидности χ-преобразований, определенных над конечными алгебраическими системами, обладающими структурой кольца. χ-Преобразования в пространстве $L(G_N, K)$ (K — произвольное конечное кольцо) являются ортогональными преобразованиями, свойства которых изоморфны свойствам преобразований в пространстве $L(G_N, C)$. По аналогии можно в пространстве $L(G_N, K)$ определить другие преобразования, аналогичные некоторым преобразованиям в пространстве $L(G_N, C)$. Например, в пространстве $L(G_N, K)$ можно определить функции, аналогичные известным в пространстве $L(G_N, C)$ функциям $y = \sin x$, $y = \cos x$, и другие функции и преобразования [87, 193].

Пусть ε — первообразный примитивный корень мультипликативной группы кольца K. Обозначим через i произвольный квадратичный невычет в кольце K, т. е. такой элемент в K, что $i^2 = 1$. Отметим, что в некоторых кольцах таких элементов может и не быть, а в некоторых может быть и несколько.

Упражнение 4.4. Найти квадратичные невычеты в кольце Z_9 и в поле GF(13). В поле комплексных чисел свойствами квадратичного невычета обладает один элемент — мнимая единица.

Определение 4.3 [87]. Функции, задаваемые равенствами

$$\mathrm{sig}\,\varphi = (\varepsilon^{i\varphi} - \varepsilon^{-i\varphi})/2i; \tag{4.29}$$

$$\mathrm{cog}\,\varphi = (\varepsilon^{i\varphi} + \varepsilon^{-i\varphi})/2, \tag{4.30}$$

называются соответственно синусом и косинусом Галуа с мнимой единицей i.

Упражнение 4.5. Построить график функций $y = \mathrm{sig}\ \varphi$ и $y = \mathrm{cog}\ \varphi$, определенных в поле GF (13) и в поле GF(29), выбрав подходящие значения ε и i.

Определение 4.4 [87]. Функции, задаваемые равенствами

$$\mathrm{shg}\,(\varphi) = (\varepsilon^{\varphi} - \varepsilon^{-\varphi})/2; \tag{4.31}$$

$$\mathrm{chg}\,(\varphi) = (\varepsilon^{\varphi} + \varepsilon^{-\varphi})/2, \tag{4.32}$$

называются соответственно гиперболическими синусом и косинусом Галуа.

Точно так же можно ввести аналогии функций $y = e^x$ и $y = \ln x$ в конечных кольцах. Функции $y = e^x$ соответствует функция $y = \varepsilon^x$, x, y, $\varepsilon \in K$; функции $y = \ln x$ — функция $y = \mathrm{lng}\, x$, причем выполняется равенство $\varepsilon^y = x$. Свойства приведенных выше функций, определенных в кольце K, изоморфны свойствам аналогичных функций, определенных в поле комплексных чисел. Подобным образом можно определить и другие функции, которые необходимо или удобно использовать при построении математических моделей.

* * *

Следует выделить основные особенности Х-преобразований, определенных над конечным полем или кольцом, которые отличают их от Х-преобразований, определенных над полем комплексных чисел. К положительным качествам в первую очередь необходимо отнести снижение объема вычислений при реализации, связанное с более простой арифметикой конечных колец по сравнению с арифметикой поля комплексных чисел. Кроме того, легко увидеть следующие преимущества: в силу специфики арифметики конечных полей и колец отсутствует шум округлений; при машинных вычислениях сохраняются ассоциативный и коммутативный законы арифметических операций суммы и умножения по модулю, а также дистрибутивный закон операции умножения по отношению к сложению. Это обеспечивает разработку эффективных алгоритмов ЦОС.

Отрицательными являются следующие свойства Х-преобразований:

выбор матриц преобразований $\chi_\alpha\,(n)$ заданной размерности $N \times N$ связан с поиском и выбором первообразного корня и единицы порядка N. Если над полем комплексных чисел существует первообразный корень из единицы порядка N для любых целых N, то в конечном поле или кольце порядок первообразного корня из единицы пробегает далеко не все целочисленные значения, не превышающие порядка этого поля или кольца. Получить заданный порядок первообразного элемента можно выбором соответствующего конечного поля или кольца, т. е. выбором соответствующего значения модуля M. Однако не для каждого значения M возможна эффективная реализация с помощью двоичной схемотехники;

естественный модуль арифметического устройства ЦВМ $m = 2^n$ не подходит для выбора в качестве порядка конечного кольца, так как m должно быть либо простым, либо разлагается на простые сомножители, наименьший общий делитель которых должен быть на единицу большим N. Следовательно, необходима разработка арифметических устройств с модулем, отвечающим требованиям, вытекающим из условий определения Χ-преобразований.

Однако преимущества, связанные со снижением объема вычислений, делают отмеченные недостатки несущественными. Мы уже видели, что существуют такие числа M, операции суммы и умножения по модулю которых можно эффективно реализовать как программным путем с помощью обычных ЦВМ, так и с помощью специализированных устройств. Недостаток, связанный с ограничениями на размерность матрицы Χ-преобразований, в некоторой степени компенсируется использованием конечных полей и колец различной структуры (например, рассмотренные конечное поле комплексных чисел, конечные гиперкомплексные системы и др.). Кроме того, на практике размерность матрицы Χ-преобразований выбирают из ограниченного числа значений. Чаще всего N равняется степени 2 в пределах от 4 до 1024.

ГЛАВА 5

ПРЕОБРАЗОВАНИЕ ГАУССА

1. Общие положения

Пусть анализу на ЦВМ подвергаются комплексные сигналы $z(t)$. Тогда их квантованные значения $z(n)$ можно рассматривать как функцию, заданную на группе целых чисел Z и принимающую значения в кольце целых комплексных чисел: $z(n) : G \to Z[i]$. Целыми комплексными числами называются числа вида $a + ib$, где $i = \sqrt{-1}$; a и b — целые числа. Такие числа образуют кольцо, которое обозначено через $Z[i]$. В этом кольце с целыми комплексными числами можно оперировать не по модулю простого целого рационального числа p, а по модулю целого комплексного числа $m = p + iq$. Это позволяет смотреть на сигнал $z(n)$ как на функцию, заданную на группе G со значениями в кольце $Z_m[i]$ классов вычетов по модулю $m = p + iq$. Естественно, что модуль m нужно выбрать настолько большим, что для тех значений, которые принимает сигнал $z(n) = x(n) + iy(n)$, законы сложения и умножения в $Z[i]$ совпадают с соответствующими законами в $Z_m[i]$. Пространство таким образом определенных сигналов обозначим через $L(G, Z_m[i])$. Приведенные соображения заставляют обратиться к изучению свойств $Z[i]$-арифметики и ей подобных арифметик.

Вся теория чисел для обыкновенных целых рациональных чисел в большой мере связана с вопросом их делимости. Целые рациональные числа очень просто составляются сложением и вычитанием из простейшего в отношении этих операций целого числа 1. Причем относительно сложения и вычитания их совокупность представляет собой бесконечную циклическую абелеву группу с образующей 1.

Несравненно сложнее ведет себя совокупность целых рациональных чисел по отношению к умножению. В этом смысле она уже не представляет группы. Основным здесь является то, что в ряду натуральных чисел содержится бесконечное число простых чисел, которые расположены в ряду всех натуральных чисел весьма неравномерно, причем любое рациональное число представляется, притом только одним способом, в виде произведения этих простых чисел и еще одной из единиц: 1 или —1.

Множество целых чисел является простейшим кольцом. Оказывается, что в произвольном коммутативном кольце может быть

построена теория чисел, аналогичная обычной, если для этого кольца справедлива теорема об однозначном разложении всякого его элемента на конечное число простых множителей.

Простейшее, после кольца целых рациональных чисел, кольцо, для которого была построена такая же теория чисел, как для рациональных чисел, есть гауссово кольцо всех целых комплексных чисел. Гаусс [50] в 1824 г. показал, что и в этом кольце также есть в бесконечном числе простые числа и что всякое заданное число этого кольца также представляется одним и только одним способом в виде произведения конечного числа этих простых и еще одной из четырех, так называемых, единиц $(1,\ i-1,\ -i)$ кольца $Z[i]$. Однако в других кольцах, хотя с виду и совершенно аналогичных гауссовому, например в кольце чисел $a+b\sqrt{-5}$ или $a+b\sqrt{-11}$, а тем более в более сложных кольцах, теорема об однозначном разложении на множители не справедлива. Хотя в них и есть такие числа, которые не распадаются на множители из данного кольца, так сказать «простые» числа, однако любое число кольца может быть разложено на такие «простые» множители иногда весьма многими, существенно различными способами.

Теоретико-числовые преобразования над подобными кольцами представляют большой практический интерес, но для их изучения необходим более мощный математический аппарат, чем тот, который использовался до сих пор. Его изучение выходит за рамки настоящей работы. Ниже изучается кольцо $Z_m[i]$ и ТЧП, которые можно на его основе построить.

2. Основные свойства кольца $Z[i]$

Комплексное число будем называть простым комплексным числом, если оно не может быть представлено в виде произведения двух комплексных чисел, отличных от единицы. В противном случае оно называется составным комплексным числом. Из этого определения непосредственно следует, что составное вещественное число является также и составным комплексным числом. Обратное не всегда верно: простое вещественное число может быть составным комплексным числом. Так, например, $2=(1+i)(1-i)$.

Комплексное число $\dot{A}=a+bi$ будет кратно комплексному числу $\dot{m}=p+qi$ (или $\dot{m}$ будет делителем числа $\dot{A}$), если частное $\dot{A}:\dot{m}$ является целым комплексным числом. Если

$$\frac{\dot{A}}{\dot{m}}=\frac{a+bi}{p+qi}=\frac{(a+bi)(p-qi)}{p^2+q^2}=\frac{ap+bq}{p^2+q^2}+i\,\frac{bp-aq}{p^2+q^2},$$

то $\dot{A}:\dot{m}$ будет целым числом в том и только в том случае, когда

$$\begin{aligned} ap+bq &\equiv 0 \bmod (p^2+q^2);\\ bp-aq &\equiv 0 \bmod (p^2+q^2). \end{aligned} \tag{5.1}$$

Если (5.1) не выполняется, то $\dot{A}$ не делится на $\dot{m}$. Пусть $\dot{s}=e+fi$

таково, что $\dot{A} - \dot{s}$ делится на $\dot{m}$. Тогда можно написать, что

$$s \equiv \dot{A} \pmod{\dot{m}}, \tag{5.2}$$

или s является вычетом $\dot{A}$ по модулю $\dot{m}$.

Нетрудно видеть, что сравнение (5.2) на множестве всех целых комплексных чисел задает отношение эквивалентности; оно рефлексивно, так как $\dot{s} \equiv \dot{s} \pmod{\dot{m}}$, симметрично, поскольку из $\dot{A} \equiv \dot{B} \pmod{\dot{m}}$ следует $\dot{B} \equiv \dot{A} \pmod{\dot{m}}$, транзитивно, так как из $\dot{A} \equiv \dot{B} \pmod{\dot{m}}$, $\dot{B} \equiv \dot{C} \pmod{\dot{m}}$ следует $\dot{A} \equiv \dot{C} \pmod{\dot{m}}$. Тем самым отношение $\langle \equiv \pmod{\dot{m}} \rangle$ разбивает множество всех целых комплексных чисел на непересекающиеся классы эквивалентности. Причем два целых числа сравнимы между собой по модулю $\dot{m}$ тогда и только тогда, когда они лежат в одном и том же классе. Эти классы называются классами комплексных вычетов по модулю $\dot{m}$. Взяв из каждого класса вычетов по одному представителю, получим ПСВ по модулю $\dot{m}$.

В дальнейшем целесообразно в сравнениях типа (5.2) от символа сравнения перейти к символу равенства. С этой целью ПСВ по модулю $\dot{m}$ обозначим символом $\langle \cdot |_{\dot{m}}$ или $Z_{\dot{m}}$ [i]. Операцию выделения из числа $\dot{A}$ по модулю $\dot{m}$ остатка $\dot{S}$ обозначим символом $\langle \dot{A} |_{\dot{m}}$. Иными словами, если $\dot{A} = \dot{Q}_m + S$, то $\dot{S} = \langle \dot{A} |_m$.

Для изображения ПСВ по вещественному модулю m будем использовать символ $| \cdot |_m$. Известно, что $| \cdot |_m = Z_m = \{0, 1, \ldots, m-1, \odot, \oplus \bmod m\}$. Относительно $\langle \cdot |_{\dot{m}}$ пока ничего сказать невозможно.

Прежде всего нужно выяснить вопрос о количестве элементов во множестве $\langle \cdot |_{\dot{m}}$, а потом заняться определением вида элементов этого множества. Для выяснения данных вопросов рассмотрим еще раз процедуру выделения остатка числа $\dot{A} = a + bi$ при делении на $\dot{m}$. Известно, что

$$\frac{\dot{A}}{\dot{m}} = \frac{a+bi}{p+qi} = \frac{ap+bq}{\| m \|} + i\frac{bp-aq}{\| m \|},$$

где $\| \dot{m} \|$ — норма комплексного числа, равная $p^2 + q^2$.

Зададимся некоторой ПСВ $| \cdot |_{\| \dot{m} \|}$ по вещественному модулю $\| \dot{m} \|$. Тогда сравнение (5.1) можно переписать следующим образом:

$$ap + bq = l_1 \| \dot{m} \| + | ap + bq |_{\| \dot{m} \|};$$

$$bp - aq = l_2 \| \dot{m} \| + | bp - aq |_{\| \dot{m} \|}.$$

Поэтому

$$a + bi = (l_1 + il_2)\, m + (| ap + bq |_{\| \dot{m} \|} + i\, | bp - aq |_{\| \dot{m} \|}) \frac{\dot{m}}{\| m \|}.$$

Так как $a + bi$, $l_1 + l_2 i$, $p + qi$ — целые комплексные числа, то величина $|\, ap + bq \,|_{\|m\|} + i \,|\, bc - ad \,|_{\|m\|}$ является целым комплексным числом. Следовательно, справедлива формула

$$S = <A|_m = <a + bi|_m = (|\, ap + bq \,|_{\|m\|} + c \,|\, bp - aq \,|_{\|m\|}) \frac{m}{\|m\|}, \quad (5.3)$$

из которой следует, что способ задания ПСВ по комплексному модулю зависит от способа задания ПСВ по вещественному модулю $\|m\|$.

В качестве ПСВ по вещественному модулю можно взять ПСНВ $(|\cdot|_m^+)$. В соответствии с этим ПСВ по комплексному модулю $m = p + iq$, определяемую формулой

$$<a + bi|_m^+ = (|\, ap + bq \,|_{\|m\|}^+ + i \,|\, bp - aq \,|_{\|m\|}^+) \frac{m}{\|m\|}, \quad (5.4)$$

назовем КПСНВ по комплексному модулю m. Если возьмем ПСАНВ по вещественному модулю $(|\cdot|_m^-)$, то получим КСАНВ:

$$<a + bi|_m^- = (|\, ap + bq \,|_{\|m\|}^- + i \,|\, bp - aq \,|_{\|m\|}^-) \frac{m}{\|m\|}. \quad (5.5)$$

Пример 5.1. Определим наименьший и абсолютно наименьший вычеты числа $A = a + bi = 15 + 2i$ по модулю $m = 3 + 2i$. Имеем

$$\|m\| = 3^2 + 2^2 = 13;$$

$$|\, ap + bq \,|_{13}^+ = |\, 15 \cdot 3 + 2 \cdot 2 \,|_{13}^+ = |\, 49 \,|_{13}^+ = 10;$$

$$|\, bp - aq \,|_{13}^+ = |\, 2 \cdot 3 - 15 \cdot 2 \,|_{13}^+ = |\, -24 \,|_{13}^+ = 2.$$

Кроме того,

$$|\, ap + bq \,|_{13}^- = |\, 49 \,|_{13}^- = -3; \quad |\, bp - aq \,|_{13}^- = |\, -24 \,|_{13}^- = 2.$$

Поэтому

$$<15 + 2i|_{3+2i}^+ = (15 + 2i) \bmod (3 + 2i) = (10 + 2i) \frac{3 + 2i}{13} = 2 + 2i;$$

$$<15 + 2i|_{3+2i}^- = (-3 + 2i) \frac{3 + 2i}{13} = -1.$$

Теперь можно доказать следующую теорему:

Теорема 5.1. Число элементов ПСВ по комплексному модулю $m = a + bi$ равно норме модуля m, т. е.

$$\text{card}\,(<\cdot|_m) = \text{card}\,(Z_m(i)) = \|m\| = a^2 + b^2 = N.$$

Доказательство. В соответствии с формулой (5.4) совокупность ЦКЧ $x_1 + ix_2$ образует ПСВ по модулю m тогда и только тогда, когда x_1 и x_2 являются целочисленным решением системы вида

$$px_1 + qx_2 = y_1; \quad px_2 - qx_1 = y_2, \quad (5.6)$$

где y_1 и y_2 пробегают значения некоторой ПСВ по вещественному модулю $\| m \|$. Действительно, если $x_1 + ix_2 \in <\cdot|_m$, то

$$<x_1 + ix_2|_m = x_1 + ix_2 = (|px_1 + qx_2|_{\|m\|} + i|px_2 - qx_1|_{\|m\|}) \frac{m}{\|m\|} =$$

$$= (y_1 + iy_2) \frac{m}{\|m\|}, \quad y_1, y_2 \in |\cdot|_{\|m\|}. \tag{5.7}$$

Следовательно, вопрос о числе элементов ПСВ по комплексному модулю m сводится к вопросу о числе пар (y_1, y_2), для которых система (5.6) имеет целочисленное решение. Из (5.7) следует, что

$$x_1 = \frac{py_1 - qy_2}{\|m\|}; \quad x_2 = \frac{py_2 + qy_1}{\|m\|}. \tag{5.8}$$

Поэтому поставленному требованию удовлетворяют лишь те пары (5.8), для которых выполняются сравнения

$$\begin{aligned} py_1 - qy_2 &\equiv 0 \pmod{\|m\|}; \\ py_2 + qy_1 &\equiv 0 \pmod{\|m\|}. \end{aligned} \tag{5.9}$$

Рассмотрим три принципиально различных случая.

Случай 1. $p \neq 0$, $q = 0$, $\| m \| = p^2$. Система (5.9) принимает вид:

$py_1 \equiv 0 \pmod{p^2}$; $py_2 \equiv \pmod{p^2}$, или $y_1 \equiv 0 \pmod{p}$; $y_2 \equiv 0 \pmod{p}$.

Каждое из этих сравнений имеет p различных (несравнимых по модулю p^2) решений. Действительно, числа 0, p^2, $1 \cdot p^2$, $2 \cdot p^2$, ..., $(p-1) \cdot p^2$ по модулю p^2 равны нулю, поэтому можно написать

$$\left.\begin{aligned} py_1 &= 0 \cdot p^2 \equiv 0 \pmod{p^2}; & py_2 &= 0 \cdot p^2 \equiv 0 \pmod{p^2}; \\ py_1 &= 1 \cdot p^2 \equiv 0 \pmod{p^2}; & py_2 &= 1 \cdot p^2 \equiv 0 \pmod{p^2}; \\ py_1 &= 2 \cdot p^2 \equiv 0 \pmod{p^2}; & py_2 &= 2 \cdot p^2 \equiv 0 \pmod{p^2}; \\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots & & \\ py_1 &= (p-1)\, p^2 \equiv 0 \pmod{p^2}; & py_2 &= (p-1)\, p^2 \equiv 0 \pmod{p^2}. \end{aligned}\right\} \tag{5.10}$$

Откуда получаем p решений для каждого сравнения (5.10):

$$y_1^{(0)} = 0;\ y_1^{(1)} = p;\ y_1^{(2)} = 2p, \ \ldots, \ y_1^{(p-1)} = (p-1)\, p;$$
$$y_2^{(0)} = 0;\ y_2^{(1)} = p;\ y_2^{(2)} = 2p, \ \ldots, \ y_2^{(p-1)} = (p-1)\, p.$$

Следовательно, всех пар (y_1, y_2), удовлетворяющих (5.9), будет p^2, т. е. $\| m \|$.

Случай 2. $p, q \neq 0$, причем НОД $(p, q) = 1$. В этом случае появляется возможность разрешить одно из сравнений (5.9) относительно любой переменной, поскольку НОД $(p, p^2 + q^2) = 1$ и НОД $(q, p^2 + q^2) = 1$. Разрешив, например, первое сравнение относительно y, получим

$$y_1 = \left| \frac{q}{p} y_2 \right|_{\|m\|}. \tag{5.11}$$

Придавая величине y_2 значения из ПСВ $\|\cdot\|_{\|\dot{m}\|}$, находим $\|\dot{m}\|$ различных пар чисел (y_1, y_2), удовлетворяющих первому сравнению (5.9). Но эти пары удовлетворяют и второму сравнению. Действительно, имеем

$$|py_2 + qy_1|_{\|\dot{m}\|} = \left| py_2 + q\left|\frac{q}{p}y^2\right|_{\|\dot{m}\|}\right|_{\|\dot{m}\|} = \left|\frac{1}{p}(p^2+q^2)y_2\right|_{\|\dot{m}\|} = 0.$$

Таким образом, число различных пар (y_1, y_2), удовлетворяющих (5.9), равно $\|\dot{m}\|$.

Случай 3. $\dot{m} = dm_1$, $m_1p_1 + q_1i$, причем НОД $(p, q) = 1$. В этом случае число элементов в ПСВ по комплексному модулю $\dot{m} = dm_1$ также равно $\|\dot{m}\|$. Доказательство этого утверждения [6, 7] не будем проводить, поскольку ПСВ по такому модулю в данной работе не применяется.

Рассмотрим теперь способ построения ПСВ по комплексному модулю $\dot{m} = p + iq$.

Случай 1. $q = 0$, $p \neq 0$. ПСВ описывается ЦКЧ $x_1 + ix_2$, где x_1 и x_2 независимо пробегают ПСВ $|\cdot|_p$ по вещественному модулю p. Действительно,

$$<a+ib)_m = <a+ib|_p = <a|_p + i<b|_p =$$
$$= |a|_p + i|b|_p = x_1 + ix_2.$$

Случай 2. $q \neq 0$, $p \neq 0$, НОД $(p, q) = 1$. ПСВ представляет совокупность ЦКЧ $x_1 + ix_2$, где

$$x_1 = \frac{1}{\|\dot{m}\|}\left(p\left|\frac{q}{p}r\right|^{\pm}_{\|m\|} - qr\right); \quad x_2 = \frac{1}{\|\dot{m}\|}\left(pr + q\left|\frac{q}{p}r\right|^{\pm}_{\|\dot{m}\|}\right) \quad (5.12)$$

и r пробегает значения ПСВ $|\cdot|^{\pm}_{\|\dot{m}\|}$.

Действительно, из (5.7) с учетом (5.11) и обозначения $y_2 = r$ имеем (5.12).

Пример 5.2. $\dot{m} = 3 + 0i$, т. е. $m = p = 3$, $q = 0$ (случай 1). Имеем ПСНВ

$$<\cdot|^{+}_{3} = \{0,\ 1,\ 2,\ i,\ i+1,\ 2+i,\ 2i,\ 1+2i,\ 2+2i\}$$

и ПСАНВ

$$<\cdot|^{-}_{3} = \{-1,\ 0,\ 1,\ -1,\ -i,\ -1+i,\ -i,\ 1-i,\ i,\ 1+i\}.$$

Пример 5.3. $\dot{m} = 2 + 5i$, НОД $(2, 5) = 1$, $\|\dot{m}\| = 29$ (случай 2). Имеем ПСНВ $<\cdot|^{+}_{2+5i} = x_1 + x_2i$, где $x_1 = \frac{1}{29}(2\cdot|17r|^{+}_{29} - 5r)$; $x_2 = \frac{1}{29}(2r + 5|17r|^{+}_{29})$, $0 \leqslant r \leqslant 28$, и ПСАНВ $<\cdot|^{-}_{2+5i} = x_1 + x_2i$, где $x_1 = \frac{1}{29}(2\cdot|-12r|^{-}_{29} - 5r)$; $x_2 = \frac{1}{29}(2\cdot r + 5|-12r|^{-}_{29})$, $-14 \leqslant \leqslant 2 \leqslant +14$.

Изменяя r, получаем

$$< \cdot |^{+}_{2+5i} = \{0,\ i,\ -1,\ +i,\ -2+i,\ 2i,\ -1+2i,\ -2+2i,$$
$$-3+2i,\ -4+2i,\ 1+3i,\ 3i,\ -1+3i,\ -2+3i,\ -3+3i,$$
$$-4+3i,\ 1+4i,\ 4i,\ -1+4i,\ -2+4i,\ -3+4i,\ -4+4i,$$
$$1+5i,\ 5i,\ -1+5i,\ -2+5i,\ -3+5i,\ -1+6i,\ -2+6i,$$
$$-3+6i\};$$
$$< \cdot |^{-}_{2+5i} = \{0,\ \pm i,\ \pm 2i,\ \pm 1,\ \pm 1 \pm i,\ \pm 1 \pm 2i,\ \pm 2,\ \pm 2 \pm i,$$
$$\pm 2 \pm 2i,\ 3+i,\ -1+3i,\ -3-i,\ -1-3i\}.$$

3. Геометрическая интерпретация комплексных вычетов

Рассмотрим вопрос геометрической интерпретации вычетов на комплексной плоскости (рис. 13). Точка M с координатами (p, q) изображает комплексное число $p + qi = m$. Прямая OM представляет величину $\sqrt{N}$. Сама норма $N = \| m \|$ представляется площадью квадрата, построенного на прямой OM (квадрат $ORLM$). Если всю плоскость покрыть такими квадратами (проведением прямых, параллельных соответственно OM и OR, на расстояниях $\sqrt{N}$ одна от другой), то вершинам этих квадратов будут соответствовать числа, кратные $p + qi$. Так, из условия перпендикулярности OR и OM следует, что точке R соответствует комплексное число $-q + pi$ и частное $(-q + pi)/(p + qi) = i$. Вследствие параллельности OM и RL точке L будет соответствовать комплексное число $(p - q) + (p + q)\, i$, и соответствующее частное равно $1 + i$. Пронумеруем прямые, параллельные OR и OM, номерами O (прямая OR); 1, 2, ..., l; -1, -2, ..., $-l$ и O (прямая OM); 1, 2, ..., s; -1, -2, ..., $-s$. Пусть дана вершина N_i такого квадрата, образованного l-й прямой, параллельной OR, и s-й прямой, параллельной OM. Точке N_i будет соответствовать число $l\,(p + qi) + s\,(-q + pi) = lp - sq + (lq + sp)\, i$, и частное от деления этого числа на $p + qi$ равно $l - si$. Что касается точек, лежащих внутри какого-либо квадрата или на его сторонах, но не совпадающих с его вершинами, то они представляют числа, не делящиеся на данный модуль $m = p + qi$.

Пусть даны два каких-либо квадрата **Г** и **А**. Наложим эти квадраты один на другой так, чтобы их соответствующие вершины совпадали. Назовем внутренние точки этих квадратов, совпадающие при таком наложении, конгруентными. Тогда имеет место следующая теорема.

Теорема 5.2. Числа, изображенные конгруентными точками, сравнимы между собой по модулю $p + qi$.

Для простоты возьмем в качестве одного из квадратов квадрат $ORLM$, вершина O которого совпадает с началом координат. Второй квадрат будем полагать таким, что его вершина N_i, соответствующая при наложении точке O, изображает число $(lp - sq) + (lq + sp)\, i$.

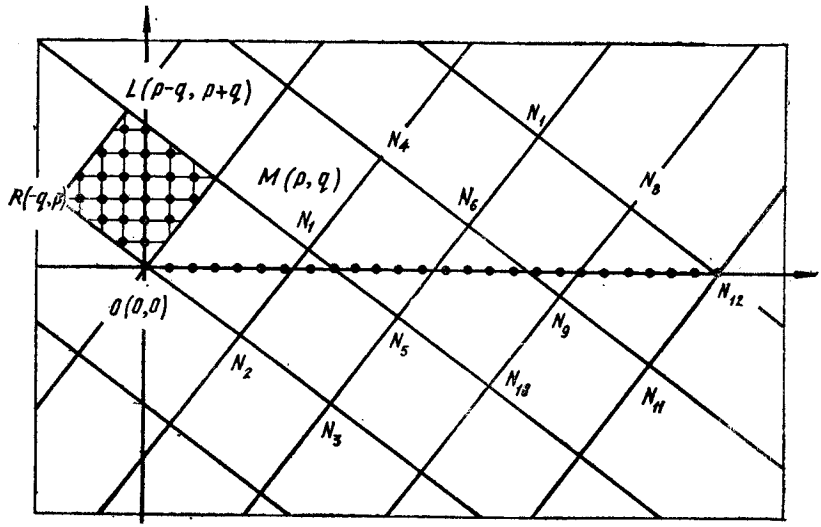


Рис. 13. Геометрическое представление ПСНВ по модулю $m = p + iq$.

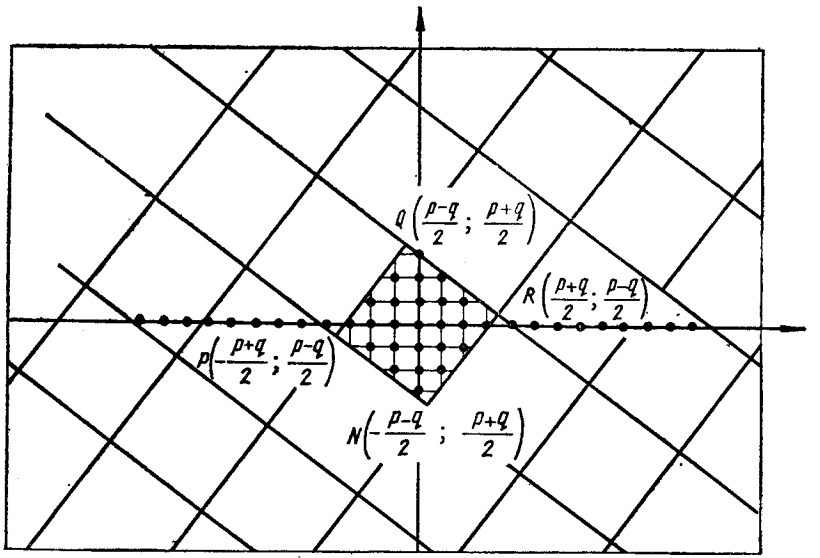


Рис. 14. Геометрическое представление ПСАНВ по модулю $m = p + iq$.

Пусть некоторая внутренняя точка N_i квадрата $ORLM$ изображает число $\dot{A} = a + bi$. Тогда конгруентная ей точка будет изображать число $\dot{B} = (lp - sq + a) + (lq + sp + b)\ i$. Разность $\dot{B} - \dot{A} = (lp - sq) + (lq - sp)\ i$, как показано выше, делится на $p + qi$. Следовательно, $\dot{B} \equiv \dot{A} \bmod (p + qi)$.

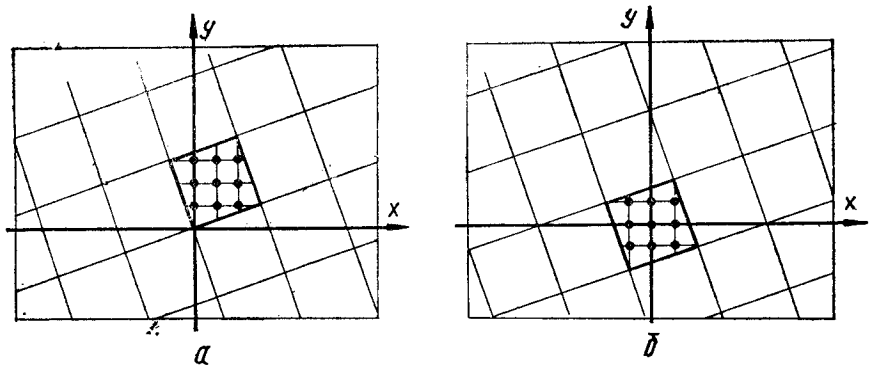


Рис. 15. Геометрическое представление вычетов ПСНВ (*а*) и ПСАНВ (*б*) по модулю $\dot{m} = 3 + i1$.

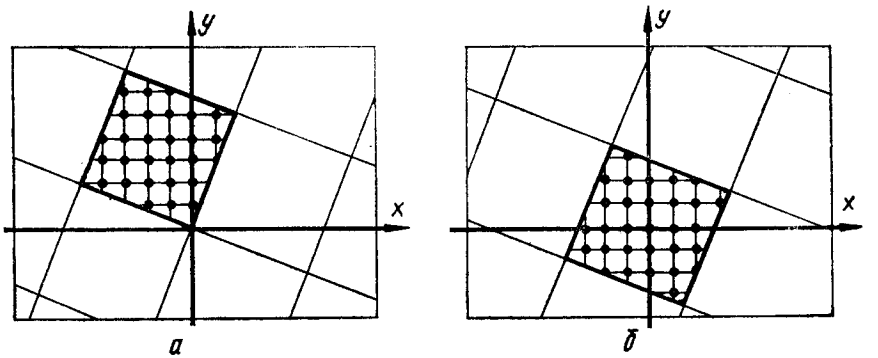


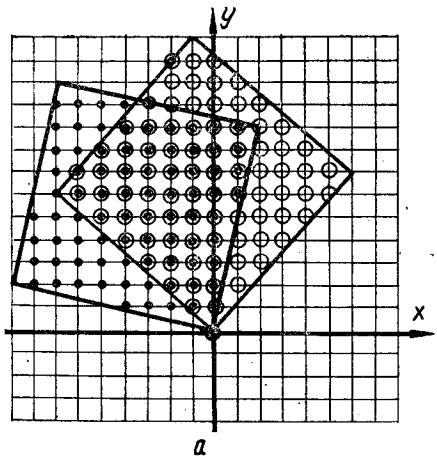
Рис. 16. Геометрическое представление вычетов ПСНВ (*а*) и ПСАНВ (*б*) по модулю $\dot{m} = 2 + 5i$.

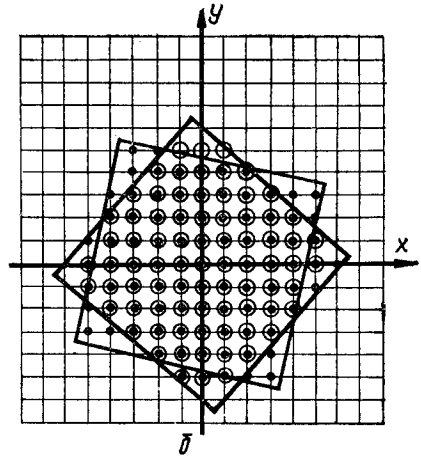
Для того чтобы теорема была доказана для любой пары конгруентных точек, можно каждый из квадратов сопоставить с квадратом $ORLM$, и если $\dot{B}$ и $\dot{B}'$ изображаются точками двух разных квадратов, каждая из которых конгруентна точке, изображающей число $\dot{A}$, то имеют место сравнения

$$\dot{B} \equiv \dot{A} \bmod (p + qi); \quad \dot{B}' \equiv \dot{A} \bmod (p + qi).$$

Откуда и следует, что $\dot{B}' \equiv \dot{B} \bmod (p + qi)$.

Из этой теоремы легко сделать следующий вывод: всего несравнимых между собой чисел может быть столько, сколько целых точек находится внутри любого квадрата и на его двух непараллельных сторонах, включая и одну вершину, и все эти точки определяют в совокупности полную систему вычетов по данному модулю. Можно геометрически показать, что количество таких точек равно $N = p^2 + q^2$ и что, следовательно, количество вычетов в полной системе равно N.





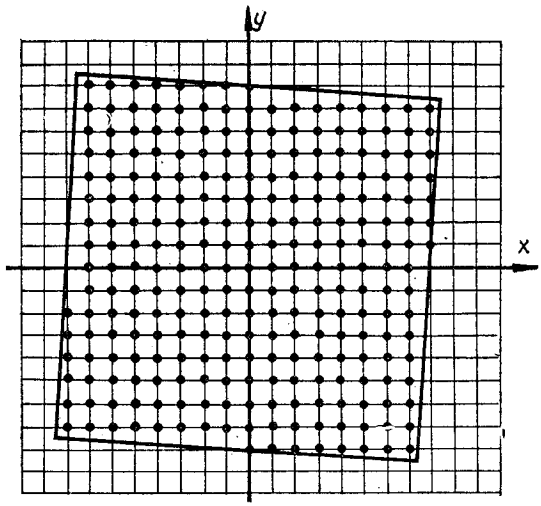


Рис. 17. Геометрическое представление вычетов ПСНВ (*а*) и ПСАНВ (*б*) по модулям $m_1 = 2 + 9i$ и $m_2 = 6 + 7i$ (где $|m_1| = |m_2| = 85$).

Рис. 18. Геометрическое представление ПСАНВ по модулю $m = 1 + 16\ i$ (где $|m| = 257$).

Таким образом, полная система наименьших вычетов по модулю $m = p + qi$ может быть получена геометрическим построением квадрата со стороной $\sqrt{p^2 + q^2}$, проходящим через точку O, и перечислением всех целых комплексных чисел, представленных внутренними точками этого квадрата. Легко вычислить координаты вершин этого квадрата: O (0, 0); R $(-q, p)$; L $(p - q, p + q)$; M (p, q). Геометрическая интерпретация полной системы абсолютно наименьших вычетов дается квадратом $NPQR$ (рис. 14), вершины которого имеют следующие координаты: $N\left(-\frac{(p-q)}{2}, \frac{(p+q)}{2}\right)$; $P\left(-\frac{(p+q)}{2}, \frac{(p-q)}{2}\right)$; $Q\left(\frac{p-q}{2}, \frac{p+q}{2}\right)$; $R\left(\frac{p+q}{2}, \frac{p-q}{2}\right)$.

На рис. 15—18 в качестве примера представлены ПСНВ и ПСАНВ по некоторым модулям.

4. Теоремы Гаусса. Первообразные корни и индексы в кольце $Z_m[i]$

Теорема 5.3. (Фундаментальная теорема Гаусса [50]). По заданному комплексному модулю $m = p + qi$, норма которого $N = p^2 + q^2$ и для которого p и q — взаимно простые числа, каждое целое комплексное число сравнимо с одним и только одним вычетом из ряда 0, 1, 2, ..., $N - 1$.

Доказательство. Из теории чисел известно, то для двух взаимно простых чисел p и q можно найти таких два целых числа u и v, что $up + vq = 1$. Отсюда

$$i = i(up + vq) + (pv - qu) - (pv - qu) = (uq - vp) + m(v + ui). \quad (5.13)$$

Пусть дано комплексное число $a + ib$. Перепишем его, заменив i значением из (5.13):

$$a + ib = a + (uq - vp)\,b + m(v + ui)\,b.$$

Пусть $a + (uq - vp)\,b = h \pmod N$. Тогда

$$a + (uq - vp)\,b = h + sN = h + s(p + qi)(p - qi) = h + m(ps - qs)$$

и выполняется равенство

$$a + bi = h + m(ps - qs) + m(v + ui)\,b =$$

$$= h + m[(p - qi)\,s + (v + iu)\,b]$$

или в форме сравнения

$$a + bi \equiv h \pmod m. \quad (5.14)$$

Этим доказано, что $a + bi$ сравнимо с одним из чисел 0, 1, 2, ..., $N - 1$ по модулю m. Нетрудно доказать, что это число единственное и определяется из сравнения $a + (uq - vp)\,b \equiv h \pmod N$, где $aq - vp = \rho$. С учетом $up + vq = 1$ имеем

$$\rho = -p/q = q/p = (q - p)/(p + q) \pmod N.$$

Определение 5.1. Выражение $\rho = -p/q$, посредством которого устанавливается соответствие между комплексными и вещественным вычетами по модулю $p + qi$, называется коэффициентом изоморфизма.

Пример 5.4. Решим сравнение $16 + 7i \equiv h \bmod (5 + 2i)$. Поскольку НОД $(5, 2) = 1$, то условие теоремы Гаусса выполняется. Коэффициент изоморфизма модуля $5 + 2i$ равен $\rho = -\frac{5}{2} \pmod{29} = 12$, так как $\frac{1}{2} \pmod{29} \equiv 15$. Поэтому $h = 16 + 7 \cdot 12 = 100 \equiv 19 \pmod{29}$. Следовательно, $16 + 7i = 13 \bmod (5 + 2i)$.

Опираясь на эту теорему, можно доказать справедливость следующего: пусть для двух чисел $A_1 = a_1 + b_1 i$ и $A_2 = a_2 + b_2 i$

существуют такие h_1, h_2, h_+, h_x, что

$$A_1 \equiv h_1 \pmod{m}; \quad \dot{A}_2 \equiv h^2 \pmod{m};$$

$$\dot{A}_1 \pm \dot{A}_2 \equiv h_+ \pmod{m}; \quad \dot{A}_1 \dot{A}_2 \equiv h_x \pmod{m}.$$

Тогда

$$h_+ \equiv h_1 \pm h_2 \pmod{N}; \quad h_x \equiv h_1 h_2 \pmod{N},$$

где N — норма m.

Пример 5.5. Нужно построить наименьшие комплексные вычеты по модулю $m = 3 + 4i$ и определить соответствующие им вещественные вычеты. Здесь $up + vq = 3u + 4v = 1$ при $u = -1$, $v = 1$; $\rho = -3 \pmod{25} = -7$; $N = 3^2 + 4^2 = 25$. Поэтому наименьшие комплексные вычеты, подсчитанные по формуле (5.8),

$$x_1 + ix_2 = \frac{r_1 p - r_2 q}{\|m\|} + i\,\frac{r_2 p + r_1 q}{\|m\|}, \quad r_1,\ r_2 \in |\cdot|_N \qquad (5.15)$$

и их представление в виде вещественных вычетов по модулю N будут иметь вид

$0 \equiv 0$; $1 \equiv -3 + 3i$; $2 \equiv -2 + 3i$; $3 \equiv -1 + 3i$; $4 \equiv 3i$; $5 \equiv 1 + 3i$;
$6 \equiv 2 + 3i$; $7 \equiv -1 + 6i$; $8 \equiv 6i$; $9 \equiv -2 + 2i$; $10 \equiv -1 + 2i$;
$11 \equiv 2i$; $12 \equiv 1 + 2i$; $13 \equiv 2 + 5i$; $14 \equiv -1 + 5i$; $15 \equiv 5i$;
$16 \equiv 1 + 5i$; $17 \equiv -1 + i$; $18 \equiv -i$; $19 \equiv -3 + 4i$; $20 \equiv -2 + 4i$;
$21 \equiv -1 + 4i$; $22 \equiv 4i$; $23 \equiv 1 + 4i$; $24 \equiv 2 + 4i$.

Устанавливаемый теоремой Гаусса изоморфизм для модуля с взаимно простыми компонентами позволяет заменить выполнение рациональных операций над наименьшими комплексными вычетами выполнением тех же операций над соответствующими им вещественными вычетами по вещественному модулю, равному норме комплексного модуля. Этот факт особенно важен при разработке быстродействующих цифровых алгоритмов спектрального анализа комплексных сигналов. В том случае, когда p и q в $m = p + qi$ имеют общий множитель d, верна другая теорема.

Теорема 5.4. (Фундаментальная теорема II Гаусса [50]). По комплексному модулю $m = p + iq$, норма которого $N = p^2 + q^2$ и для которого p, q имеют наибольший общий делитель d, каждое целое комплексное число $a + bi$ сравнимо с вычетом $x_1 + x_2 i$, обладающим тем свойством, что x_1 является одним из чисел 0, 1, 2, ..., $N/d - 1$, а x_2 — одним из чисел 0, 1, 2, ..., $d - 1$, причем только с одним единственным из всех N вычетов, имеющих такой вид. Величины a и b определяются из соотношений

$$b = x_2 \pmod{d}; \quad a + (uq - vp)\,\frac{b - x_2}{a} \equiv x_1 \left(\mathrm{mod}\ \frac{N}{d}\right); \quad up + vq = d.$$

Таким образом, для модуля с невзаимно простыми компонентами уже нет изоморфизма с вещественными числами.

Геометрически интерпретируем I теорему Гаусса. Ранее было показано, что все числа $a + bi$, делящиеся на заданное комплексное число $m = p + qi$, разбивают бесконечную плоскость на множество квадратов со стороной, равной $\sqrt{p^2 + q^2}$. Каждому числу, не делящемуся на модуль $m = p + qi$, соответствует точка, расположенная внутри одного из таких квадратов.

Все числа внутри некоторого определенного квадрата вместе с нулем образуют полную систему вычетов. Следовательно, существует бесконечное множество полных систем вычетов. Полную систему наименьших вычетов содержит только квадрат $ORLM$ (см. рис. 13). Далее известно, что числа, сравнимые по модулю m, занимают в своих квадратах конгруентные положения. Выберем среди множества квадратов квадраты, которые содержат вещественные вычеты от нуля до $N - 1$. На чертеже это будут квадраты $ORLM$ (число 0), OMN_1N_2 (числа 1—6), $N_1N_2N_3N_5$ (числа 7—8), $N_1N_5N_6N_4$ (числа 9—12), $N_5N_6N_9N_{10}$ (числа 13—16), $N_6N_7N_8N_9$ (числа 17—18), $N_8N_9N_{11}N_{12}$ (числа 19—24). Среди этих квадратов, очевидно, нет таких, которые конгруентны относительно вещественной оси. В самом деле, по предположению НОД $(p, q) = 1$, поэтому первым в натуральном ряду вещественным числом, делящимся на модуль $m = p + iq$, будет число $p^2 + q^2$ (вершина N_{12} квадрата $N_8N_9N_{11}N_{12}$). Следовательно, только начиная с квадрата $N_8N_9N_{11}N_{12}$, наступает повторение указанных квадратов, а это значит, для всех вещественных вычетов из указанных квадратов найдутся конгруентные точки в квадрате $ORLM$ ПСНВ.

Очевидно, переход от полной системы вычетов по модулю N к полной системе вычетов по комплексному модулю $m = p + iq$ можно осуществить следующим образом (рассматривается случай НОД $(p, q) \neq 1$). В соответствии с формулой (5.15) система вычетов $Z_m[i]$ состоит из чисел

$$x + iy = (r_1 + ir_2)\frac{m}{N(m)} = \frac{pr_1 - qr_2}{N(m)} + i\frac{qr_1 + pr_2}{N(m)}, \qquad (5.16)$$

где r_1 и r_2 независимо пробегают систему вычетов по модулю N и вычисляются из системы уравнений

$$px + qy = r_1 \pmod N; \quad py - qx = r_2 \pmod N.$$

Замечая теперь, что $h = x + \rho y$, и используя различные выражения для ρ ($\rho = q/p$ и $\rho = -p/q$), будем иметь

$$r_1 = |h_p|_N; \quad r_2 = |-h_q|_N.$$

Подставляя последние выражения в формулу (5.16), получаем

$$\rho^{-1}(h) = x + iy = \frac{p|h_p|_N - q|-h_q|_N}{N(m)} + i\frac{q|h_p|_N + p|-h_q|_N}{N(m)}, \qquad (5.17)$$

что и задает переход от h к $x + iy$. Аппаратурная или программная реализация данных соотношений проводится без затруднений.

Так же как и для колец Z_m, в кольцах $Z_m[i]$ верны следующие теоремы, которые приведем без доказательств, поскольку они без существенных изменений повторяют доказательства соответствующих теорем в кольцах Z_m.

Теорема 5.5. Если $a + ib$ — взаимно простое ЦКЧ с простым числом $m = p + qi$, норма которого равна $N = p^2 + q^2$, то

$$(a + bi)^{N-1} \equiv 1 \pmod{m}.$$

Теорема 5.6. Если $a + ib$ — взаимно простое ЦКЧ с простым ЦКЧ $m = p + qi$, норма которого равна $N = p^2 + q^2$, а t — наименьшее число такое, что $(a + bi)^t \equiv 1 \pmod{m}$, то t является делителем всякого другого показателя K, для которого $(a + bi)^K \equiv 1 \pmod{m}$. В частности, t делит или равно $N - 1$.

Определение 5.2. Взаимно простое ЦКЧ ε с простым ЦКЧ m, с нормой N называется первообразным корнем по модулю N, если наименьший показатель степени числа ε, сравнимого с единицей по модулю m, равен $\varphi(N)$.

Теорема 5.7. Если ε обозначает первообразный корень по модулю m, норма которого равна N, то члены ряда $1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-2}$ будут попарно несравнимы между собой, т. е. этот ряд представляет полную приведенную систему вычетов, если к нему присоединить нулевой элемент.

5. Модулярное ТЧП Гаусса

Полученный изоморфизм ρ между кольцами $Z_m[i]$ и Z_N можно распространить и на пространства $L(G_M, Z_m[i])$ и $L(G_M, Z_N)$:

$$\rho : L(G_M, Z_m[i]) \to L(G_M, Z_N); \tag{5.18}$$

$$\rho^{-1} : L(G_M, Z_N) \to L(G_M, Z_m[i]). \tag{5.19}$$

Использование преобразований ρ и ρ^{-1} при решении различных задач цифровой обработки комплексных сигналов позволяет погрузить, как это видно из (5.18), комплексное пространство $L(G_M, Z_m \times [i])$ в модулярное $L(G_M, Z_N)$. Тем самым создается возможность работать в целочисленной области с комплексными числами без разбиения их на действительную и мнимую части. Этот факт дает возможность при разработке быстродействующих цифровых алгоритмов гармонического анализа комплексных случайных сигналов по-новому взглянуть на машинную реализацию преобразования Фурье.

Пусть теперь $m = p + qi$ является целым комплексным числом, где НОД $(p, q) = 1$; $z(t) \in L(G, Z_m[i])$, а $\varepsilon = a + ib$ — взаимно простое ЦКЧ с $m = p + iq$. Тогда ε будет принадлежать мультипликативной группе (приведенной системе вычетов по модулю m) кольца $Z_m[i]$ и иметь некоторый период T, являющийся делителем

числа $\varphi(N)$, где $N = p^2 + q^2$ — норма ЦКЧ m. Построим следующую систему функций на группе G_T:

$$\chi_\alpha(t) = \varepsilon^{\alpha t}, \quad \alpha,\ t = 0,\ 1,\ \ldots,\ T-1. \tag{5.20}$$

Так как $\chi(0) = 1$, $\chi_\alpha(t_1 \oplus t_2) = \chi_\alpha(t_1)\,\chi_\alpha(t_2)$ (где символ $\oplus$ обозначает сложение по модулю T) и если в кольце имеет смысл деление на число T, то введенные функции образуют множество характеров группы, а значит, и ортогональный базис в пространстве $L(G_T, Z_m[i])$. Построенный таким образом базис будем называть базисом Гаусса, а соответствующее ему преобразование — ТЧП Гаусса.

Действуя изоморфизмом ρ на комплексный элемент ε мультипликативной группы кольца $Z_m[i]$, получаем целое рациональное число $\rho(\varepsilon)$. При этом система функций на группе G_T

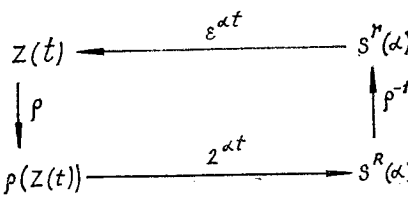
$$\chi_\alpha(t) = (\rho(\varepsilon))^{\alpha t}, \quad \alpha,\ t = 0,\ 1,\ \ldots,\ T-1$$

будет образовывать ортогональный базис в пространстве $L(G_T, Z_N)$. Естественно, что в качестве вещественного представления базиса $\rho(\varepsilon^{\alpha t})$ целесообразно использовать базис Рейдера $2^{\alpha t}$. Таким образом, задачу выбора базиса Гаусса в пространстве $L(G_T, Z_m[i])$, т. е. выбор подходящего ε, мы свели к выбору его образа $\rho(\varepsilon)$ в пространстве $L(G_T, Z_N)$. Следовательно, класс преобразований Гаусса мы ограничиваем такими $\varepsilon = \sqrt[l]{1}$, для которых $\rho(\varepsilon) = 2$. При этом

$$\chi_\alpha(t) = \rho^{-1}(2^{\alpha t}) = \varepsilon^{\alpha t}, \quad \rho(\chi_\alpha(t)) = 2^{\alpha t},$$

что устанавливает взаимно однозначное соответствие между преобразованиями Гаусса и Рейдера.

Таким образом, гармонический анализ комплексных сигналов на ЦВМ можно проводить по двум схемам, представленным следующей коммутативной диаграммой:



где $S^r(\alpha)$ — преобразование Гаусса сигнала $z(t) \in L(G_T, Z_m[i])$; $S^R(\alpha)$ — преобразование Рейдера сигнала $\rho(Z(t)) \in L(G_T, Z_N)$. По этой схеме спектр $S^r(\alpha)$ сигнала $z(t)$ вычисляется в базисе Гаусса:

$$S^r(\alpha) = \sum_{t=0}^{T-1} z(t)\,\varepsilon^{-\alpha t} \pmod m, \tag{5.21}$$

а второй сигнал предварительно превращается в целочисленный сигнал $\rho(z(t))$, спектральный анализ которого проводится в базисе

Рейдера:

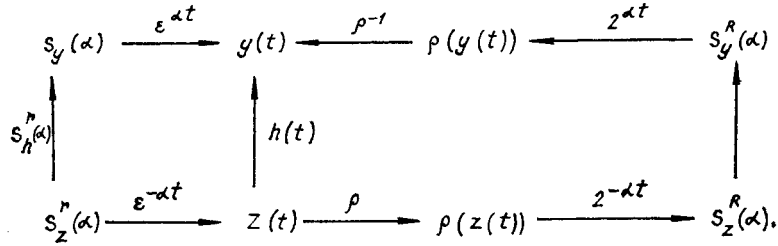
$$S^R(\alpha) = \sum_{t=0}^{T-1} \rho(z(t))\, 2^{-\alpha t} \pmod N. \tag{5.22}$$

Затем с помощью обратного преобразования ρ^{-1} находим спектр Гаусса.

Аналогично, если дана свертка (комплексная)

$$y(t) = \sum_{\tau=0}^{T-1} h(t-\tau)\, z(\tau), \tag{5.23}$$

то ее можно смоделировать по двум схемам: применяя преобразование Гаусса и применяя преобразования ρ и ρ^{-1} совместно с ТЧПР:



По первой схеме находим спектр Гаусса сигнала $z(t)$:

$$S_Z^r(\alpha) = \sum_{t=0}^{T-1} z(t)\, \varepsilon^{-\alpha t} \pmod m,$$

умножая который на спектр $S_h^r(\alpha)$ весовой функции, получаем спектр Гаусса выходного сигнала $y(t)$. Действуя на последний обратным преобразованием Гаусса, находим свертку входного сигнала $z(t)$ с весовой функцией $h(t)$. По второй схеме (правая часть) входной сигнал $z(t)$ предварительно подвергается преобразованию и превращается в модулярный. С помощью ТЧПР $\rho(z(t))$ определяется спектр сигнала $\rho(z(t))$, умножая который на спектр Рейдера $\rho_h^R(\alpha)$ весовой функции $h(t)$, определяем спектр выходного сигнала $S_y^R(\alpha)$. Действуя теперь на $S_y^R(\alpha)$ последовательно обратным ТЧПР и изоморфизмом ρ^{-1}, получаем выходной сигнал $y(t)$.

Пример 5.6. Определим циклическую автосвертку комплексных чисел:

$$z(0) = (0 + 1i); \quad z(1) = (1 + i); \quad z(2) = z(3) = 0 + i0.$$

Для контроля рассчитаем свертку по формуле (5.23):

$$y(0) = -1; \quad y(1) = -2 - 2i; \quad y(2) = 2i; \quad y(3) = 0.$$

Для $m = 2 + 5i$, $\rho = 12$, $N = 29$ число 2 является первообразным корнем степени $28 : 2^{N-1} = 2^{28} = 1 \pmod{29}$. Поэтому $\varepsilon =$

$= 2^7 \equiv 12 \pmod{29}$ — корень четвертой степени из единицы. Тогда

$$S_Z^R(\alpha) = R[\rho(z(t))] =$$

$$= \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 12 & -1 & 17 \\ 1 & -1 & 1 & -1 \\ 1 & 17 & -1 & 12 \end{bmatrix} \times$$

$$\times \begin{bmatrix} 12 \\ 13 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} -4 \\ -6 \\ -1 \\ 1 \end{bmatrix};$$

$$S_y^R(\alpha) = \begin{bmatrix} 16 \\ 7 \\ 1 \\ 1 \end{bmatrix};$$

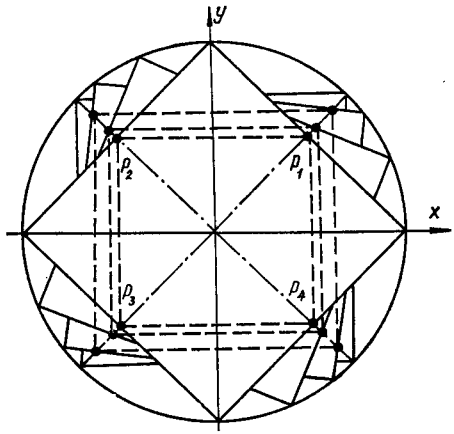


Рис. 19. Геометрическое представление ПСАНВ по различным модулям, имеющим одинаковую норму.

$[\rho(y(t))]' = [T^{-1}R^{-1}S_y^R(\alpha)]' = [28; 22; 24; 0]$, где $T^{-1} = 22$.

Действуя на полученный вектор преобразованием ρ^{-1}, используя для этой цели соотношения (5.17), находим $y(t)$:

$$y(0) = -1; \quad y(1) = -2 + 2i; \quad y(2) = 2i; \quad y(3) = 0.$$

Найдем теперь условия, при которых использование $Z_{\dot{m}}[i]$-арифметики приводит к тем же значениям, что и $Z[i]$-арифметика. Очевидно, это возможно в том случае, когда значения $y(t)$, подсчитанные в $Z_{\dot{m}}[i]$, лежат внутри полной системы вычетов $Z_{\dot{m}}[i]$. Если отвести под мнимую и действительную части одинаковые динамические диапазоны, то значения $y(t)$ должны попасть внутрь квадрата $P_1P_2P_3P_4$ (рис. 19). Так как вершина P_1 лежит на прямой $\varphi = x$ и $px + qy = N/2$, то она имеет следующие координаты:

$$x = y = \frac{1}{2}\,\frac{p^2+q^2}{p+q} = \frac{1}{2}\,\frac{N}{p+q}.$$

Это приводит к необходимости ограничить рабочие области квантованных комплексных сигналов $z(t) = x(t) + iy(t)$ и переходных функций $h(t) = h_{\mathrm{Re}}(t) + ih_{\mathrm{Im}}(t)$ величиной $\frac{1}{2}\,\frac{N}{p+q}$. Поэтому имеем

$$\left|\sum_{\tau=0}^{T-1} h_{\mathrm{Re}}(t-\tau)\,x_1(\tau) + h_{\mathrm{Im}}(t-\tau)\,y(\tau)\right| \leqslant$$

$$\leqslant \sum_{\tau=0}^{T-1} (|h_{\mathrm{Re}}(t-\tau)|\,|x(\tau)| + |h_{\mathrm{Im}}(t-\tau)|\,|y(\tau)|) \leqslant \frac{1}{2}\,\frac{N}{p+q};$$

$$\left|\sum_{\tau=0} h_{\mathrm{Re}}(t-\tau)\,y(\tau)+h_{\mathrm{Im}}(t-\tau)\,x(\tau)\right|\leqslant$$

$$\leqslant\sum_{\tau=0}^{T-1}\left(|h_{\mathrm{Re}}(t-\tau)||y(\tau)|+h_{\mathrm{Im}}(t-\tau)||x(\tau)|\right)\leqslant\frac{1}{2}\,\frac{N}{p+q}.$$

Если $\max\limits_t h_{\mathrm{Im}}(t)=\max\limits_t h_{\mathrm{Re}}(t)=\max\limits_t x(t)=\max\limits_t y(t)$, то из последних неравенств наибольшее значение A определяется как

$$A=\left\lfloor\frac{1}{2}\sqrt{\frac{N}{(p+q)\,T}}\right\rfloor. \tag{5.24}$$

Очевидно, A зависит от выбора p и q, даже если при этом величина $p^2+q^2=N$ остается неизменной. Для $p\approx q$ имеем

$$A_1=\left\lfloor\frac{1}{2}\sqrt{\frac{N}{pT}}\right\rfloor.$$

Если $p\gg q$ (или наоборот), то

$$A_2=\left\lfloor\frac{1}{2}\sqrt{\frac{N}{pT}}\right\rfloor. \tag{5.25}$$

Отсюда видно, что $A_2>A_1$.

Если, например, $p=F_5-1$, $q=1$, $N(F_5-1+i)=(F_5-1)^2+1=2^{64}+1$, то

$$A_2=\left\lfloor\frac{1}{2}\sqrt{\frac{2^{64}}{2^{32}\cdot 2^8}}\right\rfloor\approx 2^{11}.$$

Это означает, что при $-2^{11}\leqslant h_{\mathrm{Re}}(t)$, $h_{\mathrm{Im}}(t)$, $x(t)$, $y(t)\leqslant+2^{11}$ обеспечена возможность для $y(t)$ находиться внутри квадрата $P_1P_2P_3P_4$.

6. Максимальный объем ТЧП Гаусса

Натуральные числа являются целыми числами Гаусса; простые натуральные числа не всегда являются простыми числами Гаусса. Например, 7 — простое число Гаусса, а $5=(2+i)(2-i)$ — разложимое.

Теорема 5.8. Если $z\in Z[i]$ и $N(z)$ — простое натуральное число, то z — простое число Гаусса.

Доказательство. Пусть $z\in Z[i]$, $N(z)=p$ — простое. Допустим, что $z=z_1z_2$, где $z_1,\ z_2\in Z[i]$. Тогда $N(z)=N(z_1)\times N(z_2)$ и либо $N(z_1)=1$, либо $N(z_2)=1$, а значит, либо $z_1\mid 1$, либо $z_2\mid 1$, и z представимо в виде произведения целого числа Гаусса и делителя единицы, т. е. z — простое число Гаусса.

Теорема 5.9. Норма простого числа Гаусса является либо простым числом, либо квадратом простого числа.

Доказательство. Пусть z — простое число Гаусса. Тогда существует такое натуральное число p, что $z\mid p$. Поэтому $p=z\alpha$, где α — целое число Гаусса. Но $p^2=N(p)=N(z)\,N(\alpha)$, $N(z)\neq 1$, так как $z\neq 1$. Значит, либо $N(z)=p$, либо $N(z)=p^2$.

Определение 5.3. Простые числа Гаусса, нормы которых — простые натуральные числа, называются числами первого порядка, а те, нормы которых равны квадратам простых чисел,— числами второго порядка.

Приведем примеры простых чисел Гаусса первого и второго порядков и выделим из множества простых натуральных чисел те, которые являются простыми и в кольце $Z[i]$.

Пример 5.7. 1) $z_1 = 1 + i$, $z_2 = 2 + i$ — простые числа первого порядка, так как $N(1 + i) = 2$, $N(2 + i) = 3$; 2) $z_3 = 3$ — простое число Гаусса второго порядка, так как $N(3) = 3^2$. Простые числа Гаусса второго порядка всегда являются целыми рациональными простыми числами.

Определение 5.4. Простые натуральные числа, остающиеся простыми в кольце $Z[i]$, называются неразложимыми. Простые натуральные числа p, соответствующие нормам простых чисел Гаусса первого порядка, называются разложимыми.

Для решения вопроса об отборе неразложимых простых натуральных чисел заметим, что множество простых натуральных чисел охватывается числами вида $4n + 1$ и $4n + 3$ при $n = 0, +1, \ldots$. В самом деле, любое натуральное число может быть записано одной из форм $4n$, $4n + 1$, $4n + 2$, $4n + 3$, но первая и третья выражают только составные числа, на долю всех простых и части составных чисел остаются вторая и четвертая формы.

Теорема 5.10. Натуральное число $4n + 3$ является неразложимым.

Доказательство. Допустим, что $p = 4n + 3$ раскладывается на простые множители в кольце $Z[i]$:

$$p = (a + bi)(a - bi) = a^2 + b^2.$$

Тогда для получения нечетного числа $4n + 3$ числа a и b должны быть разной четности. Поэтому $a^2 + b^2 = 1 \pmod 4$, т. е. $a^2 + b^2 = 4n + 1$, что противоречит условию. Следовательно, $p = 4n + 3$ не может быть разложено в произведение целых комплексных чисел.

Пусть теперь $z \mid p$, т. е. $p = zt$ (где t — простое число Гаусса, но не первого порядка). Тогда $N(p) = N(z)\,N(t)$, но $N(z) \neq p$, значит, $N(z) = p^2$. Поэтому $N(p) = p^2$, $N(z) = p^2$, $N(t) = 1$ и $t \mid 1$. Таким образом, p — простое неразложимое число.

Теорема 5.11. Каждое простое число $p = 4n + 1$ является разложимым в кольце $Z[i]$.

Доказательство. Допустим, что произвольное простое число p (не обязательно вида $4n + 1$) разложимо в кольце $Z[i]$, а $p = \prod_{k=1}^{\tau} \pi_k$ — его единственное разложение на простые элементы кольца. Так как $N(\pi_k) > 1$, то из $p^2 = N(p) = \prod_{k=1}^{r} N(\pi_k)$ следуют равенства $r = 2$; $p = \pi_1\ \pi_2$; $N(\pi_1) = N(\pi_2) = p$. Если $\pi_1 = a + ib$, то $p = N(\pi_1) = a^2 + b^2 = (a + ib)(a - ib)$. Откуда

$\pi_2 = a - ib$. Итак, если простое число $p \in Z$ допускает нетривиальное разложение в $Z[i]$, то

$$p = \pi_1 \cdot \pi^* = (a + ib)(a - ib) = a^2 + b^2,$$

где $a + ib$, $a - ib$ — простые элементы в $Z[i]$.

Заметим далее, что $t^2 \equiv 0$ или $1 \pmod 4$ для любого $t \in Z$. Поэтому для нечетного простого p, не являющегося простым в $Z[i]$, критерий (5.25) приводит к выводу $p = a^2 + b^2 = 0, 1, 2 \bmod 4$, т. е. имеет вид $p = 4n + 1$.

В тесной связи с вопросом об изоморфизме колец $Z_{\dot{m}}[i]$ и Z_N (где $N = |m|$) находится вопрос о представлении натурального числа N в виде суммы двух квадратов $a^2 + b^2$. Очевидно, на сумму двух квадратов раскладываются те простые натуральные числа, которые в кольце $Z[i]$ являются разложимыми, а именно 2 и числа вида $4n + 1$. Например, $5^2 + 2^2 = 29 = 4 \cdot 7 + 1$, $2^2 + 3^2 = 13 = 4 \cdot 3 + 1$. Простые натуральные числа вида $4n + 3$ не являются нормами целых чисел Гаусса и поэтому не могут быть представлены в виде суммы двух квадратов.

Выясним, какие числа и сколькими способами можно представить в виде суммы двух квадратов. Эта задача равносильна задаче об отборе натуральных чисел, которые можно рассматривать как нормы целых чисел Гаусса, а значит, равносильна задаче нахождения изоморфных колец $Z_{\dot{m}}[i]$ и Z_N.

Пусть N — натуральное число, а z таково, что $N(z) = N$. Обозначим через p_i простые числа вида $4n + 1$, а через q — вида $4n + 3$. Тогда каноническое разложение числа N будет иметь следующий вид:

$$N = 2^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k} q_1^{\mu_1} q_2^{\mu_2} \dots q_s^{\mu_s}.$$

Каноническое разложение z в кольце $Z[i]$ будет выглядеть так (принимая во внимание, что $z = (1 + i)(1 - i) = (1 + i)^2 i$ и, следовательно, $2 \sim (1 + i)^2$):

$$z = \varepsilon (1 + i)^{\sigma} \pi_1^{\sigma_1} \bar{\pi}_1^{\tau_1} \dots \pi_k^{\sigma_k} \bar{\pi}_k^{\tau_k} q_1^{\nu_1} \dots q_s^{\nu_s},$$

где ε — единица кольца $Z[i]$; $1 + i$, π_1, $\bar{\pi}_1$, ..., $\bar{\pi}_k$, π_k — простые числа Гаусса, соответствующие разложениям простых чисел p_i, $i = 1, 2, \dots, n$; q_i — неразложимые простые числа.

Из выражений

$$N_1(z) = N((1 + i)^{\sigma_0}) N(\pi_1^{\sigma_1} \bar{\pi}_1^{\tau_1}) \dots N(\pi_k^{\sigma_k} \bar{\pi}_k^{\tau_k}) N(q_1^{\nu_1}) \dots N(q_s^{\nu_s});$$

$$N(z) = N = 2^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \dots p_k^{\lambda_k} q_1^{\mu_1} \dots q_s^{\mu_s}$$

следует, что $N_1(z) = N$ тогда и только тогда, когда

$$\sigma = \lambda_0;\ \sigma_1 + \tau_1 = \lambda_1;\ \sigma_2 + \tau_2 = \lambda_2,\ \dots,\ \sigma_k + \tau_k = \lambda_k;$$

$$\mu_1 = 2\nu_1;\ \mu_2 = 2\nu_2,\ \dots,\ \mu_s = 2\nu_s.$$

Из последних равенств следует, что необходимым и достаточным условием представимости числа N в виде суммы двух квадратов (хо-

тя бы одним способом) является четность всех μ. Иначе: простые множители вида $4n + 3$ должны входить в разложение числа N в четных степенях. Например, $N = 2 \cdot 3 \cdot 11 \cdot 5 = 330$ не разлагается на сумму двух квадратов, $N_1 = 5 \cdot 7^2 = 245$ — разлагается, а именно $245 = 7^2 + 14^2$. Одно из комплексных чисел с подобной нормой равно $7 + 14i$ и легко получается из выражения для нормы $5 = N(1 + 2i)$, а $N(7) = 7^2$. Значит, $N(7 + 14i) = 245$.

При фиксированных $\lambda_1, \lambda_2, \ldots, \lambda_k, \mu_1, \ldots, \mu_s$, а именно такими они являются для заданного N, показатели $\sigma_0, \nu_1, \nu_2, \ldots, \nu_s$ определяются однозначно, а $\sigma_1, \sigma_2, \ldots, \sigma_k; \tau_1, \tau_2, \ldots, \tau_k$ — неоднозначно. Следовательно, количество представлений числа N суммой квадратов зависит от числа выборов, возможных для показателей σ_1 и τ_1, σ_2 и τ_2 и т. д. Для показателей σ_1 и τ_1 таких возможных наборов будет $\lambda_1 + 1$, так как λ_1 набрать суммами двух неотрицательных слагаемых можно $\lambda_1 + 1$ способами: $0 + \lambda_1$, $1 + (\lambda_1 - 1)$, $2 + (\lambda_2 - 2)$, ..., $(\lambda_1 - 1) + 1$, $\lambda_1 + 0$. Аналогично для σ_2 и τ_2 имеется $\lambda_2 + 1$ возможностей и так далее. Всего таким образом будет $(\lambda_1 + 1)(\lambda_2 + 1) \ldots (\lambda_k + 1)$ возможностей.

Если теперь учтем четыре делителя единицы $(1, -1, i, -i)$, то получим, что всего различных комбинаций будет $4(\lambda_1 + 1)(\lambda_2 + 1) \ldots (\lambda_k + 1)$ и, следовательно, N может быть представлено в виде суммы двух квадратов $4(\lambda_1 + 1)(\lambda_2 + 1) \ldots (\lambda_k + 1)$ способами. При проведенном подсчете оказались учтенными все решения $N = a^2 + b^2$, но некоторые могут дать одно и то же представление. Например, если $n = 2^2 + 3^2$, то $N = (-2)^2 + (-3)^2$, т. е. и это одно и то же представление, хотя использованы две различные пары $(2, 3)$ и $(-2, -3)$. Вообще одно и то же представление дают пары чисел: (a, b), $(a, -b)$, $(-a, b)$, $(-a, -b)$, (b, a), $(-b, a)$, $(b, -a)$, $(-b, -a)$. Если $b = 0$ или $a = 0$, или $a = \pm b$, то из восьми указанных пар четыре различные. Но это имеет место только тогда, когда N — полный квадрат или удвоенный полный квадрат. В самом деле, если $a = a \pm b$, то $N = 2b^2$; если $a = 0$, то $N = b^2$ (это тогда, когда все $\lambda_1, \lambda_2, \ldots, \lambda_k$ — четные). Следовательно, если $N \neq x^2$ и $N \neq 2x^2$, то для подсчета числа различных представлений в виде суммы двух квадратов нужно полученное число разделить на 8.

Итак, если $M(N)$ — число представлений N в виде суммы двух квадратов и не все λ_i $(i = 1, 2, \ldots, k)$ четные, то

$$M(N) = \frac{1}{2}(\lambda_1 + 1)(\lambda_2 + 1) \ldots (\lambda_k + 1) = \frac{1}{2}\prod_{i=1}^{k}(\lambda_i + 1).$$

Если $N = x^2$ или $N = 2x^2$, т. е. если в каноническом разложении N все λ_i четные, то формула числа представлений N в виде суммы квадратов будет несколько иной.

Пусть $M(N)$ — число представлений такого N. Подсчитаем его, для чего выразим различными способами число всех решений уравнения $N = a^2 + b^2$. Выше установлено, что оно равно числу $4(\lambda_1 + 1)(\lambda_2 + 1) \ldots (\lambda_k + 1)$. Иначе его можно подсчитать следующим образом. Исключим из рассмотрения одно представление — то, которое фактически задано ($N = a^2$ или $N = 2a^2$) и дает 4 решения урав-

нения. Оставшихся решений будет 8 $[M(N)-1]$, следовательно, всех решений будет $8[M(N)-1]+4$. Итак,

$$4(\lambda_1+1)(\lambda_2+1)\ldots(\lambda_k+1)=8[M(N)-1]+4,$$

откуда

$$M(N)=\frac{1}{2}[(\lambda_1+1)(\lambda_2+1)\ldots(\lambda_k+1)+1].$$

Таким образом,

$$M(N)=\begin{cases}\frac{1}{2}[(\lambda_1+1)(\lambda_2+1)\ldots(\lambda_k+1)], & \text{если не все } \lambda_i \text{ четные;}\\ \frac{1}{2}[(\lambda_1+1)(\lambda_2+1)\ldots(\lambda_k+1)+1], & \text{если все } \lambda_i \text{ четные.}\end{cases} \tag{5.26}$$

Пример 5.8. 1) $M(80)=M(2^4\cdot 5)=\frac{1}{2}\cdot 2=1$;

2) $M(100)=M(2^2\cdot 5^2)=\frac{1}{2}[(2+1)+1]=2$.

Формулу (5.26) можно записать в более компактном виде:

$$M[N=a^2+b^2]=\begin{cases}\frac{1}{8}\left[\sum\limits_{\substack{d\mid N,\\ d\equiv 1 \bmod 4}}1-\sum\limits_{\substack{d\mid N,\\ d\equiv 3 \bmod 4}}1\right]=\sum\limits_{\substack{d\mid N,\\ d-\text{нечетные}}}(-1)^{\frac{d-1}{2}};\\ \frac{1}{2}\left[\sum(-1)^{\frac{d-1}{2}}+1\right]=\frac{1}{8}[1+\sum 1-\sum 1].\end{cases} \tag{5.27}$$

Выражение (5.27) называется формулой Якоби.

Эйлер обратил внимание на то обстоятельство, что если число раскладывается несколькими способами на сумму двух квадратов, то оно не может быть простым. Простые числа вида $4n+1$ раскладываются на сумму двух квадратов единственным способом. Это подтверждается изложенной выше теорией. В самом деле, если N — простое, то $N=p$; если $p=4n+3$, то N не разлагается на сумму двух квадратов, так как $4n+3$ в нечетной степени; если $p=4n+1$, то N разлагается на сумму двух квадратов, но поскольку $\lambda_1=1$, то $M[p]=\frac{1}{2}(1+1)=1$.

Из всех представлений интересно выделить такие, в которых квадраты взаимно просты. Но если НОД $(a^2+b^2)=1$, то НОД $(a, b)=1$. Назовем число $z=a+bi$, где НОД $(a, b)=1$, примитивным числом Гаусса. Тогда примитивному представлению числа N в виде суммы квадратов соответствует выражение числа в виде нормы примитивного числа Гаусса. Именно теперь мы подошли вплотную к вопросу об изоморфизме колец Z_N и $Z_m[i]$, где $N=|\overset{*}{m}|=N(p+iq)$. Естественно, что нас будут интересовать сомножители числа N.

Пусть $N=N(z)$ и $2^l\mid N$, $l>1$. Тогда $2^l\mid(a+b_i)\times(a-b_i)$ и $2^l=(1+i)^l(1-i)^l$. Допустим, что $(1-i)^l\mid a-b_i$,

следовательно, $(1-i)^2 \mid a-b_i$. Однако $(1-i)^2 = -2i$, значит, $2 \mid a-b_i$, т. е. $2 \mid a$, $2 \mid b$ и НОД $(a, b) \neq 1$, другими словами, представление не примитивно. Значит, $l \leqslant 1$ и $\sigma_0 \leqslant 1$, т. е. 2 может входить в разложение числа N не более чем в первой степени.

Покажем, что при $\sigma_0 = 1$ представление может быть примитивным, а может и не быть примитивным. Если $N = N(z) = (a+bi) \times (a-bi)$ и $2 \mid N$, то, по крайней мере, один из сомножителей $(a+bi)$ или $(a-bi)$ делится на $1-i$. Пусть $1-i \mid a-bi$, тогда $1+i \mid a+bi$, но $1+i = i(1-i)$, значит, $1-i \mid a+bi$. Итак, $(1-i)^2 \mid (a-bi)(a+bi)$, но так как $(1-i)^2 = -2i$, то $2 \mid (a-bi)(a+bi) = a^2+b^2$ и a и b могут быть как взаимно простыми, так и не взаимно простыми.

Пусть $N = N(z)$ и $q_i^{2\nu_i} \mid N$, $\nu_i \neq 0$. Тогда $q_i^{2\nu_i} \neq (a+bi)(a-bi)$. Но q_i — неразложимое простое число Гаусса, следовательно, оно делит один из сомножителей $a+bi$ или $a-bi$. Например, $q_i^{2\nu_i} \mid a+bi$, тогда $q_i^{2\nu_i} \mid a$ и $q_i^{2\nu_i} \mid b$. Значит, НОД $(a, b) \neq 1$, $\nu_i = 0$, $i = 1, 2, \ldots, s$. Итак, примитивное представление допускают такие числа N, что

$$N = 2^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k},$$

где $\lambda_0 = 0, 1$; $p_i = 4n+1$, $i = 1, 2, \ldots, k$.

Теорема 5.12. Теоретико-числовое преобразование Гаусса по модулю $m = p + iq$ существует тогда и только тогда, когда норма примитивного числа m, т. е. такого, что НОД $(p, q) = 1$, является числом нечетным и имеет максимальный объем преобразования, выражающийся числом вида $4n$.

Доказательство. Норма примитивного числа всегда имеет вид

$$N = 2^{\lambda_0} p_1^{\lambda_1} p_2^{\lambda_2} \ldots p_k^{\lambda_k},$$

где p_i $(i = 1, 2, \ldots, k)$ — простые числа вида $4n_i + 1$. По теореме 4.1 в кольце Z_N ТЧП существует тогда и только тогда, когда N — число нечетное. Поэтому λ_0 должно равняться нулю. В силу этой теоремы имеем

$$N_{\max} = \text{НОД}(p_1 - 1, p_2 - 1, \ldots, p_k - 1) =$$
$$= \text{НОД}(4n_1, 4n_2, \ldots, 4n_k) = 4\,\text{НОД}(n_1, n_2, \ldots, n_k) = 4n,$$

где $n = \text{НОД}(n_1, n_2, \ldots, n_k)$.

Подсчитаем количество примитивных представлений

$$z = a + bi = \varepsilon (1+i)^{\sigma} \pi_1^{\sigma_1} \bar{\pi}_1^{\tau_1} \ldots \pi_k^{\sigma_k} \bar{\pi}_k^{\tau_k},$$

где НОД $(a, b) = 1$, $\sigma = 0, 1$.

Если $\sigma_1 > 0$ и $\tau > 0$, то $\pi_1 \mid a+bi$, $\bar{\pi}_1 \mid a+bi$, $\pi_1 \bar{\pi}_1 \mid a+bi$, $p_1 \mid a+bi$, $p_1 \mid a$, $p_2 \mid b$, значит, НОД $(a, b) \neq 1$. Следовательно, $\sigma_1 > 0$, $\tau_1 > 0$ одновременно быть не могут. Остаются две возможности: а) $\sigma_1 = 0$, $\tau_1 = \lambda_1$; б) $\sigma_1 = \lambda_1$, $\tau = 0$. Аналогичные рассуждения для $p_2, \ldots, p_k$ приведут к тому, что для каждого p_i независимо от того,

в какой оно степени, будет лишь два представления. Обозначая число всех примитивных представлений через $M_1(N)$, получаем

$$M_1(N) = \frac{1}{8} \cdot 4 \cdot 2^h = 2^{h-1}.$$

Пример 5.9. 1) $N = 2 \cdot 5 \cdot 13 = 130$, $M_1(N) = 2^1 = 2$, $M_1 \times (130) = 2$, $130 = 3^2 + 11^2 = 7^2 + 9^2$. Оба представления примитивные.

2) $N = 2 \cdot 5^3 = 250$, $M_1(N) = 2^0 = 1$, $M_1(N) = \frac{1}{2}(3 + 1) = 2$, $250 = 5^2 + 15^2 = 9^2 + 13^2$. Из двух представлений одно является примитивным.

Вообще говоря, из всей совокупности $M_1(N)$ представлений не все равноценны. Наиболее широко используются числа кольца $Z_{\dot{m}}[i]$ тогда, когда ПСАНВ $Z_{\dot{m}}[i]$ геометрически ближе всего к квадрату со сторонами, параллельными осям координат (см. рис. 17—19). Это будет в том случае, когда p и q сильно отличаются друг от друга по абсолютной величине.

7. χ-Преобразования Гаусса

В четвертой главе введены теоретико-числовые χ-преобразования над кольцами типа Z_m. В дальнейшем будем называть их симплексными или простыми ТЧП. Введение этого термина оправдывается тем, что кроме них рассматриваются χ-преобразования над кольцами $Z_{\dot{m}}[i]$, которые естественно назвать комплексными ТЧП. Кроме того, введены гиперкомплексные ТЧП.

Пусть система ортогональных функций

$$\chi_\alpha(n) = \chi_{\alpha_1\alpha_2\ldots\alpha_m}(n_1, n_2, \ldots, n_m) = \varepsilon_1^{\alpha_1 n_1}\varepsilon_2^{\alpha_2 n_2}\ldots\varepsilon_n^{\alpha_n n_m} \quad (5.28)$$

является системой характеров некоторой конечной абелевой группы $H = H_{h_1} \times H_{h_2} \times \ldots \times H_{h_m}$ над кольцом K.

Пусть $p_1^{k_1} p_2^{k_2} \ldots p_n^{k_m}$ — каноническое разложение числа $N = p^2 + q^2$ и кольцо $Z_{\dot{m}}[i]$ таково, что наименьшее общее кратное чисел $h_1, h_2, \ldots, h_n$ (НОК $(h_1, h_2, \ldots, h_m) = q$) делит наибольший общий делитель чисел $p_1 - 1, p_2 - 1, \ldots, p_m - 1$ (НОД $(p_1 - 1, p_2 - 1, \ldots, p_m - 1) = M$), т. е. $q \mid M$. Тогда $h_1 \mid M$, $h_2 \mid M$, ..., $h_n \mid M$ и в кольце $Z_{\dot{m}}[i]$ существуют первообразные корни степеней $h_1, h_2, \ldots, h_n$:

$$\varepsilon_{n_1} = \varepsilon_1 = \sqrt[h_1]{1} \in Z_{\dot{m}}[i], \ldots, \varepsilon_{h_m} = \varepsilon_m = \sqrt[h_m]{1} \in Z_{\dot{m}}[i].$$

В таком случае, если числа h и N взаимно простые, что является необходимым и достаточным условием существования в кольце $Z_{\dot{m}}[i]$ элемента, обратного h относительно умножения, то функции

$$\chi_\alpha(n) = \chi_{\alpha_1\alpha_2\ldots\alpha_m}(n_1 n_2, \ldots, n_m) = \varepsilon_1^{\alpha_1 n_1}\varepsilon_2^{\alpha_2 n_2}\ldots\varepsilon_m^{\alpha_m n_m}$$

являются характерами группы $H = G_{h_1} \times G_{h_2} \times \ldots \times G_{h_m}$ над кольцом $Z_{\dot{m}}[i]$, т. е. образуют ортонормированный базис в пространстве $L(G_{h_1}, \ldots, G_{h_m}, Z_m[i])$ всех функций, заданных на отрезке $[0, h - 1]$ со значениями в кольце $Z_m[i]$. Преобразования в этом базисе назовем теоретико-числовыми χ-преобразованиями Гаусса или просто χ-преобразованиями Гаусса.

Используя изоморфизм Гаусса ρ, можно установить взаимно однозначное соответствие между пространствами $L(H, Z_N)$ и $L(H, Z_{\dot{m}}[i])$:

$$\rho : L(H, Z_{\dot{m}}[i]) \to L(H, Z_N); \quad \rho^{-1} : L(H, Z_N) \to L(H, Z_{\dot{m}}[i]),$$

а значит, и между характерами группы $H = G_{h_1} \times G_{h_2} \times \ldots \times G_{h_m}$ над кольцом Z_N:

$$\chi_{\alpha_1\alpha_2\ldots\alpha_m}(n_1, n_2, \ldots n_m) = \rho(\varepsilon_1)^{\alpha_1 n_1} \rho(\varepsilon_2)^{\alpha_2 n_2} \ldots \rho(\varepsilon_m)^{\alpha_m n_m} \quad (5.29)$$

и над кольцом $Z_{\dot{m}}[i]$:

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(n_1, n_2, \ldots, n_m) = \varepsilon_1^{\alpha_1 n_1} \varepsilon^{\alpha_n n_2} \ldots \varepsilon_m^{\alpha_n n_m}. \quad (5.30)$$

Действуя изоморфизмом ρ на комплексные числа $\varepsilon_k = 2k + i\beta_k$ ($k = 1, 2, \ldots, n$) мультипликативной группы кольца $Z_{\dot{m}}[i]$, получаем целые рациональные числа $\rho(\varepsilon_k)$. При этом функции (5.29) будут образовывать ортогональный базис в пространстве $L(H, Z_N)$. Другими словами, образом χ-базиса Гаусса (5.30) при изоморфизме ρ будет некоторый симплексный базис (5.29).

Пусть, например, $h_k = p$, $k = 1, 2, \ldots, n$. Тогда преобразования ρ и ρ^{-1} устанавливают взаимно однозначное соответствие между базисами Крестенсона — Галуа типа H, Z_N и базисами Крестенсона — Гаусса типа $HZ_{\dot{m}}[i]$. Особый интерес с точки зрения цифровых расчетов на ЦВМ представляет связь между базисом Крестенсона — Рейдера и его прообразом в пространстве $L(H, Z_{\dot{m}}[i])$, т. е. соответствующим базисом Крестенсона — Гаусса типа H, $Z_{\dot{m}}[i]$. При этом

$$\chi_{\alpha_1\alpha_2\ldots\alpha_n}(n_1, n_2, \ldots, n_m) = 2^{\alpha_1 n_1 + \alpha_2 n_2 + \ldots + \alpha_m n_m}, \quad Z_N; \quad (5.31)$$

$$\rho(\chi_{\alpha_1\alpha_2\ldots\alpha_m}(n_1, n_2, \ldots, n_m)) = \varepsilon^{\alpha_1 n_1 + \alpha_2 n_2 + \ldots + \alpha_m n_m}, \quad Z_m[i]. \quad (5.32)$$

Следовательно, изоморфизм ρ является универсальным средством, связывающим комплексные и действительные ТЧП.

* * *

Таким образом, ТЧП могут определяться над любой конечной абстрактной алгебраической системой, обладающей структурой кольца. Однако при выборе конкретной системы необходимо решить ряд задач математического характера, связанных с поиском подходящих

первообразных элементов. Важным моментом является то, что всегда существует изоморфизм между симплексными и комплексными (гиперкомплексными) ТЧП.

Реализация арифметических операций кольца $Z_m[i]$ (или Z_p^c), вообще говоря, не проще по сравнению с реализацией операций поля комплексных чисел. Тем не менее в связи с возможностью выбора первообразного элемента, умножение на степени которого реализуется просто, комплексные ТЧП представляют определенный интерес. Кроме того, в случае применения комплексных и гиперкомплексных ТЧП, как и при использовании симплексных ТЧП, отсутствует шум округлений при вычислениях. Важной является возможность погружения комплексного пространства в модулярное и замены комплексных вычислений при реализации ТЧП модульными вычислениями.

ГЛАВА 6

ПРЕОБРАЗОВАНИЕ СПЕКТРОВ ЦИФРОВЫХ СИГНАЛОВ

1. Постановка задачи

В ряде случаев при гармоническом анализе, а также при обработке, использующей спектральное представление сигналов, необходимо преобразование спектра цифрового сигнала из одного базиса в другой. Преобразование спектров можно проводить, например, с целью физической интерпретации, удобства и повышения эффективности обработки.

Пусть $S_1(\alpha)$ — спектр цифрового сигнала $x(n)$, полученный в результате вычисления χ-преобразования, определенного в пространстве $L_1(G_{m_1}, K_1)$, и $S_2(\alpha)$ — спектр этого же сигнала, но полученный в результате вычисления χ-преобразования, определенного в пространстве $L_2(G_{m_2}, K_2)$. Тогда задача преобразования спектров в общем виде сводится к нахождению в аналитическом виде и реализации отображения

$$S_1(\alpha) \to S_2(\alpha). \tag{6.1}$$

При этом возможны следующие четыре случая:

1) $G_{m_1} = G_{m_2} = G_m$, $K_1 = K_2 = K$;
2) $G_{m_1} \neq G_{m_2}$, $K_1 = K_2 = K$;
3) $G_{m_1} = G_{m_2} = G_m$, $K_1 \neq K_2$;
4) $G_{m_1} \neq G_{m_2}$, $K_1 \neq K_2$.

Первый случай тривиален. Пространства $L_1(G_{m_1}, K_1)$ и $L_2(G_{m_2}, K_2)$, а следовательно, и спектры $S_1(\alpha)$ и $S_2(\alpha)$ совпадают.

Во втором случае необходимо решить задачу преобразования спектра сигнала $x(n)$ из базиса, соответствующего структуре группы G_{m1}, в базис, соответствующий структуре группы G_{m_2}, причем оба базиса определены над одним и тем же кольцом K. Эта задача легко решается, если $m_1 = m_2 = m$, т. е. области определения сигналов совпадают и различна только структура группы G_m. Запишем выражения для спектров $S_1(\alpha)$ и $S_2(\alpha)$:

$$S_1(\alpha) = \sum_{n=0}^{m-1} x(n)\, {}_1\chi_\alpha^{-1}(n), \quad \alpha = 0,1, \ldots, m-1; \tag{6.2}$$

$$S_2(\alpha) = \sum_{n=0}^{m-1} x(n)\, {}_2\chi_\alpha^{-1}(n), \quad \alpha = 0,1, \ldots, m-1. \tag{6.3}$$

Из выражения (6.2) находим значение сигнала $x(n)$:

$$x(n) = N^{-1} \sum_{\alpha=0}^{m-1} S_1(\alpha)\, {}_1\chi_\alpha(n)$$

и подставим его в выражение (6.3). Тогда

$$S_2(\alpha) = N^{-1} \sum_{n=0}^{m-1} \sum_{\alpha=0}^{m-1} S_1(\alpha)\, {}_1\chi_\alpha(n)\, {}_2\chi_\alpha^{-1}(n) =$$

$$= N^{-1} \sum_{\alpha=0}^{m-1} S_1(\alpha) \sum_{n=0}^{m-1} {}_1\chi_\alpha(n)\, {}_2\chi_\alpha^{-1}(n).$$

Обозначим

$${}_{21}\chi_\alpha(n) = N^{-1} \sum_{n=0}^{m-1} {}_1\chi_\alpha(n)\, {}_2\chi_\alpha^{-1}(n). \qquad (6.4)$$

Функцию, задаваемую выражением (6.4), назовем ядром χ-преобразования (по аналогии с ядром Фурье, рассматриваемым в работе [160]). Следовательно, в этом случае спектры $S_1(\alpha)$ и $S_2(\alpha)$ связаны линейным преобразованием

$$S_2(\alpha) = \sum_{\alpha=0}^{m-1} S_1(\alpha)\, {}_{21}\chi_\alpha(n). \qquad (6.5)$$

Если $G_{m_1} = G_{m_2} = G_m$ и $K_1 \neq K_2$, то задача преобразования спектров существенно усложняется. Сигнал $x(n)$ разлагается в одном и том же базисе, но определяемом над различными кольцами K_1 и K_2 (либо различными полями). Значит, при вычислении $S_1(\alpha)$ и $S_2(\alpha)$ используются две различные арифметики: арифметика кольца K_1 и арифметика кольца K_2. Поэтому задача сводится к преобразованию значений спектра $S_1(\alpha)$ из кольца K_1 в кольцо K_2. Ниже рассматривается важный, с точки зрения практического применения, случай, когда в качестве колец K_1 и K_2 используется поле комплексных чисел и поле Галуа.

Наконец, в случае, когда $G_{m_1} \neq G_{m_2}$ и $K_1 \neq K_2$, задачу преобразования спектров можно представить в виде композиции двух подзадач: а) преобразование значения спектра $S_1(\alpha)$ из кольца K_1 в кольцо K_2, $S_1(\alpha) \to S_1^2(\alpha)$; б) вычисления спектра $S_2(\alpha)$ по выражению (6.5). Как указывалось, вторая часть задачи разрешима просто. Основная проблема — это решение первой подзадачи.

2. Преобразование значений спектральных коэффициентов из поля комплексных чисел в поле Галуа

Итак, пусть задан цифровой сигнал $x(n)$. В соответствии со структурой группы G_N в области определения этого сигнала построены системы базисных функций над полем комплексных чисел C и над полем Галуа GF (p^v), т. е. определены χ-преобразования в пространствах $L_1(G_N, C)$ и $L_2(G_N, \mathrm{GF}(p^v))$. Обозначим

через $X(\alpha)$ спектр сигнала $x(n)$ в базисе над полем C и через $S(\alpha)$ — спектр этого же сигнала в этом же базисе, но над полем GF (p^v). Следовательно, необходимо найти аналитическое выражение для отображения

$$f_1 : X(\alpha) \to S(\alpha). \tag{6.6}$$

Рассмотрим поля C и GF (p^v) как векторные пространства. Обозначим их соответственно через V_C и V_P. Тогда спектральные коэффициенты $X(\alpha_i)$ и $S(\alpha_i)$ при некотором значении $\alpha = \alpha_i$ $(i = 0, 1, \ldots, N-1)$ можно представить как векторы этих векторных пространств. Задача преобразования спектров (см. (6.6)) сводится к преобразованию векторов из векторного пространства V_C в векторное пространство V_P, т. е. преобразование спектра может производиться «поточечно» — отдельно для каждого спектрального коэффициента $X(\alpha_i)$ спектра $X(\alpha)$. Пространство V_C — двухмерное, а пространство V_P одномерное. Преобразование значения спектрального коэффициента $X(\alpha_i)$ в поле GF (p^v) можно осуществить, умножив его слева на матрицу некоторого оператора и «согласовав» арифметику поля C и поля GF (p^v).

Обозначим оператор, преобразующий значение спектрального коэффициента $X(\alpha_i)$ в множество действительных чисел R, через A. Матрицу этого оператора обозначим такой же буквой и она будет представлять собой матрицу размерности $1 \times 2 : A = [a_1, a_2]$, где $a_1, a_2 \in R$. Соответствующий коэффициенту $X(\alpha_i)$ коэффициент $S(\alpha_i)$ находим по формуле

$$S(\alpha_i) = \lambda\{]AX(\alpha_i)[\}, \tag{6.7}$$

где скобки] [обозначают округление до ближайшего целого числа; λ — оператор, согласующий арифметику кольца целых чисел Z (результат умножения $AX(\alpha_i)$ и последующего округления принадлежит кольцу Z) и поля GF (p^v), т. е. оператор, ставящий в соответствие каждому целому числу определенный элемент поля GF (p^v); $X(\alpha_i)$ — вектор-столбец, элементы которого представляют собой действительную Re $X(\alpha_i)$ и мнимую Im $X(\alpha_i)$ части коэффициента $X(\alpha_i)$; $X'(\alpha_i) = [\mathrm{Re}\ X(\alpha_i), \mathrm{Im} X(\alpha_i)]$; t — знак транспонирования. Так как спектральные коэффициенты являются линейной комбинацией степеней первообразного элемента ε, матрицу оператора A можно найти из условий

$$\left.\begin{aligned} &\lambda\{A\varepsilon^0\} = (\varepsilon')^0; \\ &\lambda\{A\varepsilon\} = (\varepsilon'); \\ &\lambda\{A\varepsilon^2\} = (\varepsilon')^2; \\ &\quad\ldots\ldots\ldots\ldots \\ &\lambda\{A\varepsilon^{N-1}\} = (\varepsilon')^{N-1} \end{aligned}\right\}, \tag{6.8}$$

где $\varepsilon' \in$ GF (p^v), $\varepsilon \in C$. Число уравнений в системе (6.8) равно числу различных значений степеней первообразного элемента ε. Заметим, что число различных значений степеней первообразного элемента ε равно числу различных значений степеней первообразного элемента ε', так как степени элементов ε и ε' образуют характеры одной и той

же группы G_N, определенные соответственно над полем комплексных чисел C и над полем Галуа GF (p^v). Максимальное число различных значений степеней ε равно N, что соответствует структуре группы $G_N = G_N$, т. е. N не представляется в виде произведения своих сомножителей (базис Фурье). Если выбрать структуру группы $G_N = G_{n_1} \times G_{n_2} \times \ldots \times G_{N_i}$ $(i = 1, 2, \ldots, m)$, где $N = n_1 n_2 \ldots n_i$, то систему характеров этой группы можно представить в виде

$$\chi_{\alpha_1 \alpha_2 \ldots \alpha_m}(n) = \chi_{\alpha_1}(n_1) \times \chi_{\alpha_2}(n_2) \times \cdots \times \chi_{\alpha_m}(n_m), \qquad (6.9)$$

где $\chi_{\alpha_i}(n_i)$ — система дискретных экспоненциальных функций, определенных для группы G_{n_i}.

Очевидно, что максимальное число различных степеней первообразного элемента $\varepsilon = \varepsilon_1 \varepsilon_2 \ldots \varepsilon_m$, порождающего систему характеров (6.9), равно произведению $n_1 n_2 \ldots n_i = N$. Значит, для любого базиса число уравнений в системе (6.8) не превышает N. Решив эту систему для худшего случая, когда число уравнений равно N, найдем значение матрицы оператора A, которое будет одним и тем же для базиса, соответствующего любому разложению N на сомножители. Следует заметить, что для заданной конкретной структуры группы G_N и базиса, порождаемого этой группой, число уравнений в (6.8) может быть значительно меньшим N. Например, если $G_N = G_p \times G_p \times \ldots \times G_p$, то число уравнений в (6.8) равно p (а не p^m).

Предположим, что базисные функции определяются над простым полем Галуа GF (p) $(v = 1)$. Тогда система (6.8) преобразуется к виду

$$\left.\begin{aligned} A\varepsilon^0 &\equiv (\varepsilon')^0 \bmod p; \\ A\varepsilon &\equiv \varepsilon' \bmod p; \\ A\varepsilon^2 &\equiv (\varepsilon')^2 \bmod p; \\ &\ldots\ldots\ldots\ldots \\ A\varepsilon^{N-1} &\equiv (\varepsilon')^{N-1} \bmod p; \end{aligned}\right\} \qquad (6.10)$$

В этом случае оператор λ (см. (6.7)) представляет собой оператор сравнения по модулю p, λ_p:

$$\lambda_p h = h \pm lp; \quad h,\ l \in \boldsymbol{Z},\ (h \pm lp) \in \mathrm{GF}(p).$$

Учитывая, что ε^k записывается через свои действительную и мнимую части в виде $\varepsilon^k = [\mathrm{Re}\ \varepsilon^k, \mathrm{Im}\ \varepsilon^k]$, систему (6.10) можно записать следующим образом:

$$\begin{bmatrix} \mathrm{Re}\,\varepsilon^0 & \mathrm{Im}\,\varepsilon^0 \\ \mathrm{Re}\,\varepsilon & \mathrm{Im}\,\varepsilon \\ \mathrm{Re}\,\varepsilon^2 & \mathrm{Im}\,\varepsilon^2 \\ \ldots\ldots & \ldots\ldots \\ \mathrm{Re}\,\varepsilon^{N-1} & \mathrm{Im}\,\varepsilon^{N-1} \end{bmatrix} \begin{bmatrix} a_1 & a_1 & a_1 & \cdots & a_1 \\ a_2 & a_2 & a_2 & \cdots & a_2 \end{bmatrix} \equiv$$

$$\equiv \begin{bmatrix} (\varepsilon')^0 & & & \\ & \varepsilon' & & \\ & & (\varepsilon')^2 & \\ & & & \ddots \\ & & & (\varepsilon')^{(N-1)} \end{bmatrix} \bmod p. \qquad (6.11)$$

Вводя обозначения для матриц в выражении (6.11), получаем

$$\check{B}A^t \equiv \check{D} \bmod p.$$

Общее выражение для нахождения спектра $S(\alpha)$ следующее:

$$\begin{bmatrix} S(0) \\ S(1) \\ \vdots \\ S(N-1) \end{bmatrix} =$$

$$= \begin{bmatrix} \lambda_p & & & \\ & \lambda_p & & \\ & & \ddots & \\ & & & \lambda_p \end{bmatrix} \left\{ \begin{bmatrix} A & & & \\ & A & & \\ & & \ddots & \\ & & & A \end{bmatrix} \begin{bmatrix} X(0) \\ X(1) \\ \vdots \\ X(N-1) \end{bmatrix} \right\}. \qquad (6.12)$$

Каждое произведение AX (i) в (6.12) округляется до ближайшего целого числа, что условно показано в виде «обратных» квадратных скобок] [.

Выражение (6.11) представляет собой систему N сравнений первой степени с двумя неизвестными a_1 и a_2, которая разрешима, в частности, для множества векторов D, лежащих в гиперплоскости, являющейся линейной оболочкой вектор-столбцов матрицы $\check{B}$. Число сравнений в системе (6.11) больше числа неизвестных, т. е. эта система переопределенная. Практическое решение переопределенных систем сравнений является нерешенной математической проблемой [158]. Еще сложнее решение систем уравнений вида (6.8). Подобные исследования выходят за рамки настоящей работы. Ограничимся приведением в табл. 30 значений матрицы оператора A, которые удалось получить эвристическим путем, для некоторых значений N, структур группы G_N и полей Галуа GF (p).

Описанное преобразование спектров использовалось в работах [27, 37, 38, 41] при спектральном синтезе функций k-значной логики. Здесь эти результаты обобщаются и используются для преобразования спектров цифровых сигналов.

Пример 6.1. Пусть задан цифровой сигнал $x(n)$, который запишем в виде транспонированного вектор-столбца $x^t(n) = [3; 4; 5; 5; 4; 2]$. Спектры его в базисе дискретных экспоненциальных функ-

Таблица 30. Значения матрицы оператора A

N	Структура группы G	Первообразный элемент	Поле GF (p)		
			GF (3)	GF (5)	GF (7)
2	2	$\varepsilon = p - 1$	[1, 0]	[1, 0]	[1, 0]
2^m	$\underbrace{2 \cdot 2 \ldots 2}_{m}$	$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m = p - 1$	[1, 0]	[1, 0]	[1, 0]
3	3	$\varepsilon = 2$			$\left[1, \frac{5}{\sqrt{3}}\right]$
3^m	$\underbrace{3 \cdot 3 \ldots 3}_{m}$	$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m = 2$			$\left[1, \frac{5}{\sqrt{3}}\right]$
4	4	$\varepsilon = 3$		[1, 3]	
4^m	$\underbrace{4 \cdot 4 \ldots 4}_{m}$	$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m = 3$		[1, 3]	
6	6	$\varepsilon_1 = 3$			$\left[1, \frac{5}{\sqrt{3}}\right]$
6	$2 \cdot 3$	$\varepsilon_1 = 2,\ \varepsilon_2 = 3$			$\left[1, \frac{5}{\sqrt{3}}\right]$
6^m	$\underbrace{6 \cdot 6 \ldots 6}_{m}$	$\varepsilon_1 = \varepsilon_2 = \ldots = \varepsilon_m = 3$			$\left[1, \frac{5}{\sqrt{3}}\right]$

ций (базис Фурье) и в аналогичном базисе, но определенном над полем GF (7), равны:

$$X^t(\alpha) = [23;\ (-3{,}50 - i2{,}60);\quad (0{,}50 - i0{,}87);\quad (0{,}50 + i0{,}87);\quad (-3{,}50 + i2{,}60)]; \tag{6.13}$$

$$S^t(\alpha) = [2;\ 3;\ 5;\ 1;\ 3;\ 4]. \tag{6.14}$$

Вычислим по выражению (6.7) коэффициент S (2):

$$S(2) = \lambda_p \left\{ [1,\ 2{,}89] \begin{bmatrix} 0{,}50 \\ -0{,}87 \end{bmatrix} \right\} = \lambda_p \{ |0{,}5 - 2{,}52| \} = \lambda_p (-2) = -2 + 7 = 5.$$

Значения матрицы оператора $A = [1;\ 5/\sqrt{3}] = [1;\ 2{,}89]$ (см. табл. 30) взяты с точностью до 0,01. Вычисления проводились с такой же точностью. Полученное значение S (2) совпадает со значением, вычисленным непосредственно по выражению для ПФГ (см. (6.14)). Аналогично вычисляются другие коэффициенты $S(\alpha_i)$.

Упражнение 6.1. Вычислить значение коэффициентов S (0) и S (5) (см. пример 6.1).

Заметим, что результаты вычислений по выражению (6.7) зависят от точности вычислений. Если абсолютная погрешность округлений, получаемая при нахождении произведения $AX(\alpha_i)$, не превосходит величины, равной половине интервала квантования $\Delta/2$ ($\Delta = 1/k$), то значение $S(\alpha_i)$, вычисленное по (6.7), будет соответствовать абсолютно точному значению $X(\alpha_i)$, выраженному в радикалах. Так, в примере 6.1 получено истинное значение коэффициента $S(2)$, хотя соответствующий ему коэффициент $X(2) = 0{,}50 - i0{,}87$ определен с точностью до 0,01 (действительная и мнимая части).

Упражнение 6.2. Вычислить значение коэффициентов $S(2)$ и $S(5)$ (см. пример 6.1) с точностью до 0,1 и 0,5.

Трудности, возникающие при решении системы сравнений (6.10) и системы уравнений (6.8), обусловили необходимость поиска других методов преобразования значений спектральных коэффициентов из поля комплексных чисел в поле Галуа. Для краткости условимся называть такое преобразование переходом $X(\alpha) \to S(\alpha)$. Изучим метод перехода $X(\alpha) \to S(\alpha)$, при применении которого не требуются сложные предварительные вычисления, связанные с нахождением матрицы оператора A [28].

Рассмотрим последовательность степеней первообразного элемента $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1}$ при таком значении α_i, чтобы все степени ε^i были различными на комплексной плоскости (рис. 20). Выражение для произвольного вектора на этой плоскости, представляющей значение спектрального коэффициента $X(\alpha_i)$, можно записать в виде

$$X(\alpha_i) = \varepsilon^r \{|| X(\alpha_i) || \} + \zeta, \tag{6.15}$$

где $|| X(\alpha_i) ||$ — значение модуля комплексного числа, представляющего $X(\alpha_i)$, округленное до ближайшего целого числа; $\zeta = X(\alpha_i) - \varepsilon^r \{|| X(\alpha_i) ||\}$ — некоторый вектор. Значение r вычисляется по формуле

$$r = \left] \frac{\operatorname{arctg} \dfrac{\operatorname{Im} X(\alpha_i)}{\operatorname{Re} X(\alpha_i)}}{\beta} \right[\tag{6.16}$$

и принадлежит множеству E_N ($r \in E_N$). Учитывая, что $\beta = 2\pi/N$, выражение (6.16) можно преобразовать к виду

$$r = \left] \frac{N \operatorname{arctg} \dfrac{\operatorname{Im} X(\alpha_i)}{\operatorname{Re} X(\alpha_i)}}{2\pi} \right[. \tag{6.17}$$

Вектор ζ можно приближенно представить следующим образом:

$$\zeta = \varepsilon^{r_1} \{|| \zeta || \} = \zeta', \tag{6.18}$$

где r_1 вычисляется по выражению, аналогичному (6.17):

$$r_1 = \left] \frac{N \operatorname{arctg} \dfrac{\operatorname{Im} \zeta}{\operatorname{Re} \zeta}}{2\pi} \right[. \tag{6.19}$$

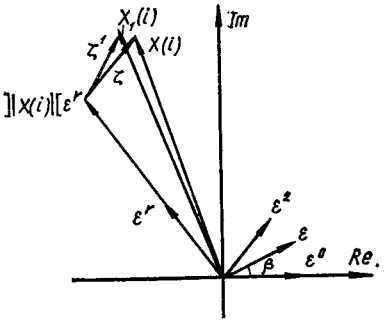


Рис. 20. Приближенное представление спектральных коэффициентов.

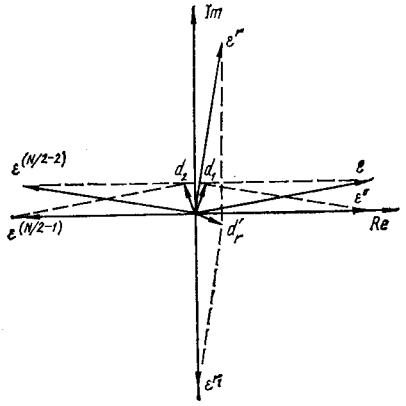


Рис. 21. Схема образования новой системы опорных координат.

Подставляя в (6.15) вместо ζ значение ζ', получаем приближенное представление $X(\alpha_i)$:

$$X(\alpha_i) = \varepsilon^r \{[\,|X(\alpha_i)|\,[\}\} + \varepsilon^{r_1}\{[\,|\zeta|\,[\}\} = X_1(\alpha_i). \qquad (6.20)$$

Теперь, зная соответствия $\varepsilon^0 \to (\varepsilon')^0$, $\varepsilon \to \varepsilon'$, ..., $\varepsilon^r \to (\varepsilon')^r$, ..., $\varepsilon^{(N-1)} \to$ $\to (\varepsilon')^{N-1}$ и подставляя значения $(\varepsilon')^r$ в выражение (6.20), можно вычислить коэффициент $S(\alpha_i)$, соответствующий коэффициенту $X(\alpha_i)$:

$$S(\alpha_i) = \{(\varepsilon')^r \lambda([\,|X(\alpha_i)|\,[) + (\varepsilon')^{r_1}\lambda([\,|\zeta|\,[)\} \bmod \mathrm{d}(p, f(x)), \qquad (6.21)$$

где

$$\zeta = X(\alpha_i) - \varepsilon^r \{[\,|X(\alpha_i)|\,[\}. \qquad (6.22)$$

Символ mod d $(p, f(x))$ в (6.21) означает, что операции выполняются по модулю p и по модулю неприводимого над GF (p) полинома $f(x)$ $(S(\alpha_i) \in \mathrm{GF}(p^v))$. Если $S(\alpha_i) \in \mathrm{GF}(p)$, то операции в (6.21) выполняются по модулю p и $\lambda = \lambda_p$. Соответствия $\varepsilon^0 \to (\varepsilon')^0$, $\varepsilon \to$ $\to \varepsilon'$, ... $\varepsilon^r \to (\varepsilon')^r$, ..., $\varepsilon^{N-1} \to (\varepsilon')^{N-1}$ должны быть установлены заранее и сохраняются в памяти вычислительного устройства. Установление их не вызывает принципиальных трудностей и не требует больших вычислительных затрат, так как сводится к построению характеров $\chi_{\alpha_i}(n)$ над полем комплексных чисел и над полем Галуа.

Заметим, что вместо последовательности степеней первообразного элемента ε^0, ε, ε^2, ..., ε^{N-1} можно использовать любые другие векторы d_1, d_2, ..., d_m, выходящие из начала координат, для которых установлены соответствия $d_1 \to d'_1$, $d_2 \to d'_2$, ..., $d_m \to d'_m$ $(d'_i \in$ $\in \mathrm{GF}(p^v)$, $i = 1, 2, \ldots, m)$. Наиболее удобно, когда векторы $d_1, d_2, \ldots$ ..., d_m являются степенями какого-то одного вектора d_i. Последовательность векторов $d_1, d_2, \ldots, d_m$ может выбираться таким образом, чтобы уменьшалась погрешность представления вектора ζ. Для этого число векторов $d_1, d_2, \ldots, d_m$ выбирается большим N $(m > N)$,

в связи с чем уменьшается угол β и увеличивается точность представления. Этот факт непосредственно следует из геометрической интерпретации выражения (6.20) (см. рис. 20). Кроме того, увеличить точность представления можно уменьшением модуля $|d_i|$ каждого из последовательности векторов $d_1, d_2, \ldots, d_m$. Вектор d_i может представлять собой линейную комбинацию нескольких векторов ε^r. В качестве примера на рис. 21 показано, каким образом можно получить векторы d_i с меньшими значениями модулей $|d_i|$ по сравнению с модулем вектора ε^r. Используя описанные приемы, можно добиться любой наперед заданной точности представления вектора ζ (см. (6.16)), а значит, и любой точности представления коэффициента $X(\alpha_i)$, естественно, не превышающей точности вычисления коэффициента $X(\alpha_i)$.

В заключение рассмотрим пример, иллюстрирующий процесс вычислений по выражениям (6.17), (6.19), (6.21), (6.22).

Пример 6.2. Пусть задан цифровой сигнал $x(n)$ и его спектры $X(\alpha)$ и $S(\alpha)$, приведенные в примере 6.1. Вычислим спектральный коэффициент $S(5)$. Последовательно по (6.17), (6.22), (6.19) и (6.21) получаем

$$r = \left]\frac{6\operatorname{arctg}\left(-\frac{2{,}6}{3{,}5}\right)}{2\pi}\right[= \left]\frac{6\cdot 2{,}5}{6{,}28}\right[= 2;$$

$$\zeta = -3{,}5 + i2{,}6 - \operatorname{Re}\varepsilon^2\{]\sqrt{(3{,}5)^2+(2{,}6)^2}[\} - \operatorname{Im}\varepsilon^2 \times$$

$$\times\{]\sqrt{(3{,}5)^2+(2{,}6)^2}[\} = -1{,}5 - i0{,}86;\ r_1 = \left]\frac{6\operatorname{arctg}\left(-\frac{0{,}86}{1{,}5}\right)}{2\pi}\right[= 4;$$

$$S(5) = \{3^2\cdot\lambda_p(4) + 3^4\lambda_p(]\sqrt{1{,}5^2+0{,}86^2}[)\} \bmod 7 = 4.$$

Здесь первообразному элементу $\varepsilon = 0{,}5 + i\sqrt{3/2}$ соответствует первообразный элемент $\varepsilon' = 3$; $\varepsilon' \in GF(7)$. Полученное значение коэффициента $S(5)$ совпадает со значением, вычисленным непосредственно по формулам ПФГ. Следовательно, погрешность представления коэффициента $X(5)$ небольшая и ликвидируется округлениями в выражениях (6.17), (6.19), (6.21) и (6.22).

3. Условия существования однозначного соответствия между значениями спектра в поле комплексных чисел и в поле Галуа

В общем случае отображение $X(\alpha_i) \to S(\alpha_i)$ не является взаимно однозначным. Одному значению $X(\alpha_i)$ может соответствовать несколько значений $S(\alpha_i)$. Для того чтобы был возможен «поточечный» переход $S(\alpha_i) \to X(\alpha_i)$, необходимо, чтобы упомянутое отображение было взаимно однозначным. Это означает, что мощность множества различных значений некоторого спектрального коэффициента $S(\alpha_i)$ должна быть равной мощности множества различных значений соответствующего ему коэффициента

$X(\alpha_i)$. Так как множество различных значений коэффициента $S(\alpha_i)$ не превосходит порядка поля Галуа GF (p), указанное условие однозначности перехода $S(\alpha_i) \to X(\alpha_i)$ можно сформулировать следующим образом: порядок поля Галуа GF (p), над которым определены χ-преобразование и спектр $S(\alpha)$, полученный в результате этого преобразования, должен быть не меньше мощности $P\{X(\alpha_i)\}$ множества различных значений коэффициента $X(\alpha_i)$, определенного над полем комплексных чисел при таком значении α_i, когда $P\{X(\alpha_i)\}$ максимальна, т. е.

$$p \geqslant P\{X(\alpha_i)\}. \tag{6.23}$$

Оценим порядок поля Галуа, необходимый для существования однозначного перехода $S(\alpha_i) \to X(\alpha_i)$.

Теорема 6.1. Мощность множества различных значений спектрального коэффициента $X(\alpha_i)$, полученного в результате вычисления χ-преобразования в пространстве $L(G_N, C)$, при структуре группы G_N, соответствующей базису Фурье (G_N не представляется в виде прямого произведения своих подгрупп), и таком значении α_i, что мощность указанного множества максимальна в случае $N = p_1^{r_1} \times \times p_2^{r_2} \ldots p_m^{r_m}$ (p_i — простые числа, $r = 0, 1, 2, \ldots$), удовлетворяет неравенству

$$P\{X(\alpha_i)\} \leqslant ([k^{p_1} - (k-1)^{p_1}]^{r_1})([k^{p_2} - (k-1)^{p_2}]^{r_2}) \times \cdots$$

$$\cdots \times ([k^{p_m} - (k-1)^{p_m}]^{r_m}) = W_1. \tag{6.24}$$

Напомним, что k — число элементов множества значений цифрового сигнала E_k.

Доказательству теоремы 6.1 предпошлем лемму.

Лемма 6.1 [37, 41]. Мощность множества различных значений спектрального коэффициента $X(\alpha_i)$ (условия получения коэффициента $X(\alpha_i)$ те же, что и в теореме 6.1) при N, равном простому числу, определяется выражением

$$W_2 = P\{X(\alpha_i)\} = k^N - (k-1)^N. \tag{6.25}$$

Доказательство. Спектральный коэффициент $X(\alpha_i)$ можно интерпретировать как вектор в N-мерном векторном пространстве, базис которого составляют векторы $\varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{N-1}$, т. е. степени первообразного элемента. Следовательно, любой коэффициент $X(\alpha_i)$ ($i = 0, 1, \ldots, N-1$) может быть записан в виде

$$X(\alpha_i) = x(0)\varepsilon^0 + x(1)\varepsilon + x(2)\varepsilon^2 + \cdots + x(N-1)\varepsilon^{N-1}. \tag{6.26}$$

Выражение (6.26) представляет круговое целое число [178] при простом показателе степени N. В работе [178] доказана теорема для круговых целых, утверждающая, что если

$$x_1(0)\varepsilon^0 + x_1(1)\varepsilon + x_1(2)\varepsilon^2 + \cdots + x_1(N-1)\varepsilon^{N-1} =$$
$$= x_2(0)\varepsilon^0 + x_2(1)\varepsilon + x_2(2)\varepsilon^2 + \cdots + x_2(N-1)\varepsilon^{N-1}$$

— два равных круговых целых числа, то обязательно выполняются следующие равенства:

$$x_1(0) - x_2(0) = x_1(1) - x_2(1) = \cdots = x_1(N-1) - x_2(N-1).$$

Отсюда следует, что значения коэффициента $X(\alpha_i)$ одинаковы для одного и того же сигнала $x(n)$ либо для различных сигналов $x_1(n)$ и $x_2(n)$, отличающихся постоянной составляющей, т. е. сигналов, для которых

$$x_1(0) - x_2(0) = x_1(1) - x_2(1) = \cdots = x_1(N-1) - x_2(N-1).$$

Назовем сигнал $x(n)$ основным, если у него хотя бы одно значение $x(n_i)$ $(i = 0, 1, \ldots, N-1)$ равно нулю. Сигналы, отличающиеся от основного сигнала на постоянную составляющую, образуют группу сигналов, порождаемую основным сигналом $x(n)$. В случае если у основного сигнала есть еще хотя бы одно значение $x(n_j)$ $(j \neq i)$, равное $k-1$, то группа состоит из одного такого сигнала. При N простом задача нахождения мощности множества различных значений спектрального коэффициента $X(\alpha_i)$ сводится к подсчету числа групп сигналов или к подсчету сигналов, имеющих хотя бы одно нулевое значение $x(n_i)$.

Запишем транспонированные вектор-столбцы значений цифрового сигнала $x(n)$ в виде списка:

$$\left.\begin{array}{l} 0,\ 0,\ 0,\ \ldots,\ 0; \\ 0,\ 0,\ 0,\ \ldots,\ 1; \\ 0,\ 0,\ 0,\ \ldots,\ 2; \\ \ldots\ldots\ldots \\ k-1,\ k-1,\ k-1,\ \ldots,\ k-1. \end{array}\right\} \quad (6.27)$$

N значений

Каждую строчку в (6.27) можно рассматривать как некоторое N-разрядное число в k-значной системе счисления. Пусть эти числа упорядочены естественным образом (в порядке возрастания величины числа). Тогда число наборов (строк в списке (6.26)), у которых $x(0) = 0$, равно k^{N-1}; число наборов, у которых $x(1) = 0$, равно $(k-1)\,k^{(N-2)}$ (исключая те наборы, у которых $x(0) = 0$ и $x(1) = 0$); число наборов, у которых $x(2) = 0$, равно $(k-1)^2\,k^{(N-2)}$ (исключая те наборы, у которых $x(0) = 0$, $x(1) = 0$ и $x(2) = 0$). Продолжая таким образом дальше и суммируя результаты, получаем

$$W_2' = \sum_{i=0}^{N-1} (k-1)^i\, k^{(N-i-1)}.$$

Докажем, что $W_2 = W_2'$, т. е. что

$$\sum_{i=0}^{N-1} (k-1)^i k^{(N-i-1)} = k^N - (k-1)^N.$$

Разделим почленно левую и правую части этого равенства на $k^{(N-1)}$. Тогда

$$\sum_{i=0}^{N-1} (k-1)^i k^{-i} = \frac{k^N - (k-1)^N}{k^{(N-1)}}. \qquad (6.28)$$

Левая часть (6.28) представляет собой геометрическую прогрессию. Записав в левой части равенства (6.28) значение суммы геометрической прогрессии [79], найдем

$$\frac{1 - \left(\frac{k-1}{k}\right)^N}{1 - \frac{k-1}{k}} = k - \frac{(k-1)^N}{k^{(N-1)}} = \frac{k^N - (k-1)^N}{k^{N-1}}.$$

Равенство левой и правой частей (6.27) доказано, что завершает доказательство леммы 6.1.

Доказательство теоремы 6.1. Пусть $N = p^r$. Тогда первообразный элемент ε можно представить в виде $\varepsilon = \varepsilon_1\varepsilon_2 \ldots$ $\ldots \varepsilon_r$ и последовательность степеней ε можно разбить на p^r/p подпоследовательностей, в каждой из которых p элементов. Причем последовательность степеней каждого элемента ε_i совпадает с последовательностью степеней первообразного элемента ε_p для $N = p$ в базисе Фурье. Каждую подпоследовательность можно рассматривать как базис p-мерного векторного пространства. Поскольку N-мерное векторное пространство, в котором коэффициент $X(\alpha_i)$ представляется в виде вектора, равно прямой сумме p^r/p p-мерных пространств,

$$P\{X(\alpha_i)\} = [k^p - (k-1)^p]^r. \qquad (6.29)$$

Однако последовательность степеней первообразного элемента ε (ε^0, ε, ε^2, ..., ε^{N-1}) является проекцией p^r-мерного векторного пространства на комплексную плоскость. Интерпретировать последовательность ε^0, ε, ε^2, ..., ε^{N-1} как базис N-мерного векторного пространства можно только тогда, когда между элементами этой последовательности отсутствует линейная зависимость. В этом случае отсутствие линейной зависимости означает, что уравнение

$$a_0\varepsilon^0 + a_1\varepsilon + a_2\varepsilon^2 + \cdots + a_{N-1}\varepsilon^{N-1} = 0$$

имеет решение только при всех $a_i = 0$. На рис. 22 показана система степеней первообразного элемента ε_0, ε, ε^2 для $N = p = 3$, являющаяся базисом трехмерного векторного пространства. На ее основе построена целочисленная решетка. Любая точка с целыми координатами представляет значение некоторого коэффициента $X(\alpha_i)$. На рис. 23 показана проекция этой целочисленной решетки на комплексную плоскость. Проекция осуществлена таким образом, что ось OO' (см. рис. 22) перпендикулярна плоскости рисунка. При этом точки целочисленной решетки, которые при проекции слились в одну точку, представляют значения спектрального коэффициента, соответствующие цифровым сигналам, отличающимся постоянной составляющей, т. е. группе сигналов. Ввиду симметрии рисунка

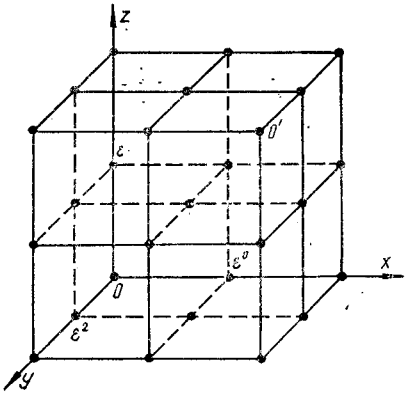


Рис. 22. Целочисленная решетка трехмерного пространства, представляющая возможные значения коэффициента X (2) при $N = k = 3$.

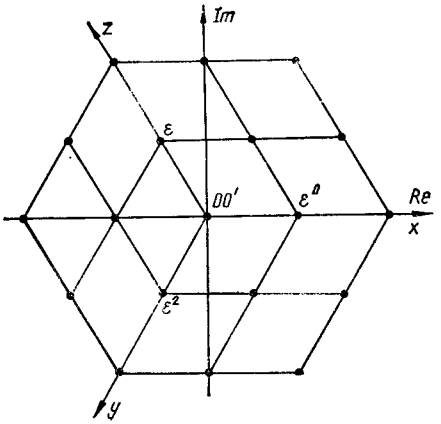


Рис. 23. Проекция целочисленной решетки, показанной на рис. 22, на комплексную плоскость.

при $p = 3$ на комплексной плоскости будут видны точки, лежащие в плоскостях xOy, xOz, yOz (см. рис. 23). Число всех точек целочисленной решетки равно k^3 или в случае p-мерного пространства — k^p. Число точек, лежащих в плоскостях xOy, xOz и yOz, равно $3^2 - 2^2$ или в случае p-мерного пространства — $k^p - (k-1)^p$, т. е. получен результат, доказанный в лемме 6.1. Отсюда следует важный вывод: если $N = p$ — простое число, то последовательность степеней первообразного элемента $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1}$ линейно независима.

Теперь примем, что $N = p^r$ и рассмотрим последовательность степеней первообразного элемента $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1}$ на комплексной плоскости. Эта последовательность является проекцией p^r-мерного пространства, равного прямой сумме p^r/p подпространств (рис. 24). В каждом подпространстве в качестве базисных векторов применяются степени $[\varepsilon^0, \varepsilon^{p^r/2-1}]$; $[\varepsilon, \varepsilon^{p^r/2}]$; ... ; $[\varepsilon^{(p^r/2)}, \varepsilon^{(p^r-1)}]$.

Очевидно, что выражение (6.29) справедливо только тогда, когда проекции целочисленных решеток p-мерных подпространств не совпадают ни в одной точке. Проверить выполнение этого условия можно, используя понятие группы поворотов правильного многоугольника. Концы векторов, образующих базис в p-мерном пространстве (p значений степеней первообразного элемента), являются вершинами правильного p-угольника. Будем рассматривать группу, которую образуют вращения этого p-угольника вокруг своего центра. В случае, когда $p = 3$ — это группа вращения треугольника, вершины которого образуют степени первообразного элемента ε^0, ε, ε^2, вокруг центра O этого треугольника. Элементом группы вращений правильного p-угольника является поворот его на угол $m2\pi/p$ [8], где m — целое число. Проекция каждого последующего подпространства повернута относительно проекции предыдущего на угол $2\pi/p^r$ (см. рис. 24). Проекции векторов $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p^r-1}$ и ε^0,

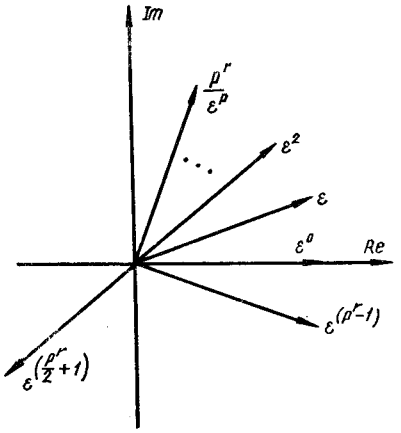


Рис. 24. Последовательность степеней первообразного элемента при $N = p^r$ на комплексной плоскости.

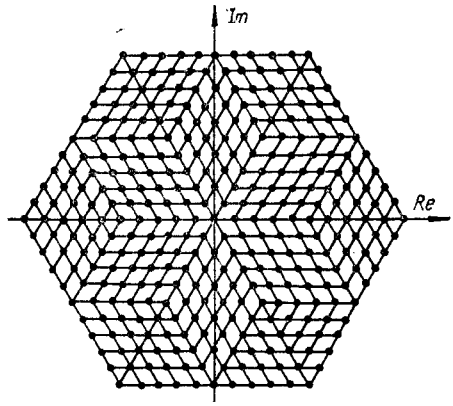


Рис. 25. Проекция целочисленной решетки шестимерного векторного пространства, представляющей различные значения коэффициента X (5), на комплексную плоскость.

ε^3, ..., ε^{p^r-2} на комплексную плоскость не совпадают, так как угол между векторами ε^0 и $\varepsilon^{p^r/p}$, равный $2\pi/p$, не равен ни одному из углов между векторами ε^0 и ε, ε^0 и ε^2, ..., ε^0 и $\varepsilon^{(p^r/p-1)}$, значение которых определяется выражением $p \cdot 2\pi \cdot (p-1)/p^r$. Очевидно, что выполняется неравенство $p \cdot 2\pi\,(p-1)/p^r < 2\pi/p$. Это и доказывает справедливость выражения (6.29). Теперь, рассматривая N-мерное пространство при $N = p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}$ как прямую сумму m подпространств размерности $p_i^{r_i}$, получаем неравенство (6.24). Знак равенства в этом неравенстве поставить нельзя. В общем случае проекции целочисленных решеток указанных подпространств на комплексную плоскость могут иметь общие точки, значит, подсчеты по (6.24) будут давать завышенные результаты. Теорема доказана.

Теперь рассмотрим некоторые частные случаи теоремы 6.1, т. е. при различных значениях N. Один такой случай приведен при доказательстве леммы 6.1, а именно определено число различных значений спектрального коэффициента $X(\alpha_i)$ при N простом. Другой частный случай получен при доказательстве теоремы 6.1 — дана точная оценка $P\{X(\alpha_i)\}$ при $N = p^r$. Кроме того, важным для практики является случай, когда N — произвольное четное число. При четном N очевидны зависимости между степенями первообразного элемента: $\varepsilon^0 = -\varepsilon^{(N/2-1)}$, $\varepsilon = -\varepsilon^{N/2}$, ..., $\varepsilon^{(N/2-2)} = -\varepsilon^{N-1}$. Следовательно, значения коэффициента $X(\alpha_i)$ можно интерпретировать как векторы в $N/2$-мерном векторном пространстве и воспользоваться для подсчета $P\{X(\alpha_i)\}$ выражением (6.24), если $N/2$ — простое число или степень простого числа. Если $N/2 = p_1^{r_1} p_2^{r_2} \ldots p_k^{r_k}$, то результаты, получаемые по (6.24), будут завышенными. Иногда правильный результат можно получить, разбивая $N/2$-мерное векторное простран-

ство на подпространства и применяя к каждому подпространству (6.24).

Пример 6.3. Пусть $N = 6$ и сигнал $x(n)$ разлагается в базисе дискретных экспоненциальных функций. Оценим величину порядка поля Галуа GF (p), над которым можно определить аналогичный базис. Причем существует однозначный переход $S(\alpha) \to X(\alpha)$.

Расчеты по (6.24) дают завышенные результаты, так как степени первообразного элемента связаны зависимостями $\varepsilon^0 = -\varepsilon^3$, $\varepsilon = -\varepsilon^4$, $\varepsilon^2 = -\varepsilon^5$ (значение $P\{X(\alpha_i)\}$, вычисленное по (6.24), равно 1001). Учитывая зависимости между степенями первообразного элемента, значения $X(\alpha_i)$ можно представить как векторы в $N/2$-мерном векторном пространстве ($N/2 = 3$). Но в этом случае почти в два раза увеличится значность сигнала $x(n)$, рассматриваемого на $N/2$ точках: $k' = 2k - 1 = 2N - 1 = 2 \cdot 6 - 1 = 11$. Единица вычитается для того, чтобы два раза не учитывать точку начала координат. Теперь можно провести вычисления по выражению (6.25), так как $N/2 = 3$ — простое число:

$$W_2 = (k')^3 - (k' - 1)^3 = 11^3 - 10^3 = 331.$$

В правильности результата можно убедиться непосредственной проверкой (рис. 25). Непосредственным подсчетом получаем, что $P \times \times \{X(\alpha_i)\} = 331$. Значит, порядок поля GF (p) должен быть не меньше 331.

Упражнение 6.3. Оценить величины $P\{X(\alpha_i)\}$ при $N = k = 4$ и базисе дискретных экспоненциальных функций (базис Фурье). Результаты проверить непосредственным построением проекции целочисленной решетки на комплексную плоскость и подсчетом точек.

Выше получены оценки для $P\{X(\alpha_i)\}$, когда $\chi_\alpha(n)$ является базисом дискретных экспоненциальных функций. Это означает, что в матрице $\chi_\alpha(n)$ есть строки, все элементы которых различны, т. е. строки, в которых степени первообразного элемента различны. Однако гармонический анализ сигнала $x(n)$ возможен и в других базисах такой же размерности (базисы функций Виленкина — Крестенсона). При этом $\chi_\alpha(n) = \chi_{\alpha_1}(n_1) \times \chi_{\alpha_2}(n_2) \times \ldots \times \chi_{\alpha_m}(n_m)$ и число различных элементов строки матрицы $\chi_\alpha(n)$ меньше или равно N. Рассмотрим случай, когда $\chi_\alpha(n) = [\chi_{\alpha_1}(n_1)]^{[r]}$, где $[r]$ обозначает r-ю кронекеровскую степень матрицы [14] $\chi_{\alpha_1}(n_1)$. Справедлива следующая теорема.

Теорема 6.2. Пусть $N = p^r$, где p — простое число и $\chi_\alpha(n) = [\chi_{\alpha_1}(n_1)]^{[r]}$. Тогда

$$W_3 = P\{X(\alpha_i)\} = [(k-1)\,p^{r-1}]^p - [(k-1)\,p^{r-1} - 1]^p. \qquad (6.30)$$

Доказательство. В этом случае в строке матрицы $\chi_\alpha(n)$ будет максимум p различных элементов, повторяющихся $p^r/p = p^{(r-1)}$ раз. Поэтому такая строка является базисом p-мерного векторного пространства. Для такого пространства $k' = (k-1)\,p^{r-1}$, так как каждый элемент строки повторяется $p^{(r-1)}$ раз и при ε^i появляются коэффициенты, максимальное значение которых равно $p^{(r-1)}$ (при

приведении подобных членов). Теперь, подставляя в (6.29) значения k' вместо k и p вместо N, получаем выражение (6.30). Теорема доказана.

Система базисных функций для разложения цифрового сигнала $x(n)$ может быть построена при рассмотрении различной структуры группы G_N в области определения этого сигнала. Число различных базисов при заданном значении N равно числу способов разложения N на сомножители. Оценить $P\{X(\alpha_i)\}$ для каждого способа не представляется возможным. Однако верхнюю оценку можно получить, пользуясь выражением (6.24). Для наиболее важных с практической точки зрения случаев можно найти точное значение $P\{X(\alpha_i)\}$ по выражениям (6.25) и (6.29). Кроме того, при некоторых значениях N вычисления можно свести к вычислениям по (6.25) и (6.29) (см. пример 6.3).

Заметим, что полученные оценки мощности множества различных значений коэффициента $X(\alpha_i)$ справедливы при абсолютно точном вычислении значений этого коэффициента, т. е. при представлении значения $X(\alpha_i)$ в радикалах. Естественно, что на практике в радикалах спектральные коэффициенты не представляются и точность их вычисления ограничена. Следовательно, спектральные коэффициенты, отличающиеся на величину, меньшую абсолютной погрешности их вычисления, будут восприниматься как один и тот же коэффициент. Таким образом, $P\{X(\alpha_i)\}$ будет меньше величины, полученной по выражениям (6.25) и (6.29). Однако это уменьшение величины $P\{X(\alpha_i)\}$ не позволяет уменьшить порядок поля GF (p), так как даже для очень близких по значению коэффициентов $X_1(\alpha_i)$ и $X_2(\alpha_i)$ соответствующие им коэффициенты $S_1(\alpha_i)$ и $S_2(\alpha_i)$ могут значительно отличаться (в смысле метрики, определяемой скалярным произведением в поле комплексных чисел). Происходит это потому, что введение в поле GF (p) метрики, аналогичной метрике поля комплексных чисел, невозможно. Поэтому для существования взаимно однозначного отображения (6.6) необходимо выполнение неравенства (6.24).

4. Преобразование спектра из поля Галуа в поле комплексных чисел

Установим аналитические выражения для преобразования значений спектральных коэффициентов из поля Галуа в поле комплексных чисел для исходных данных, принятых в параграфе 2 данной главы и при условии выполнения неравенства (6.24).

Заметим, что матрица, обратная матрице оператора A (см. выражение (6.7)), не существует. Определить спектральный коэффициент $X(\alpha_i)$ только на основе выражения (6.7) невозможно. Необходима дополнительная информация.

Обозначим для удобства действительную часть коэффициента $X(\alpha_i)$, $\mathrm{Re}\,X(\alpha_i)$ через x_1 и соответственно мнимую $\mathrm{Im}\,X(\alpha_i)$ — через x_2. Теперь запишем отображение $[X(\alpha_i)]^2 \to [S(\alpha_i)]^2$ или, учи-

тывая, что $X(\alpha_i) = x_1 + jx_2$, получаем

$$(x_1^2 - x_2^2) + j2x_1x_2 \to [S(\alpha_i)]^2.$$

С учетом выражения (6.7) можно записать систему уравнений, из которой находим действительную и мнимую части коэффициента $X(\alpha_i)$:

$$\begin{aligned}]a_1x_1 + a_2x_2[&= S(\alpha_i); \\ ](x_1^2 - x_2^2)\,a_1 + 2x_1x_2a_2[&= [S(\alpha_i)]^2. \end{aligned} \tag{6.31}$$

Из (6.31) видно, что преобразование значений спектральных коэффициентов из поля Галуа в поле комплексных чисел требует значительно бóльших вычислительных затрат, чем преобразование значений из поля комплексных чисел в поле Галуа. Кроме того, действительная и мнимая части x_1 и x_2 находятся из квадратного уравнения. Это значит, что к значениям коэффициента $X(\alpha_i)$ прибавляются значения квадратов $[X(\alpha_i)]^2$, т. е. число различных значений в поле комплексных чисел увеличивается. Поэтому для выполнения равенства во втором уравнении системы (6.31) необходимо большее значение порядка поля Галуа, в котором определены коэффициенты $S(\alpha_i)$, чем полученные по оценкам параграфа 3 данной главы. Такой способ преобразования значений спектральных коэффициентов вряд ли найдет практическое применение в связи с развитием элементной базы ЦВМ. Например, преобразование $S(\alpha_i) \to X(\alpha_i)$ можно осуществить табличным способом и эффективно реализовать с помощью ППЗУ [157].

Заметим, что в частном случае, когда $S(\alpha_i)$ — спектр цифрового сигнала в базисе функций Уолша, определенных над полем GF (p) (структура группы G_N в области определения сигнала $x(n)$ соответствует разложению N на сомножители в виде $N = 2 \cdot 2 \ldots 2 = 2^m$), система уравнений (6.31) существенно упрощается. Фактически $X(\alpha_i)$ принадлежит полю рациональных чисел. Поскольку оператор $A = [1, 0]$, система (6.31) сводится к уравнению

$$]a_1x_1[= S(\alpha_i), \tag{6.32}$$

из которого можно найти коэффициент $X(\alpha_i) = x_1$. Рассмотрим этот случай более подробно.

Известно [2, 4], что в поле Галуа GF (p) целые числа могут быть представлены однозначно, если их абсолютная величина не превосходит $p/2$. Положительные числа и нуль кодируются элементами поля Галуа 0, 1, 2, ..., $(p-1)/2$; $0 \to 0$; $1 \to 1$; $2 \to 2$; ...; $(p-1)/2 \to (p-1)/2$, отрицательные — элементами $p-1$, $p-2$, ..., $(p+1)/2$; $-1 \to p-1$; $-2 \to p-2$; $-3 \to p-3$; ...; $-(p-1)/2 \to (p+1)/2$. Тогда переход $S(\alpha_i) \to X(\alpha_i)$ может быть осуществлен по формуле [27]

$$X(\alpha_i) = \begin{cases} S(\alpha_i), & \text{если } S(\alpha_i) \leqslant (p-1)/2; \\ S(\alpha_i) - p, & \text{если } S(\alpha_i) > (p-1)/2. \end{cases} \tag{6.33}$$

Пример 6.4. Пусть задан цифровой сигнал $x^t(n) = [2; 3; 1; 3]$. Спектр его в базисе функций Уолша равен $X^t(\alpha) = [9; -3; 1; 1]$

Таблица 31. **Система базисных функций Уолша при $N = 4$ и структуре группы G, равной 2·2**

α_1	α_2	$n_1 = 0$		$n_1 = 1$	
		n_2			
		0	1	0	1
0	0	1	1	1	1
	1	1	−1	1	−1
1	0	1	1	−1	−1
	1	1	−1	−1	1

Таблица 32. **Система базисных функций Уолша при $N = 4$ и структуре группы G, равной 2·2, над полем GP (5)**

α_1	α^2	$n_1 = 0$		$n_1 = 1$	
		n_2			
		0	1	0	1
0	0	1	1	1	1
	1	1	4	1	4
1	0	1	1	4	4
	1	1	4	4	1

Таблица 33. **Система базисных функций Уолша при $N = 4$ и структуре группы G, равной 2·2, над кольцом Z_{25}**

α_1	α_2	$n_1 = 0$		$n_1 = 1$	
		n_2			
		0	1	0	1
0	0	1	1	1	1
	1	1	24	1	24
1	0	1	1	24	24
	1	1	24	24	1

(табл. 31). Спектр этого же сигнала в базисе функций Уолша, определенных над полем GF (5), равен $S^t(\alpha) = [4; 2; 1; 1]$ (табл. 32). Проведем переход $S(\alpha) \to X(\alpha)$ и проверим выполнение неравенства (6.23). По выражению (6.30) имеем

$$P\{X(\alpha_i)\} = [(4-1)\cdot 2^{(2-1)}]^2 - [(4-1)\cdot 2^{(2-1)} - 1]^2 = 36 - 25 = 11.$$

Следовательно, условие (6.23) не выполняется. Таким образом, однозначный переход $S(\alpha) \to X(\alpha)$ невозможен. Для удовлетворения (6.23) выберем кольцо Z_{25}, порядок которого равен 25 и $25 > 11$. В этом кольце существует первообразный элемент порядка 2, например, $\varepsilon = 24$ (табл. 33). Спектр сигнала $x(n)$ в базисе функций Уолша, определенных над кольцом Z_{25}, $S^t(\alpha) = [9; 22; 1; 1]$. Вычислим коэффициенты $X(0)$, $X(1)$, ..., $X(3)$. По (6.33) имеем

$$X(0) = 9; \quad X(1) = 22 - 25 = -3; \quad X(2) = 1; \quad X(3) = 1.$$

В случае определения базиса над кольцом Z_M в выражение (6.33) вместо значения p подставляется значение порядка кольца Z_M, т. е. значение M, что и сделано в этом примере.

Исходя из оценок W_1, W_2, W_3, полученных в параграфе 3 данной главы, можно сделать вывод, что уже при $N \geqslant 8$ и $k \geqslant 8$ величина порядка поля GF (p), необходимая для существования взаимно однозначного отображения $X(\alpha_i) \to S(\alpha_i)$, становится очень большой, что затрудняет табличный переход $S(\alpha_i) \to (X(\alpha_i)$. Только при определении спектра $S(\alpha)$ в базисе функций Уолша над полем GF (p) или кольцом Z_M переход $S(\alpha) \to X(\alpha)$ может быть просто осуществлен по выражению (6.33), причем требования к величине порядка поля GF (p) или кольца Z_M менее жесткие и легко могут соблюдать-

ся при практической реализации. Поэтому целесообразно рассмотреть способы, упрощающие табличный переход $S(\alpha) \to X(\alpha)$.

Один из таких способов основан на разбиении последовательности степеней первообразного элемента $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1}$ на подпоследовательности, для которых переход $S(\alpha_i) \to X(\alpha_i)$ легко осуществить табличным способом. Последовательность степеней $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{N-1}$ разбивается на l подсистем. Спектральные коэффициенты $S(\alpha)$ должны представляться в виде

$$S(\alpha_i) = \sum_{r=1}^{l} S_r(\alpha_i)\, T_r'(\alpha_i), \tag{6.34}$$

где $S_r(\alpha)$ — спектральные коэффициенты, вычисленные в базисе r-й подпоследовательности; $T_p'(\alpha_i)$ — поворачивающие множители, приводящие спектральные коэффициенты, вычисленные в базисах подпоследовательностей, к единой системе координат и определенные над полем GF (p). Переход $S_r(\alpha_i) \to X_r(\alpha_i)$ осуществляется табличным способом. В этом случае имеем менее жесткие требования к требуемому порядку поля GF (p), так как в выражения (6.24), (6.25), (6.29) и (6.30) вместо N подставляем значение $N' = N/l$. Спектральные коэффициенты $X(\alpha_i)$ находятся по выражению

$$X(\alpha_i) = \sum_{r=1}^{l} X_r(\alpha_i)\, T_r(\alpha_i), \tag{6.35}$$

где $T_r(\alpha_i)$ — поворачивающие множители, определенные над полем комплексных чисел.

Умножение на поворачивающие множители можно учесть при составлении таблиц переходов $S_i(\alpha_i) \to X(\alpha_i)$. Тогда выражение (6.35) упрощается:

$$X(\alpha_i) = \sum_{r=1}^{l} X_r'(\alpha_i), \tag{6.36}$$

где $X_r'(\alpha_i) = X_r(\alpha_i)\, T_r(\alpha_i)$.

Пример 6.5. Пусть задан цифровой сигнал $x(n)$ при $N = 6$, значение которого (а также значения спектров $X(\alpha)$ и $S(\alpha)$) совпадают с приведенными значениями в примере 6.1. Пусть спектр $S(\alpha)$ известен, а спектр $X(\alpha)$ этого сигнала необходимо найти. Покажем, как проводятся вычисления по выражениям (6.34) — (6.36). Разобьем последовательность $\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^5$ на $l = 3$ подпоследовательности; осуществим переход $S_r(\alpha_i) \to X_r(\alpha_i)$ и вычислим $X(\alpha_i)$. Чтобы не загромождать изложение, расчеты проведем для одного из спектральных коэффициентов, например для коэффициента $X(5)$. Остальные коэффициенты вычисляются аналогично. Пятая строка матрицы $\chi_\alpha^{-1}(n)$ ($\alpha = 5$) равна $[\varepsilon^0, \varepsilon, \varepsilon^2, \ldots, \varepsilon^5] = [1,\ 1/2 + i\sqrt{3}/2,\ -1/2 + i \times \times \sqrt{3}/2,\ -1,\ -1/2 - i\sqrt{3}/2,\ 1/2 + i\sqrt{3}/2]$. Эта же строка над полем GF [7] равна [1; 3; 2; 6; 4; 5]. Разбиение последовательности степеней первообразного элемента на подпоследовательности осуществим следующим образом: $\varepsilon_1 = (\varepsilon^0, \varepsilon^3)$; $\varepsilon_2 = (\varepsilon, \varepsilon^4)$; $\varepsilon_3 = (\varepsilon^2, \varepsilon^5)$.

Необходимая величина порядка поля GF (p) для возможности однозначного перехода $S_r(\alpha_i) \to X_r(\alpha_i)$ определяется из неравенства $p \geqslant W_3$ (см. (6.30)). При вычислении значения W_3 по выражению (6.30) следует учесть, что $N' = N/l$. Подставляя численные значения, получаем $6/3 = 2$, т. е. вместо $N = 2 \cdot 3$ имеем $N' = 2$. Проведя несложные подсчеты, получаем $W_3 = 11$, значит, должно выполняться неравенство $p \geqslant 11$. Однако для данного конкретного сигнала $x(n)$ можно обойтись величиной $p = 7$. Подпоследовательности $\varepsilon_1 = (\varepsilon^0, \varepsilon^3) = (1, -1)$ в поле комплексных чисел соответствует подпоследовательность $\varepsilon_1' = [(\varepsilon')^0, (\varepsilon')^3] = (1, 6)$ в поле GF (7). Подпоследовательность ε^2 повернута относительно подпоследовательности ε_1 на угол $\pi/3$, подсистема ε_3 — на угол $2\pi/3$. В поле комплексных чисел значения $T_r(\alpha_i)$ следующие: $T_1(5) = 1$; $T_2(5) = e^{i\frac{\pi}{3}}$; $T_3(5) = e^{i\frac{2\pi}{3}}$; значение поворачивающих множителей в поле GF (7): $T_1'(5) = 1$; $T_2'(5) = 3$; $T_3'(5) = 2$. Теперь вычислим значения $S_p'(\alpha)$:

$$S_1(5) = [1, 6]\begin{bmatrix}3\\5\end{bmatrix} = 3 + 5 \cdot 6 = 5 \pmod 7;$$

$$S_2(5) = [1, 6]\begin{bmatrix}4\\4\end{bmatrix} = 4 + 6 \cdot 4 = 0 \pmod 7;$$

$$S_3(5) = [1, 6]\begin{bmatrix}5\\2\end{bmatrix} = 5 + 2 \cdot 6 = 3 \pmod 7.$$

По выражению (6.33) (при таком разбиении последовательности степеней первообразного элемента на подпоследовательности возможен переход не табличным способом, а с помощью выражения (6.33), что и используется) получаем соответствующие значения $X_r(5)$: $X_1(5) = -2$; $X_2(5) = 0$; $X_3(5) = 3$. Теперь произведем умножения на поворачивающие множители:

$$X_1'(5) = X_1(5) \cdot 1 = X_1(5) = -2;$$

$$X_2'(5) = X_2(5)\, e^{i\pi/3} = 0;$$

$$X_3'(5) = X_3(5)\, e^{i2\pi/3} = 3e^{i2\pi/3} = -\frac{3}{2} + i\frac{3\sqrt{3}}{2}.$$

Тогда

$$X(5) = -2 + \left(-\frac{3}{2} + i\frac{3\sqrt{3}}{2}\right) = -\frac{7}{2} + i\frac{3\sqrt{3}}{2} = -3{,}5 + i2{,}6.$$

Выше описаны методы «поточечного» преобразования значений спектральных коэффициентов из поля Галуа в поле комплексных чисел. Недостатком таких методов являются ограничения, накладываемые на порядок поля Галуа. Для возможности осуществления однозначного перехода $S(\alpha_i) \to X(\alpha_i)$ порядок поля GF (p) приходится выбирать большим даже при умеренных значениях N и k.

Поэтому реализация перехода $S(\alpha_i) \to X(\alpha_i)$ связана с реализацией арифметического устройства с большой разрядной сеткой, что приводит к низкому быстродействию и значительным аппаратурным затратам. Возможен и другой подход, основанный на использовании при вычислении спектрального коэффициента $X(\alpha_i)$ всего спектра $S(\alpha)$. В этом случае никаких ограничений на порядок поля GF (p) не накладывается:

$$X(\alpha_i) = \varphi[S(0), \quad S(1), \ldots, S(N-1)]. \tag{6.37}$$

Представим каждый коэффициент $S(\alpha_i)$ в виде суммы

$$S(\alpha_i) = \sum_{r=1}^{m} S_r(\alpha_i). \tag{6.38}$$

Учитывая тот факт, что χ-преобразование является линейным преобразованием, и используя выражение (6.38), записываем (6.37) в виде

$$X(\alpha_i) = \varphi\left[\sum_{r=1}^{m} S_r(0) + \sum_{r=1}^{m} S_r(1) + \cdots + \sum_{r=1}^{m} S_r(N-1)\right] =$$
$$= \varphi[S_1(0) + S_1(1) + \cdots + S_1(N-1) + \varphi][S_2(0) + S_2(1) + \cdots$$
$$\cdots + S_m(N-1)]. \tag{6.39}$$

Каждая зависимость $\varphi[S_r(0) + S_r(1) + \ldots + S_r(N-1)]$, $r = 1, 2, \ldots, m$, реализуется табличным способом с помощью ППЗУ. Выбором m можно добиться приемлемого числа разрядов сумм, заключенных в квадратные скобки, в выражении (6.39).

Упражнение 6.4. Для сигнала, заданного в примере 6.5, составить таблицы соответствий

$$X_r(\alpha_i) = \varphi[S_r(0) + S_r(1) + \cdots + S_r(N-1)],$$

где $r = 1, 2, \ldots, m$.

5. Оценки вычислительных затрат и анализ погрешностей

Попытаемся найти и проанализировать вычислительные затраты, получающиеся при преобразовании спектров, для каждого из рассматриваемых случаев, перечисленных в параграфе 1 настоящей главы.

Если $G_{m_1} \neq G_{m_2}$, $K_1 = K_2 = K$, преобразование спектра проводится по выражению (6.5). Вычисления по этому выражению требуют выполнения m^2 умножений и $m(m-1)$ сложений в кольце K. Однако это справедливо только в общем случае. Матрица ${}_{21}\chi_\alpha(n)$ может быть разреженной и число арифметических операций существенно меньше. Сказанное имеет место, например, при преобразовании спектра из базиса Уолша в базис Фурье (над полем комплексных чисел) [160].

Вычисления по выражению (6.12) (случай, когда $G_{m_1} = G_{m_2} = G_m$ и $K_1 \neq K_2$) требуют реализации m операций умножения в

кольце K_1, m операций, эквивалентных операции сложения в кольце K_2 и m операций, связанных с согласованием арифметик колец K_1 и K_2. Преобразование спектра из кольца K_2 в кольцо K_1 может потребовать дополнительных вычислительных затрат или, наоборот, число операций может быть меньшим m. Это видно из рассмотренного случая преобразования спектра из поля комплексных чисел в поле Галуа и обратно — из поля Галуа в поле комплексных чисел. В общем число арифметических операций зависит от вида колец K_1 и K_2 и оценки могут быть получены для каждого конкретного случая. Так, для преобразования значения спектральных коэффициентов из поля комплексных чисел в поле Галуа необходимо произвести m комплексных умножений и m сложений действительных чисел. Кроме того, нужно осуществить m операций сравнения по модулю p. Преобразование значений спектральных коэффициентов из поля Галуа в поле комплексных чисел требует значительно большего числа арифметических операций (см. (6.31)). Однако, как это было показано в предыдущем параграфе, на практике преобразование может быть эффективно реализовано табличным способом с помощью ППЗУ. Еще более непредсказуемым представляется случай, когда $G_{m_1} \neq G_{m_2}$ и $K_1 \neq K_2$.

Теперь проанализируем погрешности, вносимые при преобразовании значений спектральных коэффициентов из поля комплексных чисел в поле Галуа и обратно — из поля Галуа в поле комплексных чисел. Анализ будем проводить, пользуясь методикой, изложенной в работах [59, 117, 153, 156]. Погрешности отдельных источников оцениваются среднеквадратическими значениями. Полагаем, что среднеквадратические значения погрешностей отдельных источников независимы. Тогда полная погрешность результата вычислений определяется выражением [153, 156]:

$$\sigma = \sqrt{\sigma_{\text{м}}^2 + \sigma_{\text{тр}}^2 + \sigma_{\text{и}}^2 + \sigma_{\text{д}}^2}, \qquad (6.40)$$

где $\sigma_{\text{м}}$, $\sigma_{\text{тр}}$, $\sigma_{\text{и}}$, $\sigma_{\text{д}}$ — соответственно методическая, трансформированная, инструментальная (арифметическая) и динамическая погрешности.

Методическая погрешность обусловливается приближенным характером алгоритма, с помощью которого описывается реальный физический процесс, и переходом к его численному представлению в вычислительном устройстве.

Трансформированная погрешность обусловливается погрешностями представления исходных данных, возникающих вследствие несовершенства способа их получения, дискретизации непрерывных величин, невозможности представления некоторых чисел конечным числом значащих цифр и т. п.

Арифметическая погрешность возникает из-за необходимости выполнения арифметических операций в вычислительном устройстве с ограниченной длиной разрядной сетки.

Перечисленные погрешности имеют статистический характер.

Динамическая погрешность обусловлена конечной скоростью вычислений. Конечная скорость вычислений приводит к запаздыванию

при решении задачи, что имеет место при обработке данных в реальном масштабе времени.

Определим значение полной погрешности при переходе $X(\alpha_i) \to S(\alpha_i)$. Так как вычисление $S(\alpha_i)$ осуществляется непосредственно по алгоритму перехода $X(\alpha_i) \to S(\alpha_i)$, который является точным, то $\sigma_м = 0$. Кроме того, полагаем, что арифметическое устройство спроектировано так, что $\sigma_д = 0$. Таким образом, необходимо оценить трансформированную и арифметическую погрешности, составляющие шум округлений.

Пусть $S(\alpha_i)$ вычисляется согласно (6.7). Тогда требуется найти полную погрешность произведения $AX(\alpha_i)$. Пусть спектральный коэффициент $X(\alpha_i)$ задан в виде

$$X(\alpha_i) = X'(\alpha_i) + \Delta X(\alpha_i), \tag{6.41}$$

где $X'(\alpha_i)$ — точное значение коэффициента $X(\alpha_i)$; $\Delta X(\alpha_i)$ — полная абсолютная погрешность вычисления коэффициента $X(\alpha_i)$.

Точно так же можно представить элементы матрицы оператора A:

$$a_1 = a_1' + \Delta a_1; \quad a_2 = a_2' + \Delta a_2, \tag{6.42}$$

где a_1' и a_2' — точные значения элементов a_1 и a_2; Δa_1, Δa_2 — абсолютные погрешности, обусловленные неточностью представления элементов a_1 и a_2 конечным числом значащих цифр.

Следовательно, необходимо найти полную погрешность вычисления функции

$$AX(\alpha_i) = a_1 \operatorname{Re} X(\alpha_i) + a_2 \operatorname{Im} X(\alpha_i). \tag{6.43}$$

Известно [156], что трансформированная погрешность операции умножения числа x на число y определяется по выражению

$$\Delta_{тр} = (\Delta x)\, y + (\Delta y)\, x, \tag{6.44}$$

где Δx, Δy — погрешности операндов, вызванные ограниченной разрядностью и конечной точностью выполнения предыдущих операций, результатом которых они являются. Учитывая (6.41) — (6.44), получаем

$$\Delta_{тр} = \Delta a_1 \operatorname{Re} X(\alpha_i) + a_1 \operatorname{Re}[\Delta X(\alpha_i)] + \Delta a_2 \operatorname{Im} X(\alpha_i) + \\ + a_2 \operatorname{Im}[\Delta X(\alpha_i)]. \tag{6.45}$$

Полная абсолютная погрешность вычисления произведения $AX(\alpha_i)$ составит

$$\Delta_A = \Delta_{тр} + \Delta_{и_1} + \Delta_{и_2}, \tag{6.46}$$

где $\Delta_{и_1}$ и $\Delta_{и_2}$ — инструментальные (арифметические) погрешности вычисления произведений $a_1 \operatorname{Re} X(\alpha_i)$ и $a_2 \operatorname{Im} X(\alpha_i)$ (см. (6.45)) соответственно. Погрешности $\Delta_{и_1}$ и $\Delta_{и_2}$ зависят от способа выполнения умножения, правил округления результата и т. п. Кроме того, на значение абсолютной погрешности Δ_A влияет операция округления в выражении (6.7). Если дробная часть (ДЧΔ_A) погрешности Δ_A больше половины погрешности квантования ДЧ$\Delta_A > \Delta/2$, то в результате округления при вычислении по выражению (6.7) от

погрешности Δ_A отнимается ДЧΔ_A или прибавляется величина $1 - $ ДЧΔ_A. Если ДЧ$\Delta_A < \Delta/2$, то значение ДЧΔ_A отбрасывается от значения Δ_A, если ДЧ$\Delta_A > \Delta/2$, то к значению Δ_A прибавляется $1 - $ ДЧΔ_A. В зависимости от знака произведения $AX(\alpha_i)$ и знака Δ_A это может ухудшить или улучшить результат не больше $\Delta/2$. В худшем случае

$$\Delta_A = \Delta_{тр} + \Delta_{и_1} + \Delta_{и_2} + \Delta/2. \qquad (6.47)$$

Исходя из (6.45) и (6.40), записываем выражение для полной среднеквадратической погрешности:

$$[\Delta_A] = \sqrt{(\sigma[\Delta a_1]\,\mathrm{Re}\,X(\alpha_i))^2 + (\sigma[\mathrm{Re}(\Delta X(\alpha_i)]\,a_1)^2 + \cdots}$$
$$\cdots + (\sigma[\Delta a_2]\,\mathrm{Im}\,X(\alpha_i))^2 + (\sigma[\mathrm{Im}(\Delta X(\alpha_i))])^2 + (\sigma[\Delta_{и_1}])^2 + \cdots$$
$$\cdots + (\sigma[\Delta_{и_2}])^2 + (\sigma[\Delta/2])^2}. \qquad (6.48)$$

Анализируя (6.48), можно прийти к выводу, что среднеквадратическая погрешность $\sigma[\Delta_A]$ отличается от среднеквадратической погрешности $\sigma[\Delta_B]$, которая получается в результате умножения вектор-строки на вектор-столбец (анализ погрешностей, возникающих при проведении матричных вычислений можно найти, например, в [119]), на величину, обусловливаемую наличием погрешности квантования $\Delta/2$. В случае больших N ($N > 128$) величиной $\Delta/2$ можно пренебречь и погрешности $\sigma[\Delta_A]$ и $\sigma[\Delta_B]$ совпадают. Значит, при преобразовании значений спектральных коэффициентов из поля комплексных чисел в поле Галуа по выражению (6.7) вносится погрешность, приблизительно эквивалентная погрешности, возникающей при вычислении произведения двухэлементных вектор-строки и вектор-столбца. В результате получается значение коэффициента $S''(\alpha_i)$, соответствующее не точному значению $X'(\alpha_i)$, а приближенному $X(\alpha_i)$, воспринимаемому как некоторое абсолютно точное значение $X''(\alpha_i)$. Коэффициенты $X'(\alpha_i)$ и $X''(\alpha_i)$ отличаются на величину полной погрешности. Пусть коэффициенту $X'(\alpha_i)$ соответствует коэффициент $S'(\alpha_i)$. Как упоминалось в параграфе 3 данной главы, значения $S'(\alpha_i)$ и $S''(\alpha_i)$, рассматриваемые как целые числа, могут значительно отличаться.

Теперь оценим по выражениям (6.17) — (6.22) погрешности, возникающие при преобразовании значений спектральных коэффициентов. Вычисление углов $\mathrm{arctg}\,\mathrm{Im}\,X(\alpha_i)/\mathrm{Re}\,X(\alpha_i)$ и $\mathrm{arctg}\,\mathrm{Im}\,\zeta/\mathrm{Re}\,\zeta$ должно производиться таким образом, чтобы точность определения угла была не хуже $\pm\beta/2$ (см. рис. 20). Заметим, что углы могут находиться табличным способом с необходимой точностью. По существу, в этом случае абсолютная погрешность определяется следующим соотношением:

$$\Delta X(\alpha_i) = e_\zeta(\alpha_i) + e_{\zeta'}(\alpha_i) + e_n(\alpha_i), \qquad (6.49)$$

где $e_\zeta(\alpha_i)$ — абсолютная погрешность вычисления по выражению (6.22); $e_{\zeta'}(\alpha_i)$ — абсолютная погрешность представления (6.18), которая является методической погрешностью; $e_n(\alpha_i)$ — абсолют-

ная погрешность вычисления по выражению

$$\varepsilon^r \{\,|\,X(\alpha_i)\,|\,\}. \qquad (6.50)$$

Анализируя (6.22), можно сделать вывод, что погрешность $e_\zeta(\alpha_i)$ можно представить в виде суммы

$$e_\zeta(\alpha_i) = e_\text{п}(\alpha_i) + \Delta X_1(\alpha_i),$$

где $\Delta X_1(\alpha_i)$ — абсолютная погрешность вычисления коэффициента $X(\alpha_i)$.

Тогда выражение (6.22) можно переписать в виде

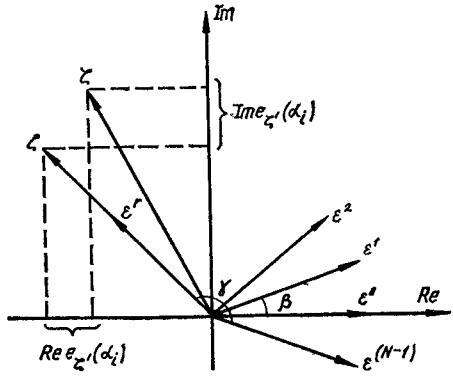


Рис. 26. Приближенное представление вектора ζ.

$$\Delta X(\alpha_i) = \Delta X_1(\alpha_i) + 2e_\text{п}(\alpha_i) + e_{\zeta'}(\alpha_i). \qquad (6.51)$$

В этом равенстве записана сумма отдельных погрешностей в предположении их независимости.

Формулу (6.50) можно записать следующим образом:

$$(\operatorname{Re}\varepsilon^r + i\operatorname{Im}\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\} = (\operatorname{Re}\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\} + (i\operatorname{Im}\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\} = \operatorname{Re}e_\text{п}(\alpha_i) + i\operatorname{Im}e_\text{п}(\alpha_i).$$

Учитывая (6.44), получаем

$$\operatorname{Re}e_\text{п}(\alpha_i) = (\operatorname{Re}\Delta\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\} + \Delta\{\,|\,X(\alpha_i)\,|\,\}(\operatorname{Re}\varepsilon^r) + \Delta_\text{ум}, \qquad (6.52)$$

где $\Delta_\text{ум}$ — инструментальная погрешность, возникающая при вычислении произведения $(\operatorname{Re}\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\}$; $\operatorname{Re}\Delta\varepsilon^r$ — действительная часть абсолютной погрешности, появляющейся при вычислении ε^r.

Погрешность $\Delta\{\,|\,X(\alpha_i)\,|\,\}$ легко определить, используя известные приемы [153, 156] и учитывая, что

$$\{\,|\,X(\alpha_i)\,|\,\} = 1 + \sqrt{[\operatorname{Re}X(\alpha_i)]^2 + [\operatorname{Im}X(\alpha_i)]^2}\;;$$

$$\Delta\{\,|\,X(\alpha_i)\,|\,\} = |\,X(\alpha_i)\,|\,\frac{\sigma[\Delta_1]}{2},$$

где

$$\Delta_1 = 2\operatorname{Re}X(\alpha_i)[\Delta\operatorname{Re}X(\alpha_i)] + 2\operatorname{Im}X(\alpha_i)[\Delta\operatorname{Im}X(\alpha_i)] + \Delta/2.$$

Таким же образом получаем выражение для $\operatorname{Im}e_\text{п}(\alpha_i)$:

$$\operatorname{Im}e_\text{п}(\alpha_i) = (\operatorname{Im}\Delta\varepsilon^r)\{\,|\,X(\alpha_i)\,|\,\} + \Delta\{\,|\,X(\alpha_i)\,|\,\}(\operatorname{Im}\varepsilon^r) + \Delta_\text{ум}. \qquad (6.53)$$

Наконец, осталось выразить погрешность $e_{\zeta'}(\alpha_i)$. Допустим, что значение ζ вычислено с точностью $\zeta = \zeta_1 + \Delta\zeta$, где ζ_1 — точное значение вектора ζ; Δζ — абсолютная погрешность. К погрешности Δζ добавляется методическая погрешность, которая обусловлена неточностью представления в (6.18) и которая может быть записана в виде суммы

$$e_{\zeta'}(\alpha_i) = e^1_{\zeta'}(\alpha_i) + e^2_{\zeta'}(\alpha_i),$$

где $e^1_{\zeta'}(\alpha_i)$ — абсолютная погрешность, вызванная округлением при вычислении r_1 (см. (6.19)); $e^2_{\zeta'}(\alpha_i)$ — абсолютная погрешность, обусловленная округлением $|X(\alpha_i)|$ в выражении (6.15). Исходя из геометрических соображений (рис. 26), легко получить выражения для этих погрешностей:

$$e^1_{\zeta'}(\alpha_i) = |\zeta|[\cos(\gamma+\delta) - \cos\gamma] + i|\zeta|[\sin(\gamma+\delta) - \sin\gamma];$$

$$e^2_{\zeta'}(\alpha_i) = \{|\zeta| -]|\zeta|[\}\cos(\gamma+\delta) + i\{|\zeta| -]|\zeta|[\}\sin(\gamma+\delta),$$

где γ — угол между осью Re и вектором, представляющим ζ; δ — угол между ζ и ζ', который может принимать как положительные, так и отрицательные значения.

Учитывая, что значение $\{|\zeta| -]|\zeta|[\}$ не может превышать величины $\Delta/2$, а значения

$$\cos(\gamma+\delta) - \cos\gamma \leqslant 2\sin\frac{2\gamma+\beta/2}{2}\sin\delta/2 \leqslant 2\sin\beta/4;$$

$$\sin(\gamma+\delta) - \sin\gamma \leqslant 2\sin\beta/4\cos\frac{2\gamma+\beta/2}{2} \leqslant 2\sin\beta/4;$$

$$\delta_{\max} = \beta/2,$$

получаем предельные значения действительной и мнимой частей методической погрешности:

$$\mathrm{Re}\, e_{\zeta'}(\alpha_i) = |\zeta|\sin\beta/4 + \Delta/2\cos(\gamma+\beta/2);$$

$$\mathrm{Im}\, e_{\zeta'}(\alpha_i) = i(|\zeta|\sin\beta/4 + \Delta/2\sin(\gamma+\beta/2).$$

Уменьшая угол β, а также абсолютную величину векторов ε^r (см. рис. 26), можно уменьшить методическую погрешность до необходимой, наперед заданной величины.

Отметим, что при вычислениях по (6.22) может возникнуть погрешность, значительно превышающая погрешности отдельных операндов $X(\alpha_i)$ и $\varepsilon^r\{]|X(\alpha_i)|[\}$, так как в этом выражении фигурирует операция вычитания. Для устранения такого нежелательного эффекта необходимо организовать вычисления так, чтобы действительная и мнимая части коэффициента $X(\alpha_i)$ не были близкими по величине соответственно к действительной и мнимой части комплексного числа, определяемого выражением $\varepsilon^r\{]|X(\alpha_i)|[\}$. Здесь в качестве элементов, через которые определяются значения $X(\alpha_i)$ и ζ, выбрана последовательность степеней первообразного элемента (см. рис. 26) (опорная последовательность). Однако для уменьшения погрешности, появляющейся при вычитании, в выражении (6.22) целесообразно выбрать две опорные последовательности. Одну с относительно большим значением угла β, обеспечивающую необходимую точность вычислений по (6.22). Чем больше угол β, тем больше отличаются действительная и мнимая части $X(\alpha_i)$ от действительной и мнимой части произведения $\varepsilon^r\{]|X(\alpha_i)|[\}$. Другая опорная последовательность должна выбираться таким образом, чтобы угол β был возможно меньшим и была обеспечена требуемая точность представления значения вектора ζ.

Из приведенного анализа ошибок можно сделать вывод, что при преобразовании значений спектральных коэффициентов из поля комплексных чисел в поле Галуа существует ряд приемов, позволяющих добиться требуемой точности преобразований. Специфические операции, связанные с согласованием арифметики полей C и GF (p), не вносят существенного шума. Теперь остается оценить погрешности, возникающие при преобразовании спектральных коэффициентов из поля Галуа в поле комплексных чисел, т. е. погрешности, появляющиеся при переходе $S(\alpha) \to X(\alpha)$.

Табличный переход $S_r(\alpha_i) \to X_r(\alpha_i)$ можно осуществить с любой наперед заданной точностью. Если при этом учитывается умножение на поворачивающие множители, то можно считать, что погрешность при переходе $S_r(\alpha_i) \to X_r(\alpha_i)$ обусловлена предварительными вычислениями при составлении таблиц перехода и может быть теоретически как угодно малой. Относительная погрешность суммы в (6.35) не превосходит относительной погрешности вычисления слагаемых $X_r'(\alpha_i)$.

Анализ погрешностей, возникающих при вычислениях по выражению (6.31), не представляет никаких принципиальных трудностей. Здесь этот анализ не проводится из-за его громоздкости, однако практически очевидно, что требуемую точность преобразований легко получить.

* * *

Наиболее простой является задача преобразования спектра из одного базиса в другой, если спектр и базисы определены над одним и тем же кольцом. В случае различных колец задача значительно усложняется. Например, преобразование спектра из поля комплексных чисел в поле Галуа сводится к преобразованию значений спектральных коэффициентов. Существует «поточечная» зависимость между спектрами цифрового сигнала в базисе функций Виленкина — Крестенсона, определенном над полем комплексных чисел, и в базисе такой же структуры, но определенном над конечным полем Галуа или над конечным кольцом. Задача преобразования значений спектральных коэффициентов из поля Галуа в поле комплексных чисел решается более сложно. С практической точки зрения наиболее приемлемым является реализация такого преобразования табличным способом с помощью ППЗУ. Лишь в частном случае, когда спектры определены в базисе функций Уолша (над полем Галуа и над полем комплексных чисел), преобразование значений спектральных коэффициентов из поля Галуа в поле комплексных чисел может быть осуществлено эффективно по аналитическим выражениям. Для того чтобы упомянутая обратная задача имела однозначное решение, порядок поля Галуа следует выбирать не меньшим некоторой величины W. Значение W зависит от объема преобразований N, числа уровней квантования k цифрового сигнала $x(n)$ (значности сигнала) и структуры группы G_N, рассматриваемой в области определения сигнала $x(n)$. Особенностью преобразования спектральных коэффициентов, определенных над различными кольцами K_1 и K_2, является необходимость

согласования арифметик этих колец. Погрешности, возникающие вследствие проведения операции согласования арифметик поля комплексных чисел и поля Галуа, незначительные по сравнению с общей погрешностью, получающейся при преобразовании спектров. В общем погрешности могут быть сведены до любой наперед заданной величины.

Анализ вычислительных затрат показал, что в случае, когда $K_1 = C$, $K_2 = \mathrm{GF}(p)$ и базисы, определенные над полем C и полем $\mathrm{GF}(p)$, имеют одну и ту же структуру, преобразование спектра требует проведения меньшего числа арифметических операций по сравнению с преобразованием спектра из одного базиса в другой при $K_1 = K_2 = C$ (или при $K_1 = K_2 = \mathrm{GF}(p)$).

ГЛАВА 7

МОДЕЛИ СИСТЕМ ОБРАБОТКИ СИГНАЛОВ

1. Модели вычисления свертки цифровых сигналов

Пусть заданы два сигнала $x_1(n)$ и $x_2(n)$. Для ряда практических приложений важное значение имеет функция от этих двух сигналов, называемая сверткой:

$$x_1(n) * x_2(n) = \sum_{n=0}^{N-1} x_1(n)\, x_2(n-m), \quad m = 0, 1, \ldots, N-1. \quad (7.1)$$

Выражение (7.1) описывает, например, поведение линейной дискретной системы. Вычисление непосредственно по (7.1) требует проведения $N(N+1)$ операций умножения, что является ограничивающим фактором при реализации. Уменьшить число умножений можно вычислением свертки с помощью ДПФ по схеме

$$x_1(n) * x_2(n) = \text{ОДПФ}\{\text{ДПФ}[x_1(n)]\,\text{ДПФ}[x_2(n)]\}, \quad (7.2)$$

где ОДПФ — обратное ДПФ.

Для того чтобы получаемая свертка была линейной, размер матрицы ДПФ должен выбираться равным $N' = 2N - 1$, где N — интервал определения сигналов $x_1(n)$ и $x_2(n)$. ДПФ можно вычислять по быстрым алгоритмам, за счет чего число умножений при вычислениях по (7.2) может быть существенно меньшим, чем число умножений при вычислениях по (7.1). Точно так же свертку можно вычислить с помощью ПФГ:

$$x_1(x) * x_2(n) = \text{ОПФГ}\{\text{ПФГ}[x_1(n)] \odot \text{ПФГ}[x_2(n)]\}, \quad (7.3)$$

где знак $\odot$ обозначает умножение по модулю p соответствующих спектральных коэффициентов.

Операция умножения комплексных чисел заменяется операцией умножения целых чисел по модулю p. В целом объем вычислений по (7.3) сокращается по сравнению с вычислениями по (7.2). Если выбрать первообразный элемент ε равным 2 или степени 2, то необходимо произвести всего N умножений целых чисел по модулю p. Чтобы вычисления по (7.3) привели к такому же результату, что и вычисления по (7.2), на значения N и p необходимо наложить некоторые ограничения.

Для того чтобы вычисления по формуле

$$x_1(n) * x_2(n) = \sum_{n=0}^{N-1} x_1(n) \odot x_2(n-m), \ \mathrm{GF}(p), \qquad (7.4)$$

проводимые по законам поля GF (p), приводили к правильным арифметическим сверткам, которые производятся по законам кольца целых чисел, необходимо ограничить рабочие области значений сигналов $x_1(n)$ и $x_2(n)$. Это означает, что

$$\left\| \sum_{n=0}^{N-1} x_1(n)\, x_2(n-m) \right\| < \sum_{n=0}^{N-1} \| x_1(n) \| \cdot \| x_2(n-m) \| < (p-1)/2, \qquad (7.5)$$

где $\| f(n) \|$ — норма функции $f(n)$. Если норму $f(n)$ определить как $\| f(n) \| = \max\limits_{n} f(n)$ и предположить, что $\max\limits_{n} x_1(n) = \max\limits_{2} x_2(n) = B$, то из (7.5) наибольшее значение B определяется как

$$B = \left\lfloor \sqrt{\frac{p-1}{2N}} \right\rfloor. \qquad (7.6)$$

Пример 7.1. Пусть $p = 2^{31} - 1$ и $N = 2^8$. С помощью (7.6) находим значение

$$B = \left\lfloor \sqrt{\frac{2^{31}-1}{2 \cdot 2^8}} \right\rfloor \approx 2^{11},$$

которое означает, что если $-2^{11} \leqslant x_1(n), x_2(n) \leqslant +2^{11}$, то обеспечивается возможность нахождения результата вычислений по (7.4) в интервале

$$\frac{2^{31}-1}{2} \leqslant x_1(n) * x_2(n) \leqslant \frac{2^{31}-1}{2}.$$

В этих условиях GF (p)-арифметика не искажает истинного значения свертки, задаваемой выражением (7.1).

Если задан динамический диапазон сигналов, то из (7.6) следует, что p должно быть больше $2NB^2$. Таким образом, даже небольшой динамический диапазон входных сигналов требует больших значений модуля p (приблизительно равного B^2), а значит, арифметическое устройство, реализующее свертку по выражению (7.3), должно иметь большую разрядную сетку. В этом заключается основной недостаток указанного подхода. Для того чтобы уменьшить длину разрядной сетки, используются ПФГ, определенные над прямыми суммами полей Галуа, а также ТЧП, определенные над конечными гиперкомплексными системами и другими конечными системами [195, 196]. ТЧП над конечными гиперкомплексными системами используются аналогично ПФГ: исходя из интервала определения сигналов $x_1(n)$ и $x_2(n)$ и динамического диапазона изменения этих сигналов (порядка множества E_k) находятся по (7.6) необходимый порядок гиперкомплексной системы и модуль поля GF (p), над которым эта система определена. Так как порядок конечной гиперкомплексной

системы равен p^m (m — размерность системы), то очевидно, что длина разрядной сетки арифметического устройства сокращается в m раз.

Теперь вычислим свертку с помощью ПФГ, определенных над прямыми суммами полей Галуа. Использование таких ПФГ основано на китайской теореме об остатках [3, 7]. Значения сигналов $x_1(n)$ и $x_2(n)$ представляются в виде остатков от деления на ряд взаимно простых чисел $s_1, s_2, \ldots, s_m$:

$$x(n) = x_{s_1}(n),\ x_{s_2}(n),\ \ldots,\ x_{s_m}(n). \tag{7.7}$$

Очевидно, что $x_{s_i}(n) \in Z_{s_i}$ и арифметические операции над компонентом $x_{s_i}(n)$ выполняются по законам конечного кольца Z_{s_i}. При этом арифметические операции могут выполняться параллельно. Динамический диапазон чисел, представленных в системе остаточных классов, определяется выражением [7] $D = s_1 s_2 \ldots s_m$. Разрядная сетка каждого арифметического устройства имеет длину $r_i = \lfloor \log s_i \rfloor$. Ряд взаимно простых чисел $s_1, s_2, \ldots, s_m$ можно выбрать так, что $\log s_i \ll \log D$. Следовательно, длина разрядной сетки арифметического устройства, реализующего операции кольца Z_{s_i} (при самом большом значении s_i), может быть значительно меньше длины разрядной сетки арифметического устройства, реализующего операции с числами разрядности $\lfloor \log D \rfloor$. Если все $s_i = p_i$ — простые числа, то система остатков от деления на ряд $p_1, p_2, \ldots, p_m$ образует поле Галуа, являющееся прямой суммой своих подполей, т. е. эту систему остатков можно отождествить с прямой суммой m полей GF (p_i). Результат вычисления свертки также будет представлен в виде (7.7). Его необходимо преобразовывать в обычную позиционную систему (точнее, в поле Галуа GF (p), где $p = p_1 p_2 \ldots p_m$). При реализации операция, задаваемая равенством (7.7), может быть аппаратурно совмещена с АЦП. Обратное преобразование из системы остаточных классов в поле GF (p) может реализоваться программным путем и в некоторых случаях (если выходной сигнал должен быть представлен в аналоговом виде) совмещаться с ЦАП.

2. Модель вычисления комплексной свертки

Рассмотрим, какие ограничения необходимо наложить на значение модуля p и интервал определения N комплексных сигналов $x(n)$ и $h(n)$, если комплексное ТЧП используется при моделировании свертки:

$$y(n) = \sum_{m=0}^{N-1} h(n-m)\,x(m) = \sum_{n=0}^{N-1} [h_1(n-m)\,x_1(m) - h_2(n-m)\,x_2(m)] + \\ + i \sum_{n=0}^{N-1} [h_1(n-m)\,x_2(m) + h_2(n-m)\,x_1(m)],\ Z_p^c, \tag{7.8}$$

где $h(n) = h_1(n) + ih_2(n)$ и $x(n) = x_1(n) + ix_2(n)$.

Для того чтобы вычисления (7.8), проводимые по законам кольца Z_p^c, совпадали с правильными арифметическими свертками, которые определяются по законам целых вещественных чисел, необходимо ограничить рабочие области комплексных значений сигналов $x(n)$ и $h(n)$. Это означает, что

$$\left|\sum_{m=0}^{N-1} h_1(n-m)\,x_1(m) + h_2(n-m)\,x_2(m)\right| \leqslant$$

$$\leqslant \sum_{m=0}^{N-1} (|h_1(n-m)|\,|x_1(m)| + |h_2(n-m)|\,|x_2(m)|) \leqslant \frac{p-1}{2}, \quad (7.9)$$

$$\left|\sum_{m=0}^{N-1} h_1(n-m)\,x_2(m) + h_2(n-m)\,x_1(m)\right| \leqslant$$

$$\leqslant \sum_{m=0}^{N-1} [|h_1(n-m)|\,|x_2(m)| + |h_2(n-m)|\,|x_1(m)|] \leqslant \frac{p-1}{2}. \quad (7.10)$$

Если

$$\max_n h_1(n) = \max_n h_2(n) = \max_n x_1(n) = \max_n x_2(n) = B,$$

то из (7.9) и (7.10) наибольшее значение B определяется как

$$B = \left\lfloor \sqrt{\frac{p-1}{4T}} \right\rfloor. \quad (7.11)$$

Пример 7.2. Пусть $p = 2^{31} - 1$ и $N = 2^8$. С помощью (7.11) находим значение

$$B = \left\lfloor \sqrt{\frac{2^{31}-1}{4 \cdot 2^8}} \right\rfloor \approx 2^{20},$$

которое означает, что если $-2^{10} \leqslant h_1(n), h_2(n), x_1(n), x_2(n) \leqslant +2^{10}$, то обеспечивается возможность для $y(n)$ находиться в интервале

$$-\frac{2^{31}-1}{2} \leqslant y(n) \leqslant \frac{2^{31}-1}{2}.$$

Комплексная свертка вычисляется с учетом модели, задаваемой выражением (7.3), т. е. рассчитываются спектры входных последовательностей $x(n)$ и $h(n)$ (соответственно $S_x(\alpha)$ и $S_h(\alpha)$), потом они перемножаются; результат умножения спектров подвергается обратному комплексному ТЧП. Вместо комплексного ТЧП можно использовать ТЧП над прямой суммой полей $\mathrm{GF}(p_1^2) + \ldots + \mathrm{GF}(p_m^2)$. Использование при этом Z_p^c-арифметики либо $\mathrm{GF}(p_1^2) + \ldots + \mathrm{GF}(p_m^2)$-арифметики целиком зависит от динамического диапазона изменения сигналов $x(n)$ и $h(n)$ и допустимой длины разрядной сетки вычислительного устройства. Остановимся на этом вопросе более подробно.

Если задан динамический диапазон B, то модуль M вычисляется из неравенства $M \geqslant 4NB^2$. Если $\log_2 M \leqslant r_{\text{АУ}}$ (где $r_{\text{АУ}}$ — допустимая длина разрядной сетки разрабатываемого вычислительного устрой-

ства либо длина разрядной сетки имеющегося вычислительного устройства), то можно пользоваться Z_M^c-арифметикой. Если $\log_2 M > r_{АУ}$, то придется пользоваться GF (p_1^2) + ... + GF (p_m^2)-арифметикой, выбирая $\max\limits_i p_i$ так, чтобы $r_{АУ} \geqslant \log_2 \max\limits_i p_i$.

Пример 7.3 [201]. Допустим $M = p_1 p_2 = (2^5 - 1)(2^3 - 1) = 217$ и $N = 2^2$. Так как $p_1^2 - 1 = 2^6 (2^4 - 1)$ и $p_2^2 - 1 = 2^4 (2^1 - 1)$, то N делит $p_1^2 - 1$ и $p_2^2 - 1$. Поэтому над $Z_M^c \sim$ GF (31^2) + + GF (7^2) существует Х-преобразование. При этом максимальные значения мнимой и действительной частей сворачиваемых последовательностей $z_1(n) = x_1(n) + iy_1(n)$, $z_2(n) = x_2(n) + iy_2(n)$ не должны превышать величины

$$B = \frac{(2^5 - 1)(2^3 - 1)}{4 \cdot 4} = 2^2.$$

Если входные данные удовлетворяют этому требованию, то можно воспользоваться либо Z_M^c-арифметикой, либо GF (p_1^2) + ... + GF (p_m^2)-арифметикой. Так как $\rfloor \log_2 217 \lfloor = 8$, $\rfloor \log_2 31 \lfloor = 5$, то в первом случае ЦВМ должна быть не менее чем восьмиразрядной, а во втором — не менее чем пятиразрядной. Покажем теперь, что использование второй арифметики приводит к тем же результатам, что и непосредственное вычисление свертки. Возьмем $z_1(n) = 3 + i1$, $z_2(n) = 3 + i0$ для всех значений $n = 0, 1, 2, 3$. Легко показать, что i является элементом порядка $N = 2^2$ в любом из полей GF (31) и GF (7). Теперь вычислим спектры сигналов $z_1(n)$ и $z_2(n)$ (см. (4.6)):

$$S_{z_1}(\alpha) = [{}_1S_{z_1}(\alpha), {}_2S_{z_2}(\alpha)] =$$

$$= \left[\sum_{n=0}^{N-1} z_1(n)(i)^{-\alpha n} \pmod{31}, \sum_{n=0}^{N-1} z_1(n)(i)^{-\alpha n} \pmod 7\right] =$$

$$= \begin{cases} (12 + i4), & (5 + i4) \text{ при } \alpha = 0; \\ (0, & 0) \text{ при } \alpha = 1, 2, 3. \end{cases}$$

Аналогично для сигнала $z_2(n)$ получаем, что

$$S_{z_2}(\alpha) = [{}_1S_{z_2}(\alpha), {}_2S_{z_2}(\alpha)] =$$

$$= \left[\sum_{n=0}^{N-1} z_2(n)(i)^{-\alpha n} \pmod{31}, \sum_{n=0}^{N-1} z_2(n)(i)^{-\alpha n} \pmod 7\right] =$$

$$= \begin{cases} (12, & 5) \text{ при } \alpha = 0; \\ (0, & 0) \text{ при } \alpha = 1, 2, 3. \end{cases}$$

Перемножаем спектры и находим спектр $S_{z_3}(\alpha) = [{}_1S_{z_3}(\alpha), {}_2S_{z_3}(\alpha)]$ искомого сигнала:

$$[{}_1S_{z_3}(\alpha), {}_2S_{z_3}(\alpha)] = [{}_1S_{z_1}(\alpha)\,{}_1S_{z_2}(\alpha), {}_2S_{z_1}(\alpha)\,{}_2S_{z_2}(\alpha)] =$$

$$= \begin{cases} (20 + i17), & (4 + i6) \text{ при } \alpha = 0; \\ (0, & 0) \text{ при } \alpha = 1, 2, 3. \end{cases}$$

Действуя обратным преобразованием, получаем выражение для $z_3(n)$ в [GF (31) + GF (7)]-арифметике:

$$[{}_1z_3(n),\ {}_2z_3(n)] = 4^{-1}\left[\sum_{\alpha=0}^{N-1} {}_1S_{z_3}(\alpha)\,(i)^{\alpha n},\ \sum_{\alpha=0}^{N-1} {}_2S_{z_3}(\alpha)\,(i)^{\alpha n}\right].$$

Так как $4^{-1} = 8 \pmod{31}$, $4^{-1} = 2 \pmod 7$, то

$$[{}_1Z_3(n),\ {}_2Z_3(n)] = (5 + i12,\ 1 + i15), \quad n = 0,\ 1,\ 2,\ 3. \qquad (7.12)$$

Для того чтобы найти значение свертки $({}_1Z_3(n),\ {}_2Z_3(n))$ в Z_p^c-арифметике, необходимо на (7.12) подействовать отображением Ψ^{-1} (см. параграф 2 четвертой главы и выражение (4.3)). В соответствии с выражением (4.4) находим

$$m_1 = M/p_1 = 217/31 = 7; \quad m_2 = M/p_2 = 217/7 = 31.$$

Далее

$$m_1^{-1} = (m_1 \bmod 31)^{-1} \bmod 31 = 7^{-1} \bmod 31 = 9 \pmod{31};$$
$$m_2^{-1} = (m_2 \bmod 7)^{-1} \bmod 7 = 3^{-1} \pmod 7 = 5 \pmod 7.$$

Поэтому

$$z_3(n) = x_3(n) + iy_3(n) = m_1m_1^{-1}z_3(n) + m_2m_2^{-1}z_3(n) =$$
$$= [m_1m_1^{-1}x_3(n) + m_2m_2^{-1}x_3(n)] + i\,[m_1m_1^{-1}y_3(n) + m_2m_2^{-1}y_3(n)] =$$
$$= [17 \cdot 9 \cdot 5 + 31 \cdot 5 \cdot 1] + i\,[7 \cdot 9 \cdot 12 + 31 \cdot 5 \cdot 3] =$$
$$= 36 + i12 \pmod{217}, \quad n = 0,\ 1,\ 2,\ 3.$$

Непосредственное вычисление свертки последовательностей $z_1(n)$, $z_2(n)$ дает аналогичный результат.

Упражнение 7.1. Провести детально все вычисления в примере 7.2.

Таким образом, для вычисления свертки и корреляции последовательностей комплексных чисел необходимо входные данные из Z_M^c-арифметики перевести в $\sum_i$ GF (p_i)-арифметику. Затем вычислить свертки с использованием спектрального анализа. Полученные результаты из $\sum_i$ GF (p_i)-арифметики могут быть снова переведены в Z_M^c-арифметику.

3. Быстрая одномерная свертка с помощью многомерных методов

На практике очень часто приходится вычислять свертку очень длинных числовых последовательностей (цифровых сигналов). Если свертка вычисляется с учетом моделей, задава-

емых выражениями (7.1) — (7.3), то при увеличении длины последовательностей значительно увеличивается объем вычислений. Поэтому сокращение объема вычислений — актуальная задача. Одним из методов ее решения является метод вычисления одномерной свертки многомерными методами с применением ТЧП [34].

Итак, пусть заданы две числовые последовательности $x(t)$ и ht, где $t \in E_N$; $x(t)$, $h(t) \in E_k$. Для удобства будем считать, что переменная t принимает значения $t = 0, 1, 2, \ldots, T-1$. Рассмотрим циклическую свертку этих последовательностей:

$$y(t) = \sum_{\tau=0}^{T-1} h(t-\tau)\, x(\tau), \quad \tau = 0, 1, 2, \ldots, T-1. \tag{7.13}$$

Представим T в виде произведения

$$T = T_1 T_2. \tag{7.14}$$

Сделаем замену переменных t и τ в (7.13) следующим образом:

$$t = (t_1, t_2) = t_1 T_1 + t_2; \quad \tau = (\tau_1 \tau_2) = \tau_1 T_1 + \tau_2, \tag{7.15}$$

где

$$t_1, \tau_1 = 0, 1, 2, \ldots, T_1 - 1; \quad t_2 \tau_2 = 0, 1, 2, \ldots, T_2 - 1. \tag{7.16}$$

При этом (7.13) превращается в

$$y(t_1 T_1 + t_2) = \sum_{\tau_2=0}^{T_2-1} \sum_{\tau_1=0}^{T_1-1} h(t_1 T_1 + t_2 - \tau_1 T_1 - \tau_2)\, x(\tau_1 T_1 + \tau_2). \tag{7.17}$$

Определим теперь двухмерный массив $\hat{x}(t_1, t_2)$ размером $T_1 \times T_2$ из первоначального сигнала $x(t)$ длиной $T = T_1 T_2$ в виде

$$\hat{x}(t_1, t_2) = x(t_1 T_1 + t_2).$$

Подобным образом определяются $\hat{h}$ и $\hat{y}$:

$$\hat{h}(t_1, t_2) = h(t_1 T_1 + t_2); \quad \hat{y}(t_1 t_2) = y(t_1 T_1 + t_2). \tag{7.18}$$

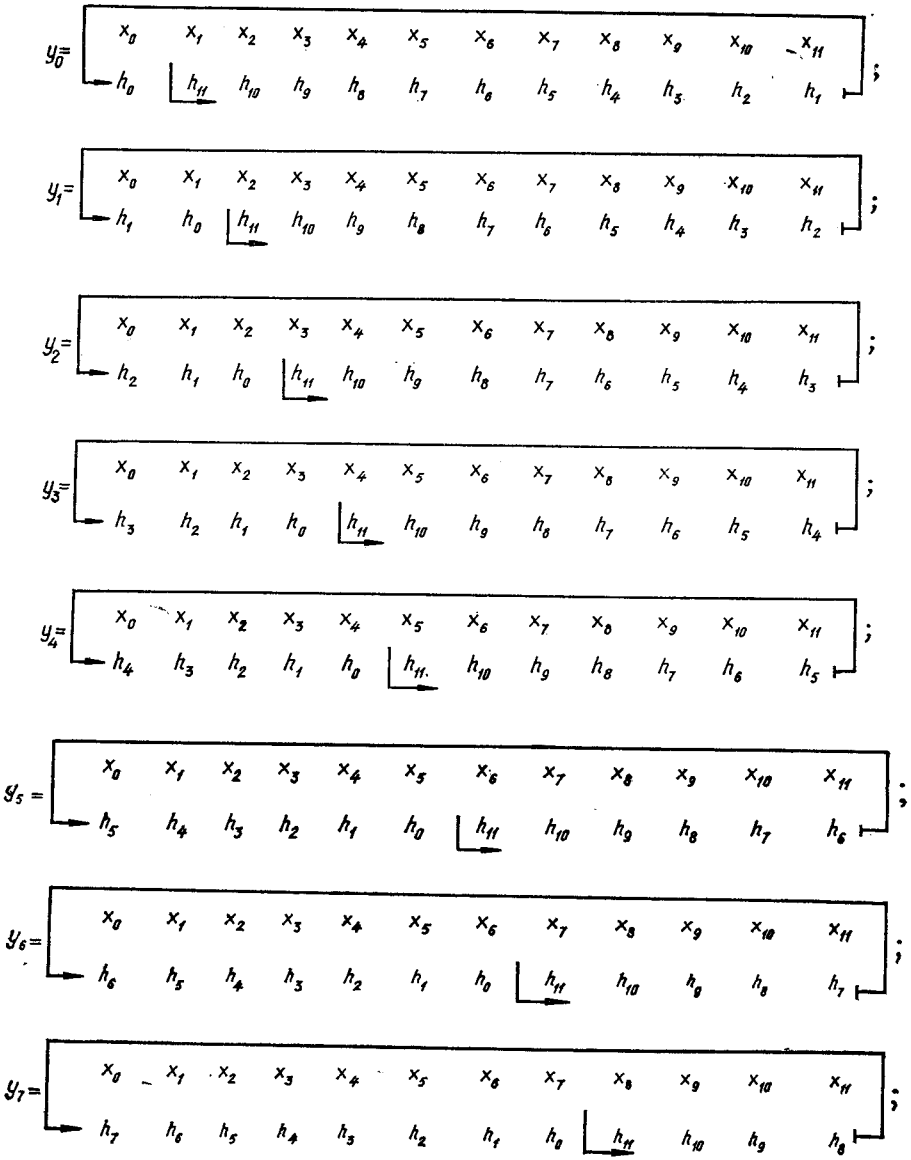
В этих обозначениях (7.13) превращается в выражение

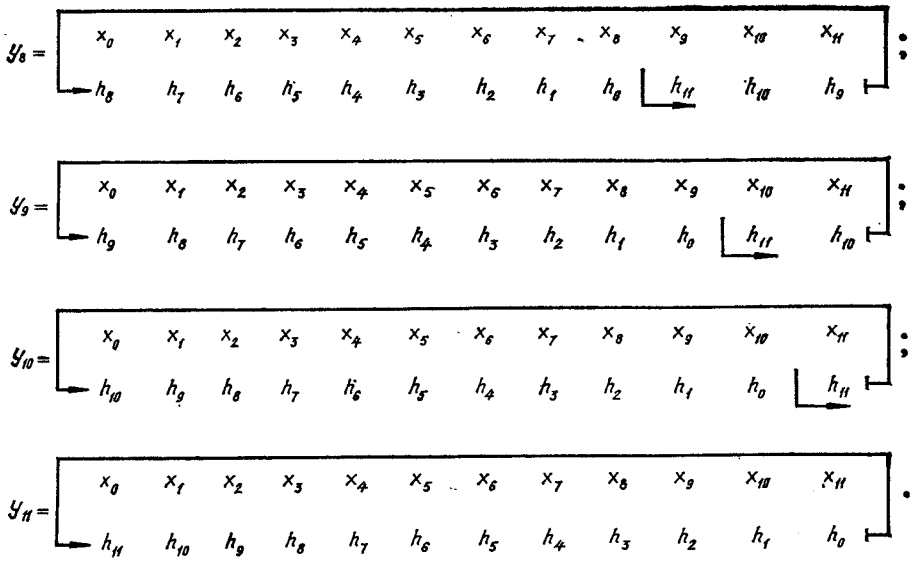
$$\hat{y}(t_1, t_2) = \sum_{t_2=0}^{T_2-1} \sum_{t_1=0}^{T_1-1} \hat{h}(t_1 - \tau_1, t_2 - \tau_2)\, \hat{x}(\tau_1, \tau_2), \tag{7.19}$$

которое представляет собой двухмерную свертку.

Заметим, что здесь требуются значения $\hat{h}$ вне массива $T_1 \times T_2$. Поскольку эти необходимые значения $\hat{h}$ входят в выражение (7.19), где $1 - T_1 \leqslant t_1 - \tau_1 \leqslant T_1 - 1$ и $1 - T_2 \leqslant t_2 - \tau_2 \leqslant T_2 - 1$, двухмерные сигналы $\hat{h}$ и $\hat{x}$ расширяют таким образом, чтобы двухмерная свертка давала желаемый результат. Расширенные сиг-

налы обозначим через $\hat{\hat{h}}$ и $\hat{\hat{x}}$. Поясним сказанное на примере. Пусть нужно циклически свернуть две последовательности. Пользуясь формулой (7.13) для значения свертки $y(t) = x(t) * h(t)$, получаем сумму следующих покомпонентных произведений:



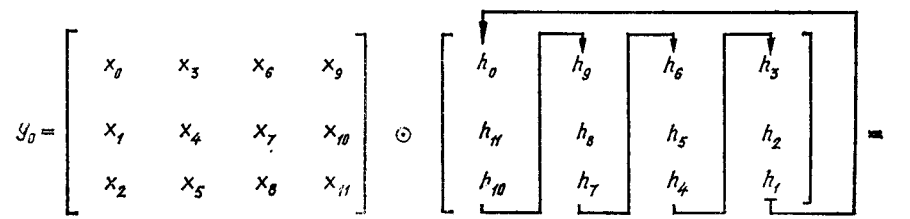


Здесь $x(t) = x_0\ x_1 \ldots x_{10}x_{11}$ и $h(t) = h_0h_1 \ldots h_{10}h_{11}$.

Так как $T = 12$, то $T_1 = 3$, $T_2 = 4$ и из $x(t)$ и $h(t)$ находим следующие массивы $\hat{x}(t_1, t_2)$, $\hat{h}(t_1, t_2)$:

$$\hat{x} = \begin{bmatrix} x_0 & x_3 & x_6 & x_9 \\ x_1 & x_4 & x_7 & x_{10} \\ x_2 & x_5 & x_8 & x_{11} \end{bmatrix}; \quad \hat{h} = \begin{bmatrix} h_0 & h_3 & h_6 & h_9 \\ h_1 & h_4 & h_7 & h_{10} \\ h_2 & h_5 & h_8 & h_{11} \end{bmatrix}.$$

Причем этот процесс сворачивания последовательностей $x(t)$ и $h(t)$ в новом виде будет выглядеть так:



$$= \hat{X} \odot \hat{H}(-\tau_1, -\tau_2),$$

Подобная запись здесь и далее будет означать, что для получения соответствующего значения $y(t)$ необходимо матрицы покомпонентно перемножить и результаты сложить, т. е. скалярно перемножить матрицы $\hat{X}$ и $\hat{H}_{\tau_1,\tau_2}$. Для последующих значений $y(t)$ будем иметь

$$y_0 = \hat{X} \odot \hat{H}_{00} = \hat{X} \odot \begin{bmatrix} h_0 & h_9 & h_6 & h_3 \\ h_{11} & h_8 & h_5 & h_2 \\ h_{10} & h_7 & h_4 & h_1 \end{bmatrix}; \quad y_1 = \hat{X} \odot \hat{H}_{01} = \hat{X} \odot \begin{bmatrix} h_1 & h_{10} & h_7 & h_4 \\ h_0 & h_9 & h_6 & h_3 \\ h_{11} & h_8 & h_5 & h_2 \end{bmatrix};$$

$$y_2 = \hat{X} \odot \hat{H}_{02} = \hat{X} \odot \begin{bmatrix} h_2 & h_{11} & h_8 & h_5 \\ h_1 & h_{10} & h_7 & h_4 \\ h_0 & h_9 & h_6 & h_3 \end{bmatrix}; \quad y_3 = \hat{X} \odot \hat{H}_{10} = \hat{X} \odot \begin{bmatrix} h_3 & h_0 & h_9 & h_6 \\ h_2 & h_{11} & h_8 & h_5 \\ h_1 & h_{10} & h_7 & h_4 \end{bmatrix};$$

$$y_4 = \hat{X} \odot \hat{H}_{11} = \hat{X} \odot \begin{bmatrix} h_4 & h_1 & h_{10} & h_7 \\ h_3 & h_0 & h_9 & h_6 \\ h_2 & h_{11} & h_8 & h_5 \end{bmatrix}; \quad y_5 = \hat{X} \odot \hat{H}_{12} = \hat{X} \odot \begin{bmatrix} h_5 & h_2 & h_{11} & h_8 \\ h_4 & h_1 & h_{10} & h_7 \\ h_3 & h_0 & h_9 & h_6 \end{bmatrix};$$

$$y_6 = \hat{X} \odot \hat{H}_{20} = \hat{X} \odot \begin{bmatrix} h_6 & h_3 & h_0 & h_9 \\ h_5 & h_2 & h_{11} & h_8 \\ h_4 & h_1 & h_{10} & h_7 \end{bmatrix}; \quad y_7 = \hat{X} \odot \hat{H}_{21} = \hat{X} \odot \begin{bmatrix} h_7 & h_4 & h_1 & h_{10} \\ h_6 & h_3 & h_0 & h_9 \\ h_5 & h_2 & h_{11} & h_8 \end{bmatrix};$$

$$y_8 = \hat{X} \odot \hat{H}_{22} = \hat{X} \odot \begin{bmatrix} h_8 & h_5 & h_2 & h_{11} \\ h_7 & h_4 & h_1 & h_{10} \\ h_6 & h_3 & h_0 & h_9 \end{bmatrix}; \quad y_9 = \hat{X} \odot \hat{H}_{30} = \hat{X} \odot \begin{bmatrix} h_9 & h_6 & h_3 & h_0 \\ h_8 & h_5 & h_2 & h_{11} \\ h_7 & h_4 & h_1 & h_{10} \end{bmatrix};$$

$$y_{10} = \hat{X} \odot \hat{H}_{31} = \hat{X} \odot \begin{bmatrix} h_{10} & h_7 & h_4 & h_1 \\ h_9 & h_6 & h_3 & h_0 \\ h_8 & h_5 & h_2 & h_{11} \end{bmatrix}; \quad y_{11} = \hat{X} \odot \hat{H}_{32} = \hat{X} \odot \begin{bmatrix} h_{11} & h_8 & h_5 & h_2 \\ h_{10} & h_7 & h_4 & h_1 \\ h_9 & h_6 & h_3 & h_0 \end{bmatrix}.$$

На всех этапах получения $y(t)$ процесс изменения матрицы $\hat{H}$ нельзя представить в виде ее двухмерных циклических сдвигов. Однако элементы подобных сдвигов в этом процессе все же имеются. Для этого обратим внимание на закономерности изменения $\hat{H}$ в группах $y_0 - y_2$; $y_3 - y_5$; $y_6 - y_8$; $y_9 - y_{11}$. Матрица $\hat{H}_{01}$ получается из $\hat{H}_{00}$ сдвигом вниз на одну позицию строк матрицы $\hat{H}_{00}$, при этом в $\hat{H}_{01}$ в качестве первой строки появляется строка $h_1h_{10}h_7h_4$, которой вообще не было в $\hat{H}_{00}$. Увеличим количество строк в матрице $\hat{H}$ в два раза (т. е. перейдем к массивам $\hat{\hat{H}}$, $\hat{\hat{X}}$), последней строкой которой сделаем строку $h_1h_{10}h_7h_4$:

$$\hat{\hat{H}}_{00} = \begin{bmatrix} h_0 & h_9 & h_6 & h_3 \\ h_{11} & h_8 & h_5 & h_2 \\ h_{10} & h_7 & h_4 & h_1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ h_1 & h_{10} & h_7 & h_4 \end{bmatrix}; \quad \hat{\hat{H}}_{01} = \begin{bmatrix} h_4 & h_{10} & h_7 & h_4 \\ h_0 & h_9 & h_6 & h_3 \\ h_{11} & h_8 & h_5 & h_2 \\ h_{10} & h_7 & h_4 & h_1 \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}. \qquad (7.20)$$

Тогда переход от $\hat{\hat{H}}_{00}$ к $\hat{\hat{H}}_{01}$ осуществляется циклическим сдвигом строк матрицы $\hat{\hat{H}}_{00}$. Сравнение $\hat{\hat{H}}_{00}$ с $\hat{\hat{H}}_{02}$ показывает, что у матрицы $\hat{\hat{H}}_{00}$ второй строкой снизу должна быть строка $h_2h_{11}h_8h_5$:

$$\hat{\hat{H}}_{00} = \begin{bmatrix} h_0 & h_9 & h_6 & h_3 \\ h_{11} & h_8 & h_5 & h_2 \\ h_{10} & h_7 & h_4 & h_1 \\ \cdot & \cdot & \cdot & \cdot \\ h_2 & h_{11} & h_8 & h_5 \\ h_1 & h_{10} & h_7 & h_4 \end{bmatrix}. \qquad (7.21)$$

Если теперь перейти от $\hat{X}$ к $\hat{\hat{X}}$:

$$\hat{\hat{X}} = \begin{bmatrix} x_0 & x_3 & x_6 & x_9 \\ x_1 & x_4 & x_7 & x_{10} \\ x_2 & x_5 & x_8 & x_{11} \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}, \tag{7.22}$$

то при циклической двухмерной свертке $\hat{\hat{H}}$ и $\hat{\hat{X}}$ вклад в $\hat{\hat{Y}}$ будут вносить только те матричные элементы $\hat{\hat{H}}$, которые находятся в верхней половине $\hat{\hat{H}}_{00}$. Теперь нетрудно видеть, что при циклических сдвигах строк и столбцов матрицы $\hat{\hat{H}}_{00}$ верхняя ее половина изменяется точно так же, как матрица $\hat{H}_{00}$, поэтому в верхней половине массива $\hat{\hat{Y}} = \hat{\hat{H}} * \hat{\hat{X}}$ будут сосредоточены значения циклической свертки $y(t) = h(t) * x(t)$. В матрице $\hat{\hat{H}}_{00}$ одна строка оказалась неопределенной, но эта строка не нужна для нахождения верхней половины $\hat{\hat{Y}}$ и, в принципе, может быть любой. Однако мы ее определим таким образом, чтобы в $\hat{\hat{H}}_{00}$ была некоторая закономерность. Поскольку в выражении (7.21) $\hat{H}_{00}$ соответствует массиву $\hat{\hat{H}}$ $(-t_1 - t_2)$, определим незаполненную строку периодическим продолжением столбцов нижней половины матрицы $\hat{\hat{H}}$ $(t_1\ t_2)$:

$$\hat{\hat{H}} = \begin{bmatrix} h_0 & h_3 & h_6 & h_9 \\ h_1 & h_4 & h_7 & h_{10} \\ h_2 & h_5 & h_8 & h_{11} \\ h_9 & h_0 & h_3 & h_6 \\ h_{10} & h_1 & h_4 & h_7 \\ h_{11} & h_2 & h_5 & h_8 \end{bmatrix}. \tag{7.23}$$

Если поменять местами нижнюю и верхнюю половины матрицы в (7.23), то верный ответ (циклическая одномерная свертка) будет находиться в нижней половине $\hat{Y}$. При этом

$$\hat{\hat{H}} = \begin{bmatrix} h_9 & h_0 & h_3 & h_6 \\ h_{10} & h_1 & h_4 & h_7 \\ h_{11} & h_2 & h_5 & h_8 \\ h_0 & h_3 & h_6 & h_9 \\ h_1 & h_4 & h_7 & h_{10} \\ h_2 & h_5 & h_8 & h_{11} \end{bmatrix}.$$

Этот массив сформирован так, что столбцы содержат периодическое расширение первоначальной последовательности $h(t)$, находящейся в верхней половине матрицы:

$$\hat{\hat{H}} = \begin{bmatrix} h(T_2T_1 - T_1) & h(0) & \dots & h(T_2T_1 - 2T_1) \\ h(T_2T_1 + 1) & h(1) & \dots & h(T_2T_1 - 2T_1 + 1) \\ \dots & \dots & \dots & \dots \\ h(T_2T_1 - 1) & h(T_1 - 1) & \dots & h(T_2T_1 - T_1 - 1) \\ h(0) & h(T_1) & \dots & h(T_2T_1 - T_1) \\ h(1) & h(T_1 + 1) & \dots & h(T_2T_1 - T_1 + 1) \\ \dots & \dots & \dots & \dots \\ h(T_1 - 1) & h(2T_1 - 1) & \dots & h(T_2T_1 - 1) \end{bmatrix}.$$

Для получения результата одномерной свертки в верхней половине матрицы $\hat{\hat{Y}}$ массив $\hat{\hat{H}}$ в самой общей форме должен иметь следующий вид:

$$\hat{\hat{H}} = \begin{bmatrix} h(0) & h(T_1) & \dots & h(T_2T_1 - T_1) \\ h(1) & h(T_1 + 1) & \dots & h(T_2T_1 - T_1 + 1) \\ \dots & \dots & \dots & \dots \\ h(T_1 - 1) & h(2T_1 - 1) & \dots & h(T_2T_1 - 1) \\ h(T_2T_1 - T_1) & h(0) & \dots & h(T_2T_1 - T_1) \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ h(T_2T_1 - 1) & h(T_1 - 1) & \dots & h(T_2T_1 - 1) \end{bmatrix}.$$

Таким образом, исходную свертку на циклической группе $G_T = G_{T_1T_2}$ мы свели к двухмерной циклической свертке на группе $G_{2T_1} \times G_{T_2}$. При использовании одномерного ДПФ на G_T необходимо осуществить $2T \log T$ операций умножения для прямого преобразования, $4T$ умножений для перемножения спектров и $2T \log T$ умножений для обратного ДПФ. В сумме будем иметь $n_1 = 4T \log T + 4T$ умножений. Использование двухмерного ДПФ на $G_{2T_1} \times G_{T_2}$ дает значение $n_{II} = 3T \log T + 12T$, что незначительно меньше n_I. Поэтому применять двухмерный подход с ДПФ для повышения эффективности вычислений свертки нецелесообразно.

Преимущества в вычислениях по сравнению с одномерным ДПФ появляются при использовании двухмерного преобразования Ферма, где возможным ограничением является требование на длины слов сумматора, которые должны быть равны $n_{АУ} = T$. Если нам нужно $T = 1024$, то и длина разрядной сетки должна быть такой же, что, естественно, нереально. Так как при двухмерном преобразовании Ферма длина $n_{АУ}$ пропорциональна либо $2T_1$, либо T_2, а не $T = T_1T_2$, как при одномерном преобразовании, длина $n_{АУ}$ пропорциональна примерно корню квадратному из T. Именно это уменьшение необ-

ходимой длины слова делает двухмерную формулировку привлекательной для преобразования Ферма (табл. 34). При вычислении двухмерной свертки есть преимущество в проведении преобразования сначала по размерности t_2 (длина T_2), а потом по размерности t_1 (длина T_1), так как половина из строк $\hat{\hat{X}}$ по размерности t_1 равна нулю и половина из строк $\hat{\hat{H}}$ по размерности t_2 циклически сдвинута на одну позицию относительно другой половины последовательностей. Кроме того, при проведении обратного преобразования выгоднее сначала брать обратное преобразование по t_1, а потом по t_2, так как нам нужна только половина последовательностей $\hat{\hat{Y}}$, следовательно, только половина последовательностей должна быть обращена по t_2. Следует иметь в виду, что явно выигрывая в длине слова при использовании двухмерного преобразования, мы проигрываем в объеме памяти. При использовании одномерной методики необходимо хранить на всех этапах преобразований T чисел, а при использовании двухмерной методики — $2T$.

Таблица 34. **Ограничения на длины последовательностей для наиболее часто встречающихся длин слов и значений $\varepsilon = 2$, $\varepsilon = \sqrt{2}$**

Длина слова, бит	ε	max N	
		Преобразование	
		одномерное	двухмерное
16	2	16	256
16	$\sqrt{2}$	32	1024
32	2	32	1024
32	$\sqrt{2}$	64	4096
64	2	64	4096
64	$\sqrt{2}$	228	16 384

Рассмотренный метод допускает дальнейшее обобщение. Например, T можно было бы разложить на три сомножителя $T = T_1T_2T_3$. Тогда сигналы $x(t)$, $h(t)$ были бы определены как трехмерные массивы и одномерная свертка превратилась бы в трехмерную свертку путем замены переменных. Для $x(t)$

$$\hat{X}(t_1, t_2, t_3) = x(T_3T_2t_1 + T_3t_2 + t_3).$$

При определении таким же способом $\hat{H}$ и $\hat{Y}$ свертка (7.13) превращается в трехмерную свертку $\hat{\hat{Y}} = \hat{\hat{H}} * \hat{\hat{X}}$. Тогда мы имели бы одномерную циклическую свертку последовательностей длины T, проводимую посредством трехмерной циклической свертки с размерностями длин $2T_1$, $2T_2$ и T_3.

Если длина сигналов, которые надо циклически свернуть в (7.13), может быть представлена как $T = 2^m$, то используемый метод можно обобщить для определения m-мерного сигнала с длиной 2 по каждой координате. Как и прежде, это делается записью чисел t и τ в двоичной системе счисления:

$$\hat{X}(t_1, t_2, \ldots, t_m) = x(2^{m-1}t_1 + 2^{m-2}t_2 + \cdots + t_m), \quad t_i = 0, 1.$$

В частности, следует, что преобразование Уолша существует над любым кольцом Z_M, где M — нечетное число. Действительно,

преобразование Уолша действует в пространстве $L(H_2 \dotplus H_2 \dotplus \ldots \ldots \dotplus H_2, Z_M)$. Поэтому $q = 2$. Так как q_i нечетное, то в каноническом разложении могут быть только степени нечетных сомножителей $q_1, q_2, \ldots, q_s$. Поэтому $2 \mid \text{НОД}(q_1 - 1, q_2 - 1, \ldots, q_s - 1)$. Пусть теперь группа $H = H_{2^{k_1}} \dotplus H_{2^{k_2}} \dotplus \ldots \dotplus H_{2^{k_m}}$, где $k_1, k_2, \ldots, k_m$ — некоторые целые числа; $Z_M = Z_{2^{2^m}+1}$; $2^{2^m} + 1$ — числа Ферма такие, что $k_i < 2^{m+2}$, $i = 1, 2, \ldots, m$.

Так как

$$q = \text{НОК}(2^{k_1}, 2^{k_2}, \ldots, 2^{k_m}) = \max_i 2^{k_i} = 2^{k_{\max}}$$

и каждый простой делитель числа Ферма имеет вид $e2^{m+2} + 1$, то

$$2^{k_{\max}} \mid \text{НОД}(e_1 2^{m+2}, e_2 2^{m+2}, \ldots, e_m 2^{m+2}).$$

Поэтому в пространстве $L(H_2 \dotplus H_2 \dotplus \ldots \dotplus H_2, Z_M)$ существует преобразование Уолша — Крестенсона — Галуа.

4. Оценка корреляционной функции

Исследуем возможность применения ПФГ при анализе случайных процессов. Пусть $x(n)$ является реализацией стационарного случайного процесса [23, 118], проквантованного по уровню и по времени, длительностью N_0. Эта реализация разбита на $k = N_0/N$ непересекающихся участков длительностью N каждый. Кроме того, пусть множество значений реализации $x(n)$ совпадает с множеством E_k. Тогда можно считать, что $x(n) \in L(G_N, \text{GF}(p))$.

Для дальнейшего изложения необходимо четко различать следующие виды КФ. Во-первых, выделим КФ, которую обозначим через $G_N\text{GF}(p)$-КФ и которая определяется выражением

$$b_G(m) = \sum_{k=1}^{k} \sum_{n=0}^{N-1} x^k(n)\, x^k(n \ominus m), \ \text{GF}(p), \qquad (7.24)$$

где $x^k(n)$ — цифровой сигнал, определенный на интервале N и являющийся участком реализации; $\ominus$ — операция вычитания по модулю N. При вычислении этой КФ все операции (умножение, деление, вычитание, сложение) производятся по законам поля GF (p), так как реализации считаются принадлежащими пространству $L(G_N, \text{GF}(p))$. Эти реализации можно считать принадлежащими пространству $L(G_N, \boldsymbol{R})$. Исходя из такой договоренности, можно ввести $G_N\boldsymbol{R}$ = КФ, которая задается следующим выражением:

$$b_{\text{кв}}(m) = \sum_{k=1}^{k} \sum_{n=0}^{N-1} x^k(n)\, x^k(n \ominus m), \ Z \text{ (или } \boldsymbol{R}). \qquad (7.25)$$

В этом выражении все операции производятся по законам поля вещественных чисел (более точно — по законам кольца целых чисел).

И наконец, нужна квантованная арифметическая КФ над полем вещественных чисел (кольцом целых чисел Z), которую можно опре-

делить следующим образом:

$$R_{\text{кв}}(m) = \sum_{k=1}^{n} \sum_{n=0}^{N-1} x^k(n)\, x^k(n-m), \quad \boldsymbol{Z}\ (\text{или } \boldsymbol{R}) \tag{7.26}$$

и которую будем называть GZ-КФ. Кроме того, можно рассматривать еще один вид КФ (GGF (p)-КФ):

$$R_G(m) = \sum_{k=1}^{k} \sum_{n=0}^{N-1} x^k(n)\, x^k(n-m), \quad \mathrm{GF}(p). \tag{7.27}$$

Различия между $G_N\mathrm{GF}(p)$-КФ и $G_N R$-КФ, а также между GGF (p)-КФ и GR-КФ определяются только нашей точкой зрения на реализации $x^k(n)$. Либо они считаются принадлежащими пространству $L(G_N, \mathrm{GF}(p))$, либо пространству $L(Z, \mathrm{GF}(p))$. Приведенные выше четыре КФ (см. выражения (7.24) — (7.27)) удовлетворяют следующим очевидным соотношениям:

$$b_G(m) = R_G(m) + R_G(N-m), \quad \mathrm{GF}(p); \tag{7.28}$$

$$b_{\text{кв}}(m) = R_{\text{кв}}(m) + R_{\text{кв}}(N-m), \quad \boldsymbol{R}.$$

Нас будет интересовать следующий вопрос: при каких условиях GGF (p)-КФ, подсчитанная по законам поля GF (p), будет совпадать с GR-КФ, подсчитанной по законам кольца целых чисел? Ясно пока одно, что если взять характеристику (порядок) поля GF (p) достаточно большой, то получим $R_G(m) = R_{\text{кв}}(m)$, а значит, и $b_G(m) = b_{\text{кв}}(m)$.

Что значит взять характеристику поля достаточно большой? Это означает, что в процессе вычислений КФ $b_G(m)$ или $R_G(m)$ по формулам (7.24) и (7.28) ни один из промежуточных результатов (и окончательный) не превысит величины p. При этом условии результаты арифметических операций в поле GF (p) и в кольце целых чисел совпадают. Действительно, пусть $p = 8191$ и складываются и умножаются два числа 10 и 21. Результаты этих операций как в поле GF (8191), так и в кольце целых чисел одинаковы:

$$10 + 21 = 31 \pmod{8191}; \qquad 10 \cdot 21 = 210 \pmod{8191};$$

$$10 + 21 = 31 \text{ в кольце } \boldsymbol{Z}; \qquad 10 \cdot 21 = 210 \text{ в кольце } \boldsymbol{Z}.$$

Маленькие участки земной поверхности кажутся плоскими, хотя Земля имеет шарообразную форму. Так и в данном случае, операции над маленькими числами по модулю большого простого числа приводят к тем же результатам, что и операции над этими числами в кольце целых чисел.

Попытаемся теперь найти то наименьшее значение p, ниже которого вычисления по законам поля GF (p) будут приводить к результатам, отличающимся от тех, которые получались бы при расчете по законам кольца целых чисел. Ясно, что характеристика p должна удовлетворять неравенству

$$0{,}5p > R_{\text{кв}}(m) = \sum_{k=1}^{k} R^k_{\text{кв}}(m), \quad m \in E_N.$$

Так как $R_{кв}(m)$ достигает максимума при $m = 0$, то последнее неравенство можно заменить на следующее:

$$0{,}5p > R_{кв}(0) = \sum_{k=1}^{h} \sum_{n=0}^{N-1} [x^k(n)]^2.$$

Поскольку $R_{кв}(0)$ является случайной, необходимо потребовать, чтобы это неравенство выполнялось с некоторой практически приемлемой вероятностью. Для этого необходимо знать или закон распределения величины $R^k_{кв}(0)$, или ее математическое ожидание $M[R_{кв}(0)]$ и дисперсию $D[R^k_{кв}]$. Тогда можно потребовать, чтобы

$$0{,}5p > k\left\{M[R^k_{кв}(0)] + l\sqrt{D[R^k_{кв}(0)]}\right\}, \qquad (7.29)$$

где $l = 1, 2, 3, \ldots$.

Для математического ожидания

$$M[R^k_{кв}(0)] = \frac{1}{N}\sum_{n=0}^{N-1} M[x^k(0)] = [m_x^2]_{кв} + [\sigma_x^2]_{кв},$$

где $[m_x^2]_{кв}$ и $[\sigma_x^2]_{кв}$ — соответственно среднеквадратичное значение и математическое ожидание изучаемого стационарного процесса $x(n)$.

Полагая, что процесс $x(n)$ имеет нормальное распределение вероятностей, для дисперсии оценки $R_{кв}(0)$ можно получить соотношение [23, 118]

$$D[R^k_{кв}(0)] = 4N^{-1}\int_0^N \{[R^2_{кв}(m)] + 2[m_x^2]_{кв}[R_{кв}(m)]\}\,dm. \qquad (7.30)$$

Рассмотрим пример низкочастотного случайного процесса, у которого

$$R_{кв}(m) = [R(0)]_{кв}\frac{\sin 2\pi Bm}{2\pi Bm}; \quad S_{кв}(f) = \begin{cases} [S_0]_{кв} + [m_x^2]_{кв}\,\delta(f), & 0 \leqslant f \leqslant B; \\ 0, & f > B. \end{cases}$$

Согласно формуле (7.30)

$$D[R_{кв}(0)] = \frac{R^2_{кв}(0)}{BN} + \frac{2[m_x]_{кв}R_{кв}(0)}{BN}.$$

Поскольку

$$[R_{кв}(0)] = K([\sigma_x^2]_{кв} + [m_x^2]_{кв}),$$

то

$$D[R_{кв}(0)] = \frac{K([\sigma_x^2]_{кв} + [m_x^2]_{кв})([\sigma_x^2]_{кв} + 3[m_x^2]_{кв})}{BN} \leqslant \frac{N([\sigma_x^2]_{кв} + 2[m^2]^2_{кв})}{BN}.$$

Таким образом, для неравенства (7.29) имеем

$$0{,}5p > K\left\{[\sigma_x^2]_{кв} + [m_x^2] + \frac{e}{\sqrt{BN}}([\sigma_x^2]_{кв} + 2[m_x^2]_{кв})\right\}.$$

Для обычно принимаемого значения $e = 3$

$$0{,}5p > K\left\{([\sigma_x^2]_{\text{кв}} + [m_x^2]_{\text{кв}} + \frac{3}{\sqrt{BN}}([\sigma_x^2]_{\text{кв}} + 2[m_x^2]_{\text{кв}})\right\}.$$

Так как для рассматриваемого случайного процесса $\tau_k = 1/2B$ и интервал N делится на некоррелированные отрезки длительностью $N = m\tau_k$ ($n = 1, 2, \ldots$), получим

$$0{,}5p > K\left\{[\sigma_x^2]_{\text{кв}} + [m_x^2] + \frac{3}{\sqrt{n/2}}([\sigma_x^2]_{\text{кв}} + 2[m_x^2]_{\text{кв}})\right\}.$$

Для случая $m \geqslant 2$

$$p > 8K[\sigma_x^2]_{\text{кв}} + 14[m_x^2]_{\text{кв}} K, \tag{7.31}$$

для $m_x = 0$ $p > 8K[\sigma_x^2]_{\text{кв}}$.

Таким образом, если выполняется условие (7.31), то оценка корреляционной функции низкочастотного случайного процесса, вычисленная по законам поля GF (p), совпадает с оценкой, вычисленной по законам чисел, т. е. $R_{\text{кв}}(m) = R_G(m)$.

5. Модели цифрового спектрального анализа

В подавляющем большинстве приложений задача спектрального анализа сводится к нахождению значений z-преобразования конечной реализации сигнала для большого числа точек, равномерно распределенных по окружности единичного радиуса [12, 16, 115, 134, 160]. Измерения такого типа соответствуют вычислению ДПФ конечной последовательности и обычно наиболее эффективно выполняются с применением алгоритмов БПФ. Как правило, интерес представляет энергетический спектр $X_{xy}(\alpha)$ и (или) корреляционная функция $R_{xy}(m)$, которые определяются выражениями

$$R_{xy}(m) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} x(n)\, y(n+m), \quad 0 \leqslant m \leqslant N-1; \tag{7.32}$$

$$X_{xy}(\alpha) = \sum_{m=-\infty}^{\infty} R_{xy}(m)\, \chi_\alpha^{-1}(n); \tag{7.33}$$

$$R_{xy}(m) = \frac{1}{N} \sum_{\alpha=0}^{N-1} X_{xy}(\alpha)\, \chi_\alpha(n). \tag{7.34}$$

Существует два хорошо известных метода измерения спектральной плотности мощности с использованием БПФ [134]. Первый метод основан на вычислении корреляционной функции с помощью алгоритма БПФ, а второй состоит в усреднении последовательности непосредственных измерений спектральной плотности. Математические модели, построенные по первому и по второму методам, схематически показаны на рис. 27, *а* и *б* соответственно. При использовании метода

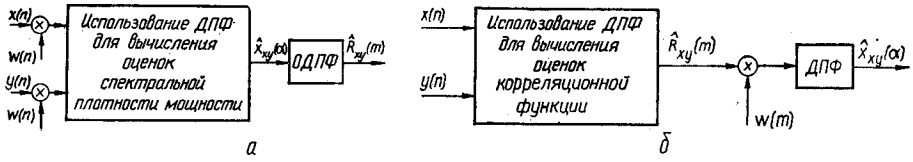


Рис. 27. Модели, выполненные по двум методам спектрального анализа.

БПФ применяется для вычисления оценок корреляционной функции $\hat{R}_{xy}(m)$ на L дискретных отсчетах, где $N = 2L$ — размерность БПФ. При вычислении по значениям $\hat{R}_{xy}(m)$ спектральной плотности мощности (см. (7.33)) для конечного числа частот необходимо применять сглаживающее окно $w(m)$ с целью уменьшения нежелательных эффектов, связанных с конечной длиной выборки, так как вместо бесконечной корреляционной последовательности используется только L ее значений. Значение $R_{xy}(m)$ на L отсчетах можно вычислить по методу, описанному в параграфе 4 настоящей главы. Вычисление БПФ сглаженной корреляционной функции (умноженной на отсчеты окна $w(m)$) можно заменить вычислением ПФГ этой же функции и преобразованием полученного спектра $S_{xy}(\alpha)$ в поле комплексных чисел (рис. 28). В результате оценок спектральной плотности мощности с помощью ПФГ снижается объем вычислений, следовательно, сокращается время спектрального анализа либо аппаратурные затраты, если модель реализуется в виде спектроанализатора. Если спектральный анализ должен осуществляться с высокой точностью, то имеет смысл дополнительная реализация вместо БПФ ПФГ и перехода $S(\alpha) \to X(\alpha)$ (оценка корреляционной функции с помощью ПФГ более точна по сравнению с оценкой, полученной с помощью БПФ, за счет отсутствия шума округлений). Такой подход требует дополнительных аппаратурных затрат на реализацию перехода $S(\alpha) \to X(\alpha)$ и, кроме того, увеличиваются аппаратурные затраты на реализацию ПФГ за счет увеличения длины разрядной сетки, обусловливаемого выполнением условий однозначности перехода $S(\alpha) \to X(\alpha)$.

При использовании второго метода (см. рис. 27, *б*) можно построить модель с использованием ПФГ по схеме, показанной на рис. 29. Здесь ПФГ используется для вычисления сдвинутых спектров $S_i(\alpha)$, $i = 0, 1, \ldots, L_1$, L_1 — число последовательностей в L отсчетов. Подпоследовательности сдвинуты относительно друг друга на T отсчетов. Энергетический спектр получается усреднением спектров подпоследовательностей. Поскольку операция усреднения в конечном поле Галуа не имеет такого физического смысла, как в поле комплексных чисел, необходимо осуществить переход $S_i(\alpha) \to X_i(\alpha)$ для каждой подпоследовательности и усреднять спектры $X_i(\alpha)$, определенные над полем комплексных чисел. В результате получим спектральную плотность мощности $\hat{X}_{xy}(\alpha)$ (см. рис. 29). Далее можно осуществить переход $\hat{X}_{xy}(\alpha) \to \hat{S}_{xy}(\alpha)$ и вычислить $\hat{R}_{xy}(m)$ в

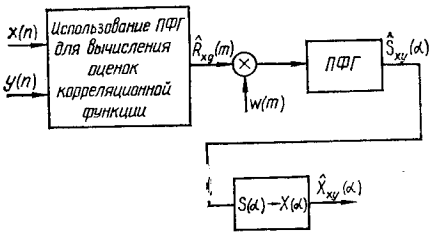
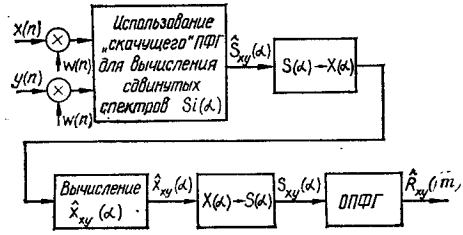
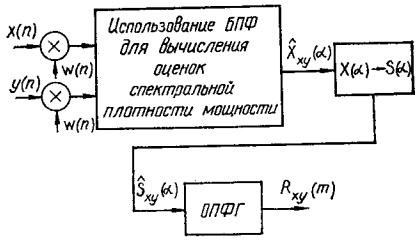


Рис. 28. Вычисление спектральной плотности мощности.

Рис, 29. Вычисление корреляционной функции.

Рис. 30. Комплексный метод вычисления корреляционной функции.





конечном кольце, подвергая $\hat{S}_{xy}(\alpha)$ ОПФГ. Можно вычислить $\hat{R}_{xy}(m)$, непосредственно подвергая $\hat{X}_{xy}(\alpha)$ обратному БПФ. Выбор варианта зависит от конкретно заданных точности вычислений, допустимых аппаратурных затрат, необходимого быстродействия. Схема еще одного возможного варианта построения модели вычислений $\hat{R}_{xy}(m)$ приведена на рис. 30.

6. Модели систем гомоморфной обработки сигналов

Методы гомоморфной обработки сигналов представляют собой класс методов нелинейной обработки сигналов. Эти методы применяются в таких областях, как улучшение изображений, анализ речи, сейсмические исследования и др. [115, 116. 159, 177]. Основаны эти методы на использовании преобразования Фурье. Реализация моделей гомоморфной обработки сигналов связана с большим объемом вычислений, снижения которого можно добиться заменой преобразования Фурье на преобразование Фурье — Галуа (и корректировка в связи с этим модели в целом).

Входные и выходные сигналы некоторой системы можно рассматривать как векторы в векторных пространствах V_1 и V_2 над полями F_1 и F_2 соответственно. Система в общем случае осуществляет отображение $V_1 \to V_2$. Для многих практически важных приложений поля F_1 и F_2 совпадают: $F_1 = F_2 = F$. Ограничимся рассмотрением этого случая.

Обозначим операции в векторных пространствах V_1 и V_2 над полем F через $\overset{1}{+}$, $\overset{1}{\cdot}$ и $\overset{2}{+}$, $\overset{2}{\cdot}$ соответственно.

Определение 7.1. [115, 116]. Гомоморфными системами называются системы, удовлетворяющие обобщенному принципу суперпо-

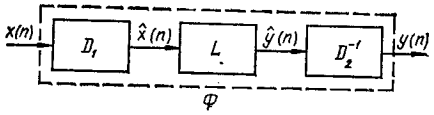


Рис. 31. Каноническое представление гомоморфных систем,

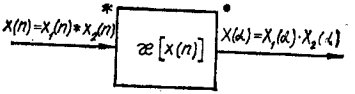


Рис. 32. Ортогональное преобразование как гомоморфное преобразование от свертки к умножению.

зиции, т. е. системы, для которых справедливы соотношения

$$f[x_1(n) \overset{1}{+} x_2(n)] = f[x_1(n)] \overset{2}{+} f[x_2(n)]; \tag{7.35}$$

$$f[c \overset{1}{\cdot} x_1(n)] = c \overset{2}{\cdot} f[x_1(n)], \tag{7.36}$$

где f — преобразование, осуществляемое системой, являющееся линейным преобразованием векторного пространства V_1 в векторное пространство V_2; c — постоянная величина ($c \in F$).

О таких системах говорят, что они подчиняются обобщенному принципу суперпозиции с входной $\overset{1}{+}$ и выходной $\overset{2}{+}$ операциями. Линейные системы являются частным случаем гомоморфных систем, для которого операции $\overset{1}{+}$ и $\overset{2}{+}$ совпадают и являются сложением, а операции $\overset{1}{\cdot}$ и $\overset{2}{\cdot}$ — умножением.

Для использования теории линейных векторных пространств необходимо, чтобы входные и выходные операции были ассоциативными, коммутативными и удовлетворяли аксиомам сложения и умножения на скаляр, принятых для векторных пространств.

Все системы, удовлетворяющие условиям (7.35) и (7.36), можно представить в виде каскадного соединения трех систем (рис. 31): D_1, D_2^{-1} и L. Система D_1 характеризуется свойством

$$D_1[x_1(n) \overset{1}{+} x_2(n)] = D_1[x_1(n)] + D_1[x_2(n)] = \hat{x}_1(n) + \hat{x}_2(n);$$

$$D_1[c \overset{1}{\cdot} x_1(n)] = cD_1[x_1(n)] = c\hat{x}_1(n).$$

Эта система подчиняется обобщенному принципу суперпозиции со входной операцией $\overset{1}{+}$ и выходной операцией $\overset{2}{+}$, являющейся обычной суммой. Комбинация сигналов, объединенных операцией $\overset{1}{+}$, преобразуется в обычную линейную комбинацию соответствующих сигналов $\hat{x}_1(n)$ и $\hat{x}_2(n)$. Система L является обычной линейной системой, удовлетворяющей условиям

$$L[\hat{x}_1(n) + \hat{x}_2(n)] = L[\hat{x}_1(n)] + L[\hat{x}_2(n)] = \hat{y}_1(n) + \hat{y}_2(n);$$

$$L[c \cdot \hat{x}_1(n)] = cL[\hat{x}_1(n)] = c\hat{y}_1(n).$$

Система D_2^{-1} преобразует сложение в операцию $\overset{2}{+}$ и удовлетворя-

ет следующим условиям:

$$D_2^{-1}[\hat{y}_1(n) + \hat{y}_2(n)] = D_2^{-1}[\hat{y}_1(n)]^2 + D_2^{-1}[\hat{y}_2(n)] = y_1(n)^2 + y_2(n);$$

$$D_2^{-1}[c\hat{y}_1(n)] = c^2 \cdot D_2^{-1}[\hat{y}_1(n)] = c^2 \cdot y_1(n).$$

Система D_1 называется характеристической системой для операции $\overset{1}{+}$. Тогда система D_2^{-1} является характеристической системой для операции $\overset{2}{+}$. Все гомоморфные системы с одинаковыми входными и выходными операциями отличаются друг от друга только линейной частью. Значит, после определения характеристических систем для рассматриваемого класса сигналов нелинейная фильтрация сводится к линейной. Например, если требуется выделить сигнал $x_1(n)$ из сигнала $x(n) = x_1(n) + x_2(n)$, то нужно выбрать линейную систему так, чтобы ее выходной сигнал $\hat{y}(n) = x_1(n)$. Тогда при $D_2 = D_1$ получим

$$y(n) = D_1^{-1}[\hat{x}_1(n)] = x_1(n),$$

где D_1^{-1} — система, действие которой обратно действию системы D_1. Чтобы полностью разделить сигналы $x_1(n)$ и $x_2(n)$, следует иметь возможность полностью разделить сигналы $\hat{x}_1(n)$ и $\hat{x}_2(n)$ с помощью линейного фильтра.

Так как для подавляющего большинства задач обработки сигналов пространства V_1 и V_2 совпадают, т. е. совпадают операции $\overset{1}{+}$ и $\overset{2}{+}$, $\overset{1}{\cdot}$ и $\overset{2}{\cdot}$, то на дальнейшее изложение накладывается еще одно ограничение, т. е. будем рассматривать только такие гомоморфные системы, которые определяются над одним и тем же векторным пространством $V = V_1 = V_2$. Наиболее известны гомоморфные системы [115], у которых операции $\overset{1}{+}$ и $\overset{1}{\cdot}$ являются умножением и возведением в степень (мультипликативные гомоморфные системы), сверткой и повторной сверткой сигнала с самим собой (гомоморфные системы относительно свертки). Рассмотрим, например, систему, гомоморфную относительно свертки. Пусть задан сигнал $x(n)$, представляющий собой свертку двух сигналов $x(n) = x_1(n) * x_2(n)$. На практике встречается очень много таких сигналов. Так, в технике связи или звукозаписи вносимые искажения можно трактовать как результат свертки шума с полезным сигналом; при обработке речевых сигналов можно считать, что сигнал возбуждения и импульсная характеристика свертываются в процессе формирования сигналов речи; при сложении независимых случайных процессов их функции плотности вероятности свертываются и т. п. [127].

Операция дискретной свертки удовлетворяет аксиомам векторного сложения и поэтому может служить основной операцией для класса гомоморфных систем. Умножение на целое число c соответствует повторной свертке сигнала $x(n)$ с собой c раз. Характеристическая

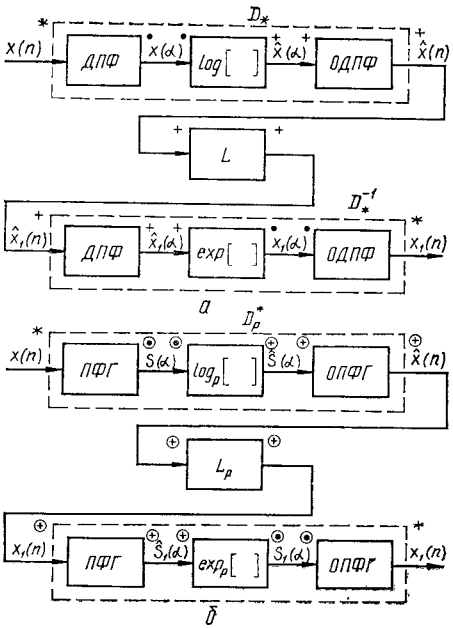


Рис. 33. Схема гомоморфной относительно свертки системы.

система D_* обладает свойством

$$D_*[x_1(n) * x_2(n)] = D_*[x_1(n)] + D_*[x_2(n)] = \hat{x}_1(n) + \hat{x}_2(n);$$

$$D_*[c \overset{*}{*} x_1(n)] = cD_*[x_1(n)] = c\hat{x}_1(n). \quad (7.37)$$

Знаком $\overset{*}{*}$ в выражении (7.37) обозначена операция повторной свертки.

Операция ортогонального преобразования, например ДПФ, может рассматриваться как гомоморфное преобразование, у которого входной операцией является свертка, а выходной — умножение (рис. 32). В общем случае вместо ортогонального преобразования выступает z-преобразование. Однако если входные последовательности являются минимально-фазовыми [133], то z-преобразование можно заменить ортогональным преобразованием. Далее, операцию умножения можно перевести в операцию суммы с помощью функции log [ ]. При использовании для построения гомоморфной относительно свертки системы ДПФ логарифмированию подвергается комплексный спектр. Поэтому необходимо использовать комплексную логарифмическую функцию. На рис. 33, *а* показана система, гомоморфная относительно свертки. Указаны операции, которые связывают входные, а также выходные данные каждой системы.

Заметим, что ДПФ и ОДПФ являются гомоморфными преобразованиями между векторными пространствами со сверткой и умножением в качестве основных операций и в то же время линейными преобразованиями в обычном смысле. Из рис. 33, *а* видно, что модель гомоморфной обработки сигналов содержит четыре последовательно выполняемых ортогональных преобразования. Это определяет основной объем вычислений при реализации данной модели, а также шум, обусловленный округлениями. Очевидно, что вследствие последовательного вычисления ДПФ и ОДПФ в несколько раз возрастают требования к точности вычисления этих преобразований даже при умеренных требованиях к точности вычисления $x_1(n)$. Если для достижения высокой точности вычислений ортогональных преобразований увеличивать разрядную сетку вычислительного устройства или переходить к форме представления чисел с плавающей запятой, то возрастают аппаратурные затраты на построение этого вычислительного устройства и снижается его быстродействие. При жестких

требованиях ко времени вычислений алгоритм приходится распараллеливать и реализовать параллельные вычисления одновременно, что еще больше увеличивает аппаратурные затраты. Поэтому до сих пор отсутствуют быстродействующие специализированные вычислительные устройства, реализующие модель, схематически представленную на рис. 33, *а*, в реальном времени. Такие модели реализуются с помощью производительных ЭВМ, осуществляющих вычисления не в реальном времени. Именно при построении таких систем представляются перспективными нахождение и реализация функциональных преобразований над конечным полем [206]. ДПФ заменяется на ПФГ, комплексный логарифм log [ ] и комплексная экспонента exp [ ] заменяются соответственно на аналогичные функциональные преобразования $\log_p$ [ ] и $\exp_p$ [ ], определенные над полем Галуа GF (p) (рис. 33, *б*). Линейная система L заменяется системой L_p, являющейся линейной системой по отношению к операции сложения по модулю p, обозначенной на рис. 33, *б* через $\oplus$. Реализация таких систем описана в работе [52].

Экономия аппаратурных затрат очевидна. Во-первых, уменьшаются аппаратурные затраты при реализации ПФГ вместо ДПФ, во-вторых, реализация функций $\log_p$ [ ] и $\exp_p$ [ ] проще по сравнению с реализацией комплексных логарифма и экспоненты. Кроме того, отсутствует шум округлений.

Список описываемых моделей цифровой обработки сигналов, определенных над конечными полями, можно было бы продолжить. Например, недавно доказана эффективность реализации над конечным полем цифровых фильтров с конечной импульсной характеристикой [199]. Однако основная цель этой главы — иллюстрация метода построения таких моделей и самое главное — изучение этого метода. Полное перечисление существующих моделей цифровой обработки сигналов, определенных над конечными полями, выходит за рамки этой работы.

* * *

Из изложенного материала можно сделать следующие выводы:

построение моделей, определенных над конечными кольцами и полями, является новым направлением в теории цифровой обработки сигналов. Тем не менее многие практически важные модели построены и реализованы и таким образом доказана их эффективность;

основным ограничивающим фактором при построении моделей, определенных над конечным полем или кольцом, является отсутствие привычного физического смысла результатов обработки в конечном поле (или в конечном кольце), что обусловливает ограничения на длину разрядной сетки вычислительного устройства. Иногда разрядная сетка должна быть недопустимо большой;

вывод об эффективности рассматриваемых моделей делался при предположении, что вычислительное устройство эффективно реализует операции конечных полей и колец. Поскольку микропрограммная реализация с помощью обычных ЦВМ хотя и дает выигрыш во времени вычислений при реализации моделей, определенных над

конечными полями и кольцами, но не позволяет полностью использовать преимущества этого подхода, задача изучения и разработки методов построения вычислительных устройств, позволяющих эффективную реализацию моделей, определенных над конечными полями или кольцами, является актуальной;

ввиду отсутствия обычного физического смысла результатов вычислений в конечном поле или кольце вполне возможно, что реализация некоторых моделей, определенных над этими алгебраическими системами, будет неэффективна или даже невозможна. Поэтому желательно, чтобы вычислительное устройство наряду с реализацией моделей, определенных над конечными полями или кольцами, позволяло реализацию обычных моделей.

ГЛАВА 8

АППАРАТУРНАЯ РЕАЛИЗАЦИЯ МОДЕЛЕЙ ЦОС

1. Особенности структуры и архитектуры аппаратных средств ЦОС

Цифровая обработка сигналов началась с моделирования на универсальной ЦВМ аналоговых систем обработки сигналов. Однако в процессе дальнейшего развития оказалось, что реализация моделей ЦОС с помощью универсальных ЦВМ далеко не всегда эффективна. Такие модели в основном реализуются с помощью специализированных вычислителей либо с помощью систем специализированных вычислителей. Процессоры общего назначения могут выполнять роль управляющего устройства для всей системы ЦОС [11, 101]. Обусловлено это высокими требованиями, предъявляемыми к быстродействию, а также к надежности, габаритам, потребляемой мощности, диктуемыми характером решаемых задач в области управления объектами и процессами в реальном времени, обработки радиолокационных, звуковых, сейсмических сигналов, сигналов изображений и др.

Конечно, программная реализация с помощью универсальной ЦВМ обладает большей гибкостью в плане использования различных моделей и алгоритмов. В некоторых случаях такая реализация дешевле разработки специализированного устройства. Попытка объединить положительные качества специализированных и универсальных вычислительных средств при решении задач ЦОС привела к появлению машин и устройств, ориентированных на обработку сигналов. Эта молодая отрасль вычислительной техники в последнее время бурно развивается в связи с появлением микропроцессоров и сверхбольших интегральных схем. Как правило, конкретная ЦВМ (вычислительное устройство, система), предназначенная для решения задач ЦОС, универсальна в рамках класса решаемых задач и специализирована в том смысле, что именно этот класс задач решается эффективно с помощью указанной ЦВМ.

В результате можно выделить класс цифровых аппаратных средств, предназначенных для ЦОС. Он подразделяется на ряд подклассов в зависимости от вида обрабатываемых сигналов (звуковые, геофизические, сейсмические и др.). Наиболее развитый в настоящее время подкласс составляют аппаратные средства, предназначенные для цифровой обработки изображений. Такие средства находят все более широкое применение и обладают характерными особенно-

стями (как и каждый подкласс систем ЦОС), отличающими их от средств обработки одномерных сигналов (см., например, [146, 183]). Однако здесь мы не будем касаться тонкостей в архитектуре и структуре систем ЦОС, диктуемых видом обрабатываемых сигналов. Рассмотрим общие черты, характерные для систем ЦОС.

В работе [11] выделяется пять основных факторов, влияющих на структуру ЦВМ и систем, предназначенных для ЦОС. К этим структурным факторам относятся: схемные компоненты; алгоритмы (математические модели ЦОС); данные; языки программирования; архитектурные компоненты машины.

Схемные компоненты полностью определяют конструкцию вычислительного устройства, быстродействие, потребляемую мощность, вид функциональных блоков. Эти факторы особенно важны в связи с быстрым развитием и совершенствованием технологии изготовления БИС и СБИС.

Появление быстродействующих транзисторно-транзисторных логических схем (ТТЛ) с диодами Шоттки и логических схем с эммитерными связями (ЭСЛ), а также БИС и СБИС ТТЛ и ЭСЛ, представляющих собой функционально законченные узлы, значительно увеличило возможности разработчиков. Появление многозначных БИС еще больше повысит технико-экономические показатели систем ЦОС в связи с уменьшением числа межсхемных соединений, увеличением быстродействия.

Тем не менее очевидно, что учет лишь схемных компонент не может привести к оптимальным решениям. Очень часто удачный выбор математической модели системы ЦОС, введение определенных архитектурных особенностей позволяют добиться одинаковых технико-экономических показателей при использовании дешевой менее быстродействующей элементной базы по сравнению с простым переходом на более быстродействующую элементную базу без оптимизации математической модели, архитектуры и структуры системы ЦОС.

Как отмечалось в первой главе, вид математической модели ЦОС существенным образом влияет на архитектуру и структуру системы ЦОС. При построении большинства моделей ЦОС применяются рекуррентные соотношения (при построении моделей цифровых фильтров [71, 134]) и обобщенные ортогональные преобразования. Известно, что произвольные рекурсивные фильтры могут быть описаны при помощи рекуррентного соотношения второго порядка

$$y(n) = Ay(n-1) + By(n-2) + Cx(n-2) + Dx(n-1) + x(n),$$

где коэффициенты A, B, C, D — действительные числа. Для эффективного вычисления по этому выражению устройство должно иметь возможность быстрого выполнения операции умножения. Достигается это параллельной аппаратурной реализацией (в виде комбинационной схемы) умножителя двух чисел либо параллельной аппаратурной реализацией функции вида $Y = ax + b$ [30, 69, 70, 171].

Вычисление ортогонального преобразования связано с выполнением операций умножения векторов и матриц. Эти операции могут выполняться с помощью одного или нескольких устройств, реализу-

ющих функцию $Y = a_n + x_n + b_n$, причем устройство построено таким образом, что возможно выполнение равенства $b_n = a_{n-1}x_{n-1}$ (умножитель с циклическим суммированием [31]). Возможна параллельная аппаратурная реализация операции умножения вектор-строки на вектор-столбец, характерная для векторных процессоров [55], или даже параллельная реализация операции умножения матрицы на вектор-столбец, характерная для матричных процессоров [55].

Другие функциональные преобразования встречаются реже. Для их реализации системы ЦОС снабжают универсальным функциональным преобразователем, реализующим произвольную функцию одной переменной [30, 40]: $y = f(x)$, где $x, y \in E_k$, $k = 2^4 \div 2^{12}$. Значения x и y кодируются двоичным кодом. Практическая реализация такого функционального преобразователя осуществляется с помощью ОЗУ. Входная переменная x подается на входы адреса, выходная переменная считывается с выходов данных, которые записываются предварительно в соответствии с выполняемой функцией. Такие функциональные преобразователи являются практически обязательной частью систем цифровой обработки изображений.

Возможности интегральной технологии позволяют выполнить процессор ЦОС в виде одной СБИС (или БИС). Иногда такая СБИС включает в себя АЦП и ЦАП [17, 49, 125]. Такие процессоры можно использовать непосредственно для обработки аналоговых сигналов.

Для эффективной реализации математических моделей ЦОС, определенных над конечными полями или кольцами, необходимо, чтобы вычислительное устройство могло эффективно реализовать арифметические операции указанных алгебраических систем. Указанное требование является единственным, так как вид аппаратно реализуемых функций в этом устройстве может быть таким же, как и при реализации обычных моделей, определенных над полем комплексных чисел (функция $Y = ax + b$, матричные и векторные операции и т. д.).

Действительно, с точки зрения конфигурации устройства, реализующего заданные алгебраические выражения (математическую модель), безразлично, над каким полем определено это алгебраическое выражение. Изменяется только внутренняя структура блоков устройства. Например, пусть некоторое устройство имеет структурную схему, показанную на рис. 34. АЛУ реализует операции в поле рациональных чисел. Обмен данными осуществляется интерфейсом, управление — управляющим автоматом (УА). С помощью АЛУ реализуется класс моделей, для построения которых используются полиномиальные и ортогональные преобразования. Допустим, что необходимо реализовать математические модели, для построения которых тоже используются полиномиальные и ортогональные преобразования, но определенные над конечным полем Галуа GF (p). Это можно осуществить, не меняя архитектуру устройства, структурная схема которого показана на рис. 34. Необходимо только заменить блоки (либо расширить их функциональные возможности). В этом случае устройство сможет реализовать модели, определенные над

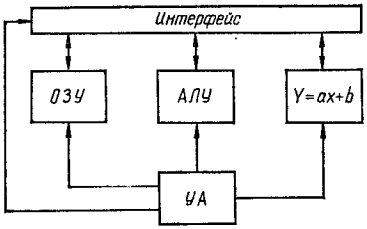


Рис. 34. Структурная схема устройства для ЦОС.

полем рациональных чисел, и модели, определенные над полем GF (p). АЛУ и функциональный преобразователь $Y = ax + b$ должны проводить вычисления в поле GF (p). Соответственно изменяется разрядность ОЗУ и интерфейса в связи с возможным несовпадением длины разрядной сетки, представляющей элементы поля GF (p) и длины разрядной сетки, используемой для представления рациональных чисел.

Рассмотрим влияние структур данных на конструкцию систем и устройств, предназначенных для ЦОС. Длина слова в большинстве случаев находится в пределах 12—18 разрядов. Числа представляются в дополнительном коде с фиксированной запятой. Иногда для повышения точности вычислений применяется поблочно плавающая и реже — плавающая запятая. Представление с плавающей запятой требует значительно большего объема аппаратуры и используется только в тех случаях, когда требуется высокая точность вычислений. Характерная черта систем ЦОС — разделение памяти. Применяется отдельная память для команд и для данных. Очень часто длина командного слова больше длины слова данных. Доступ к памяти команд может быть совмещен во времени с доступом к памяти данных.

Особое место занимает разработка языка высокого уровня, предназначенного для обработки сигналов. В настоящее время общепринятого языка нет. Как правило, составление программ алгоритмов обработки сигналов проводится на языке ассемблера, что обеспечивает высокую эффективность программ в плане быстродействия вычислений. Задача разработки языка высокого уровня для обработки сигналов еще больше усложнилась, но не потеряла актуальности в связи с появлением векторных и матричных процессоров. Языки высокого уровня полезны во многих случаях (например, когда быстрая разработка и запуск алгоритма важнее, чем быстродействие вычислений [11]; последнее особо важно при научных исследованиях).

Исходя из рассмотренных выше четырех структурных факторов, можно сформулировать основные архитектурные особенности, присущие ЦВМ и системам, предназначенным для ЦОС. Учет этих особенностей окончательно определяет структуру указанных аппаратных средств [11]:

использование параллелизма, причем распараллеливание проводится как на уровне алгоритмов, так и на аппаратном уровне;

применение специализированной памяти отдельно для хранения данных и для хранения команд;

использование специализированных арифметических устройств. В процессоре применяются арифметические расширители, которые аппаратно реализуют трудновычислимые арифметические функции. В качестве примера таких расширителей могут служить устройства, реализующие функции вида $Y = ax + b$; универсальный функцио-

нальный преобразователь; иногда более сложные устройства типа вычислителя степенного полинома [32];

применение многопроцессорных систем. Поскольку способы повышения производительности однопроцессорных систем исчерпаны [67], основным методом дальнейшего увеличения производительности вычислительных систем является использование нескольких процессоров (коллектива вычислителей [64]). При этом возможны различные подходы. Основными из них являются подход, базируемый на применении общей памяти, общего устройства управления и нескольких арифметических устройств (такой подход используется при построении векторных и матричных процессоров), а также подход, основанный на использовании нескольких самостоятельных вычислений, объединенных в коллектив с помощью специальной управляющей ЦВМ [43, 55, 64, 105, 121];

использование параллельных комбинационных схем вместо последовательных. Аппаратурная реализация функциональных преобразователей и арифметических устройств осуществляется в виде параллельных комбинационных схем. При этом за счет увеличения аппаратурных затрат значительно увеличивается быстродействие схем;

использование классических ЦВМ и процессоров для управления системой ЦОС. Специализированные устройства, предназначенные для ЦОС, часто соединяют с управляющей ЦВМ, которая имеет большую память, развитое программное обеспечение и набор стандартных устройств ввода — вывода. Устройства для ЦОС можно рассматривать как блок основной ЦВМ, выполняющий специальные функции. Функции этого блока могут изменяться программным управлением.

Теперь можно сформулировать еще одну особенность, связанную с реализацией математических моделей, определенных над конечным полем или кольцом, и вытекающего отсюда требования эффективной реализации арифметических операций конечного поля или кольца.

Арифметическое устройство должно одинаково эффективно реализовать как операции конечного поля или кольца, так и обычные арифметические операции. Это обусловлено тем, что пока мы не можем утверждать, что для всех задач ЦОС возможно построение математической модели, определенной над конечным полем или кольцом. Такой подход дает возможность реализовать как обычные математические модели, определенные над полем комплексных чисел, так и модели, определенные над конечными алгебраическими системами. Появляются дополнительные требования к блокам интерфейс и памяти. Эти устройства должны позволять передачу и запоминание кодовых слов, представляющих обычные числа и элементы конечного поля или кольца, что достигается выбором соответствующей длины кодового слова. Изменения, которым подвергаются арифметические блоки, более сложны. Поэтому рассмотрим данный вопрос более подробно.

Арифметические операции конечных алгебраических систем базируются на операциях суммы и умножения по модулю некоторого целого числа M, т. е. на арифметических операциях конечного кольца

вычетов по модулю M или поля Галуа GF (p) при простом M ($M = p$). Следовательно, сумматор (умножитель) должен осуществлять обычное суммирование (умножение) и модульное суммирование (умножение). Реализация модульных и обычных арифметических операций может быть совмещена в одном устройстве. Последнее базируется на том факте, что результат суммы (умножения) чисел a и b по модулю M, не превышающий значения модуля M, совпадает с результатом обычной суммы (умножения). Например, $9 \cdot 8 = 72$ при обычном умножении и $9 \cdot 8 = 72 = 127$, так как $72 < 127$. Значит, с помощью модульного арифметического устройства можно реализовать обычные арифметические операции. Необходимо только ограничивать диапазон изменения входных данных. Можно, наоборот, в обычных арифметических устройствах предусмотреть специальные корректирующие схемы, с помощью которых результат сложения (умножения) будет приводиться по модулю M.

Вопросы построения обычных арифметических устройств рассмотрены достаточно подробно (см. например, [69, 134, 171]). Однако проблема аппаратурной реализации арифметических операций конечных полей и колец еще окончательно не решена.

2. Модульные операции

Реализация арифметических операций конечного поля Галуа GF (p), конечного поля комплексных целых чисел Z_p^c, конечных колец Z_M, Z_p^H, Z_p^k сводится к реализации модульных операций, т. е. операций сложения и умножения, выполняемых по модулю некоторого простого (иногда составного) числа. То же самое можно сказать о реализации операций расширенного поля Галуа GF (p^v), элементами которого являются многочлены, определенные над простым полем GF (p). Поэтому в основе арифметического устройства, выполняющего операции над этими многочленами, лежит устройство, выполняющее операции сложения и умножения по модулю p. Следовательно, эффективная реализация модульных операций определяет эффективность реализации системы ЦОС в целом.

По-видимому, впервые с проблемой аппаратурной реализации модульных операций столкнулись при построении ЦВМ, работающей в системе остаточных классов. В [7] определены два основных метода реализации модульных операций: метод табличной арифметики и метод дополнительных связей переносов.

Метод табличной арифметики основан на табличной реализации модульных операций. Цифры в таблице сложения и умножения по модулю M записываются в двоичной системе счисления (либо в k-значной системе). Далее составляются таблицы истинности для цифр каждого разряда двоичных (k-значных) эквивалентов M-значных чисел, присутствующих в таблице, и проводится синтез соответствующих устройств.

Пример 8.1. Таблице сложения по модулю 3 (см. табл. 2 при $m = 3$) соответствует табл. 35, в которой вместо чисел 0, 1, 2 записа-

Таблица 35. Сложение по модулю 3

x_1	x_2		
	00	01	10
00	00	01	10
01	01	10	00
10	10	00	01

Таблица 36. Таблица истинности для цифр первого разряда значений из табл. 35

x_1	x_2		
	00	01	10
00	0	1	0
01	1	0	0
10	0	0	1

Таблица 37. Таблица истинности для цифр второго разряда значений из табл. 35

x_1	x_2		
	00	01	10
00	0	0	1
01	0	1	0
10	1	0	0

ны их двоичные эквиваленты. Из этой таблицы получаются две таблицы истинности для цифр первого разряда чисел табл. 35 (табл. 36) и цифр второго разряда этих чисел (табл. 37). Далее производятся оптимальное доопределение и минимизация функций алгебры логики, заданных в табл. 36 и 37. После этого указанные функции реализуются с помощью двоичных компонент (логические элементы, реализующие операции любого из функционально полных логических базисов [19]). Функции, подобные заданным в табл. 35 и 36, как правило, плохо минимизируются [7]. Поэтому реализация всех разрядов модульного сумматора по сравнению с реализацией обыкновенного двоичного сумматора, суммирующего числа с таким же числом разрядов, оказывается более громоздкой. Это относится и к модульным умножителям. Однако появление ППЗУ обусловило возможность эффективной реализации модульных операций с помощью метода табличной арифметики. Единственный недостаток этого метода — значительные аппаратурные затраты при реализации таблиц истинности, множество изменения переменных в которых превосходит множество изменения переменных ППЗУ. Это означает, что при больших значениях модуля M аппаратурная реализация модульных операций становится проблематичной. Последнее является ограничивающим фактором в использовании метода табличной арифметики при реализации модульных операций конечных колец, используемых в ЦОС. Однако следует заметить, что развитие интегральной схемотехники и появление ППЗУ большей емкости в некоторой степени компенсируют указанный ограничивающий фактор. Но современные ППЗУ не позволяют эффективно реализовать арифметические операции по модулю M при $M > 2^{12}$. Поэтому основным методом реализации модульных операций является метод дополнительных связей переносов, который заключается во введении дополнительных переносов между разрядами сумматора с целью достижения заданной величины модуля M, отличной от величины модуля сумматора без дополнительных переносов, равной 2^n, где n — число разрядов

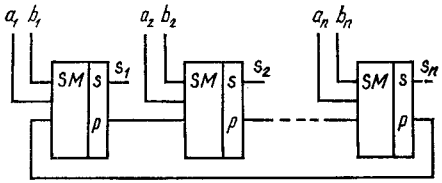


Рис. 35. Схема сумматора по модулю $M = 2^n \pm 1$.

сумматора. При этом наименьшее число дополнительных переносов для двоичного n-разрядного сумматора (всего один дополнительный перенос из старшего разряда в младший) получается при выборе значения M, равного 2 ± 1.

На рис. 35 показана схема сумматора n-разрядных чисел $A = a_1a_2...a_n$ и $B = b_1b_2...b_n$ по модулю $M = 2^n \pm 1$. Если суммирование проводится по модулю $M = 2^n - 1$, то значение переноса из старшего разряда суммируется со значением младшего разряда суммы, если суммирование проводится по модулю $M = 2^n + 1$, то значение переноса из старшего разряда вычитается из младшего разряда суммы. Поскольку при суммировании чисел по модулю $M = 2^n + 1$ приходится вычитать значение переноса, реализация операции суммы по этому модулю оказывается сложнее по сравнению с реализацией операции суммы по модулю $M = 2^n - 1$. Фактически сумматор n-разрядных чисел по модулю $M = 2^n + 1$ должен состоять из полных одноразрядных сумматоров — вычитателей, в то время как сумматор n-разрядных чисел по модулю $M = 2^n - 1$ состоит из более простых элементарных звеньев — полных одноразрядных сумматоров. Поэтому арифметика по модулю $M = 2^n - 1$ более предпочтительна, чем арифметика по модулю $M = 2^n + 1$. Однако выбор кольца вычетов по модулю $M = 2^n + 1$ обусловлен получаемыми звеньями объемов ТЧП, определенных над таким кольцом и равных степени 2. В этом случае при вычислении ТЧП можно использовать известные быстрые алгоритмы, основанные на прореживании по частоте или по времени [12, 13, 115, 120, 124, 134]. Известны также методы упрощения этой арифметики [95]. Аппаратурная реализация ТЧП, определенных над кольцом вычетов по модулю $M = 2^n + 1$, может упрощаться за счет выбора первообразного элемента, равного 2 или степени 2. При этом операции умножения заменяются операциями сдвига [98, 202]. Это касается ТЧП, определенных над кольцом вычетов по модулю любого вида. В общем случае при построении процессора ЦОС, ориентированного не только на реализацию ТЧП, необходимо реализовать операцию модульного умножения.

Умножитель n-разрядных чисел по модулю $M^n = 2^n + 1$ может быть построен на основе сумматора, показанного на рис. 36. Однако в прямом виде использование модульного сумматора неэффективно из-за наличия циклического переноса, который ухудшает быстродействие схемы. Учет циклического переноса лучше осуществлять в последующем такте вычислений (см. рис. 36). Перенос, возникающий при суммировании двух слов частичных произведений $A = a_1a_2...a_n$ и $B = b_1b_2...b_n$, подается на младший разряд сумматора, осуществляющего суммирование последующего слова частичных произведений $C = c_1c_2...c_n$ и результата суммы слов A и B.

Окончательная коррекция суммы, связанная с циклическим переносом, проводится на дополнительном $(n+1)$-м шаге вычислений. Точно так же можно учитывать циклический перенос при последовательном вычислении произведения.

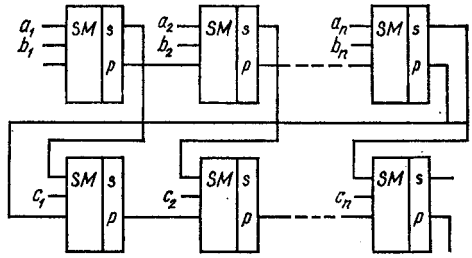


Рис. 36. Схема матрицы сумматоров.

Пример 8.2. Приведем укрупненную блок-схему матричного умножителя трехразрядных двоичных чисел по модулю $M = 2^3 - 1$. В матричном умножителе операция умножения реализуется аппаратурным, а не микропрограммным путем [69, 70, 149, 171]. Произведение двух трехразрядных чисел можно записать следующим образом:

$$\begin{array}{cccccc} & & a_1 & a_2 & a_3 & \\ & & b_1 & b_2 & b_3 & \\ \hline & & a_1b_3 & a_2b_3 & a_3b_3 & \\ & a_1b_2 & a_2b_2 & a_3b_2 & & \\ a_1b_1 & a_2b_1 & a_3b_1 & & & \\ \hline Q_6 & Q_5 & Q_4 & Q_3 & Q_2 & Q_1. \end{array}$$

Каждое слово частичных произведений необходимо привести по модулю $M = 2^3 - 1$. Для этого разряды с весом, большим 2^2, нужно сложить с младшими разрядами. Тогда

$$\begin{array}{ccccc} a_1 & a_2 & a_3 & & \\ b_1 & b_2 & b_3 & & \\ \hline a_1b_3 & a_2b_3 & a_3b_3 & & \\ a_2b_2 & a_3b_2 & a_1b_2 & & \\ a_3b_1 & a_1b_1 & a_2b_1 & & \\ \hline Q_5 & Q_4 & Q_3 & Q_2 & Q_1. \end{array}$$

Примерная блок-схема матрицы сумматоров умножителя показана на рис. 37. Окончательная коррекция результата суммы частичных произведений осуществляется с помощью сумматора *SM3*. Только у этого сумматора есть циклический перенос. Полная блок-схема состоит из формирователя частичных произведений и матрицы сумматоров.

Из примера 8.2 видно, что по сравнению с обычным умножителем [134, 171] трехразрядных двоичных чисел модульный умножитель дополнительно содержит сумматор *SM3*. В процентном отношении — это небольшое увеличение затрат оборудования. К тому же при увеличении разрядности входных слов процент увеличения затрат оборудования снижается.

Модульный умножитель n-разрядных чисел можно использовать для обычного умножения $n/2$-разрядных чисел. Легко убедиться

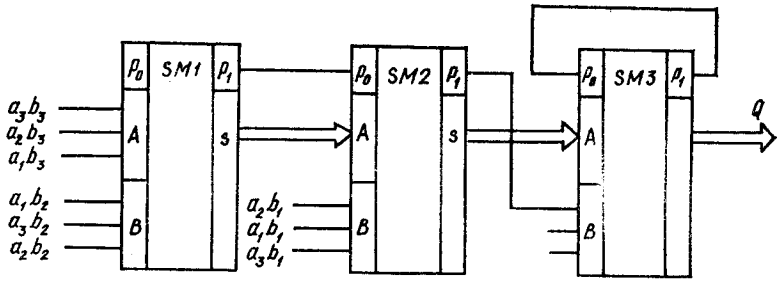


Рис. 37. Схема матрицы сумматоров умножителя чисел по модулю $M = 2^3 - 1$.

что при таком ограничении результат модульного умножения совпадает с результатом обычного умножения.

Упражнение 8.1. Построить блок-схему умножителя чисел по модулю $M = 2^4 + 1$. Операцию вычитания циклического переноса заменить операцией суммы соответствующего дополнительного кода. Оценить сложность полученной схемы и сравнить ее со схемой, рассматриваемой в примере 8.2.

Основной недостаток рассмотренного модульного сумматора — необходимость организации циклического переноса из старшего в младший разряд. Наличие такого переноса усложняет также построение матричного умножителя, но принципиально необходимо. Действительно, модуль M должен быть числом нечетным. В двоичной системе счисления только вес самого младшего разряда выражается нечетным числом, равным единице. Вес других разрядов имеет значения, выражающиеся четными числами. Модуль обычного двоичного n-разрядного сумматора равен 2^n. Уменьшение или увеличение его до некоторого нечетного числа в любом случае потребует вычитания или прибавления единицы. При этом могут быть связи переносов между другими разрядами. Мы уже видели, что наличие даже одного дополнительного переноса ощутимо ухудшает показатели арифметических устройств по быстродействию и аппаратурным затратам. Наличие многих переносов хотя и позволяет реализовать сумматор по произвольному модулю, но настолько усложняет сам сумматор, что практическое введение более двух-трех дополнительных переносов представляется бесперспективным.

Упражнение 8.2. Разработать схему сумматоров по модулю $M = 39$, $M = 29$, пользуясь методом дополнительных переносов.

Другим недостатком арифметики по модулю $M = 2^n \pm 1$ является то, что в ряде чисел $M = 2^n + 1$, $n = 0, 1, 2, \ldots$, только пять чисел Ферма $F_t = 2^{2^t} + 1$, $t = 0, 1, 2, 3, 4$, являются простыми. Остальные числа Ферма по-видимому составные [178]. Числа вида $M = 2^n - 1$ простые только при n простом. В общем случае количество простых чисел вида $M = 2^n \pm 1$ невелико (табл. 38). Эти простые числа не всегда удовлетворяют проектировщика модульных арифметических устройств, предназначенных для задач ЦОС.

Очевидно, что переходом к системе счисления, используемой при

Таблица 38. **Разложение чисел $2^n \pm 1$ на простые множители**

n	$2^n - 1$	$2^n + 1$
2	3	5
3	7	3^2
4	$3 \cdot 5$	17
5	31	$3 \cdot 11$
6	$3^2 \cdot 7$	$5 \cdot 13$
7	127	$3 \cdot 43$
8	$3 \cdot 5 \cdot 17$	257
9	$7 \cdot 73$	$3^3 \cdot 19$
10	$3 \cdot 11 \cdot 31$	$5^2 \cdot 41$
11	$23 \cdot 89$	$3 \cdot 683$
12	$3^2 \cdot 5 \cdot 7 \cdot 13$	$17 \cdot 241$
13	8191	$3 \cdot 2731$
14	$3 \cdot 43 \cdot 127$	$5 \cdot 29 \cdot 113$
15	$7 \cdot 31 \cdot 151$	$3^2 \cdot 11 \cdot 331$
16	$3 \cdot 5 \cdot 17 \cdot 257$	65 537
17	131 071	$3 \cdot 43\,691$
18	$3^3 \cdot 7 \cdot 19 \cdot 73$	$5 \cdot 13 \cdot 37 \cdot 109$
19	524 287	$3 \cdot 174\,763$
20	$5 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41$	$17 \cdot 61\,681$
21	$7^2 \cdot 127 \cdot 337$	$3^2 \cdot 43 \cdot 5419$
22	$3 \cdot 23 \cdot 89 \cdot 683$	$5 \cdot 397 \cdot 2113$
23	$47 \cdot 178\,481$	$3 \cdot 2\,796\,203$
24	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$	$97 \cdot 257 \cdot 673$
25	$31 \cdot 601 \cdot 1801$	$3 \cdot 11 \cdot 251 \cdot 4051$
26	$3 \cdot 2731 \cdot 8191$	$5 \cdot 53 \cdot 157 \cdot 1613$
27	$7 \cdot 73 \cdot 262\,657$	$34 \cdot 19 \cdot 87\,211$
28	$3 \cdot 5 \cdot 29 \cdot 43 \cdot 113 \cdot 127$	$17 \cdot 15\,790\,321$
29	$233 \cdot 1103 \cdot 2089$	$3 \cdot 59 \cdot 3\,033\,169$
30	$3^2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$	$5 \cdot 13 \cdot 41 \cdot 61 \cdot 1321$
31	2 147 483 647	$3 \cdot 715\,827\,883$
32	$3 \cdot 5 \cdot 17 \cdot 257 \cdot 65\,537$	$641 \cdot 6\,700\,417$
33	$7 \cdot 23 \cdot 89 \cdot 599\,479$	$3^2 \cdot 67 \cdot 683 \cdot 20\,857$
34	$3 \cdot 43\,691 \cdot 131\,071$	$5 \cdot 137 \cdot 953 \cdot 26\,317$
35	$31 \cdot 71 \cdot 127 \cdot 122\,921$	$3 \cdot 11 \cdot 43 \cdot 281 \cdot 86\,171$
36	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 19 \cdot 37 \cdot 73 \cdot 109$	$17 \cdot 241 \cdot 433 \cdot 38\,737$
37	$223 \cdot 616\,318\,177$	$3 \cdot 241 \cdot 433 \cdot 38\,737$
38	$3 \cdot 174\,763 \cdot 524\,287$	$5 \cdot 229 \cdot 457 \cdot 525\,313$
39	$7 \cdot 79 \cdot 8191 \cdot 121\,369$	$3^2 \cdot 2731 \cdot 22\,366\,891$
40	$3 \cdot 5^2 \cdot 11 \cdot 17 \cdot 31 \cdot 41 \cdot 61\,681$	$257 \cdot 4\,278\,255\,361$
41	$13\,367 \cdot 164\,511\,353$	$3 \cdot 83 \cdot 8\,831\,418\,697$
42	$3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419$	$5 \cdot 13 \cdot 29 \cdot 113 \cdot 1429 \cdot 14\,449$
43	$431 \cdot 9719 \cdot 2\,099\,863$	$3 \cdot 2\,932\,031\,007\,403$
44	$3 \cdot 5 \cdot 23 \cdot 89 \cdot 397 \cdot 683 \cdot 2113$	$17 \cdot 353 \cdot 2\,931\,542\,417$
45	$7 \cdot 31 \cdot 73 \cdot 151 \cdot 631 \cdot 23\,311$	$3^2 \cdot 11 \cdot 19 \cdot 331 \cdot 18\,837\,001$
46	$3 \cdot 47 \cdot 178\,481 \cdot 2\,796\,203$	$5 \cdot 277 \cdot 1013 \cdot 1657 \cdot 30\,269$
47	$2351 \cdot 4513 \cdot 13\,264\,529$	$3 \cdot 283 \cdot 165\,768\,537\,521$
48	$3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 97 \cdot 241 \cdot 257 \cdot 673$	$193 \cdot 65\,537 \cdot 22\,253\,377$

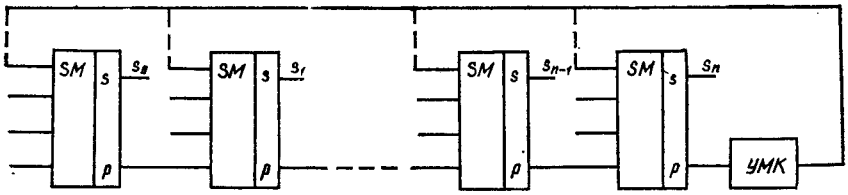


Рис. 38. Схема k-значного модульного сумматора.

кодировании элементов конечных колец с основанием, большим 2, можно значительно улучшить параметры модульного сумматора (а значит, и умножителя). Действительно, выбрав нечетное значение основания системы счисления, исключим необходимость дополнительного переноса из старшего в младший разряд, так как модуль M можно подобрать таким образом, что этот перенос будет заводиться в другой разряд и длина цепочки переноса будет меньше.

Естественно, что основание k системы счисления, используемой для кодирования элементов конечного кольца, можно выбрать равным модулю M, т. е. $k = M$. В этом случае построение устройств, реализующих модульные операции, становится тривиальным, так как для их построения необходим полный одноразрядный сумматор k-значных чисел и умножитель k-значных одноразрядных чисел. Однако возможности технологии интегральных многозначных структур [139] делают этот вариант приемлемым только при $k = 4 \div 8$. Поэтому и при реализации модульных операций с помощью многозначной элементной базы проблема остается той же, что и при реализации их с помощью двоичной элементной базы. А именно: необходимо осуществлять реализацию модульных операций с помощью вычислительных устройств и их элементов, работающих в системе счисления с основанием, равным k, при условии, что модуль M отличен от k и kM.

По аналогии с двоичной арифметикой наиболее удобными для реализации будут следующие значения модуля M для четных и нечетных k соответственно:

$$M = k^n \pm \nu; \tag{8.1}$$

$$M = k^n \pm k^r\nu, \tag{8.2}$$

где $\nu = 0, 1, \ldots, k-1$; $r = 0, 1, \ldots, n-1$. Если $k^r = 1$, то сумматор будет содержать циклический перенос из старшего в младший разряд (рис. 38). При других значениях k^r ($k^r \neq 0$) перенос будет заводиться в r-й разряд. При вычислениях по модулю $M = k + k^r\nu$ значение переноса вычитается из r-го разряда; при вычислениях по модулю $M = k^n - k^r\nu$ значение переноса необходимо сложить с r-м разрядом суммы. Если $\nu = 2, 3, \ldots, k-1$, то значение переноса из старшего разряда умножается на ν с помощью умножителя на константу *УМК* (см. рис. 38). В принципе, выражение для модуля сумматора при изменении ν_i в пределах от 0 до $k-1$ может быть следующим:

$$M = k^n + \nu_1 k^{n-1} \pm \nu_2 k^{n-2} \pm \cdots \pm \nu_{n-1} k^0. \tag{8.3}$$

Отрицательным фактом является то, что при $\nu_{n-1} = 0$ основание k системы счисления делит модуль M. Следовательно, объем ТЧП не может превышать k ($N \leqslant k$). Основание k не делит модуль M только в том случае, если $\nu_{n-1} \neq 0$, т. е. при наличии циклического переноса из старшего в младший разряд. Однако даже при значениях основания k, равных 4—8 (допустимых, исходя из условий технологии изготовления интегральных схем), организация модульного сумматора с минимальной длиной циклического переноса может использоваться в системах цифровой обработки изображений. Обработка изображений, как правило, проводится пофрагментно (по частям). Размеры фрагмента цифрового изображения находятся в пределах от 3 · 3 до 16 · 16 точек. Двухмерное ТЧП разделяется на последовательно выполняемые по строкам и по столбцам два одномерных. Объем одномерного ТЧП в этом случае находится в пределах от 3 до 16, т. е. $N = 3 \div 16$.

Другим преимуществом k-значных систем счисления по сравнению с двоичными является увеличение с возрастанием k диапазона возможных реализуемых модулей при одной и той же схеме дополнительных переносов. Например, пусть модуль, реализуемый сумматором, выражается в виде (8.2). При $k = 2$ это выражение позволяет получить три различных модуля $M_1 = 2^n - 1$, $M_2 = 2^n$, $M_3 = 2^n + 1$; при $k = 3$ число различных модулей равно 5. В общем случае при произвольном k число различных модулей равно $2k - 1$. Ясно, что чем шире диапазон различных модулей, тем больше простых чисел может быть представлено в виде (8.2).

Упражнение 8.3. Составить таблицу простых чисел, не превышающих 2^{16}, каждое из которых можно представить в виде $M = k^n - 1$ при k, равном 3, 4, 5. В связи с этим переход от двоичной к k-значной элементной базе можно рассматривать как путь повышения эффективности реализации модульных операций. Как видно, решается принципиальная проблема: облегчается реализация операций по модулю, отличающемуся от степени числа, выражающего величину основания системы счисления k. Впервые многозначная логика в целях реализации модульных операций была применена в устройствах, предназначенных для вычислений в системе остаточных классов [10].

Заметим, что переход от двоичной к многозначной элементной базе помимо указанных выше преимуществ, характерных для многозначных устройств, обусловливает еще уменьшение числа внешних выводов и межсхемных соединений, а также повышение быстродействия.

В первую очередь более подробно рассмотрим арифметику по модулю $M = 2^n - 1$. Пусть $M = 2^n - 1$, где n — составное число вида pq, где p — простое число. Тогда $2^p - 1$ делит нацело число $2^{pq} - 1$, а максимальное значение N определяется только числом $2^p - 1$. Поэтому наибольший интерес представляют только простые числа n. Числа вида $2^p - 1$, где p — простое, называются числами Мерсенна. ТЧП с использованием простых чисел Мерсенна были рассмотрены нами ранее. Но и составные числа вида $2^n - 1$ также пред-

ставляют практический интерес. Дело в том, что Z_{2^n-1}-арифметика является наиболее простой с точки зрения аппаратурной реализации, поскольку производить вычисления по модулю $2^n - 1$ в единой дополнительной арифметике сравнительно легко. Именно этот факт привлекает к себе внимание. Пусть r — какой-либо (обычно наименьший) множитель $2^n - 1$. Тогда $(2^n - 1)/r$-арифметика тоже проста в указанном выше смысле, так как в последнем случае все преобразования в арифметическом устройстве могут выполняться сначала в $2^n - 1$-арифметике, а уже в самом конце, когда необходимо получить искомую величину, результат вычисления берется по модулю $(2^n - 1)/r$. В табл. 38 приведены разложения чисел $2^n + 1$ на простые множители [58]. Из этой таблицы можно найти подходящие простые и составные числа вида $(2^n - 1)/r$. Эти числа необходимо выбирать, исходя из следующих соображений. Величина $N_{\max}$ определяется наименьшим из сомножителей. Поэтому естественно желание убрать все маленькие сомножители. Но до какой величины сомножитель можно считать маленьким? Если r — наименьший простой множитель, то $N_{\max}$ не может быть больше $r - 1$. Обычно практически используется $N_{\max} \geqslant 4 \div 6$. Поэтому все простые множители, меньшие 5—7, нужно считать маленькими. К такому же результату можно подойти и с другой стороны, а именно: мы не можем брать r слишком большим числом, так как при этом уменьшается модуль $(2^n - 1)/r$, а разрядность аппаратуры остается прежней. Если, скажем, $r = 64$, то $\log_2 = 64 = 6$, что говорит о том, что шесть разрядов аппаратуры фактически недоиспользованы и это есть плата за удобство пользования $2^n - 1$-арифметикой вместо $(2^n - 1)/r$-арифметики. Чем больше значение r, тем больше фактически недоиспользуемых разрядов. Поэтому вряд ли целесообразно брать $r > 64$. Обозначим $v = \lfloor \log_2 r \rfloor$, тогда необходимое число разрядов для представления чисел по модулю $M = (2^n - 1)/r$ равно $n - v$.

Другой простой арифметикой является Z_{2^n+1}-арифметика. Если n — нечетное, то $3 = 2^1 + 1$ делит $2^n + 1$, поэтому $N_{\max} = 2$. Значит, n должно быть четным числом. Пусть $n = s2^t$, где s — нечетное число. Тогда $2^{2^t} + 1$ делит $2^{s2^t} + 1$, и объем возможного преобразования определяется наибольшим объемом для кольца вычетов по модулю $M = 2^{2^t} + 1$. Таким образом, представляют интерес целые числа вида $2^{2^t} + 1$. Эти числа, как уже говорилось, являются числами Ферма $m = F_t = 2^{2^t} + 1 = 2^b + 1$, $b = 2^t$, а F_t называется t-м числом Ферма. Числа для t, равного 0, 1, 2, 3, 4, дают простые числа F_t, равные 3, 5, 17, 257, 65 537. Так как числа Ферма до F_4 простые, то НОД $(F_t - 1) = 2^b$. Следовательно, существуют ТЧПФ для $T = 2^m$ при $m < b < 2^t$ (см. четвертую главу).

В настоящее время известно, что F_t для t, равного 5, 6, 7, 8, 9, 11, 12, 15, 18, 23, 36, 38, 73, являются составными. Можно легко указать форму делителей составного F_t с помощью следующей теоремы.

Теорема 8.1. Для $t > 1$ каждый простой делитель числа $F_t = 2^{2^t} + 1$ имеет вид $p = k \cdot 2^{t+2} + 1$.

Доказательство. Если $p \mid F_t$, то $2^{2^t} \equiv -1 \pmod{p}$ и $2^{2^{t+1}} \equiv 1 \pmod{p}$. Поэтому число 2 принадлежит показателю 2^{t+1} по модулю $2^{2^t} + 1$, так что $p \equiv 1 \pmod{2^{t+1}}$. Таким образом, для $t > 1$, $p \equiv 1 \pmod 8$, так что $2^{(p-1)/2} \equiv 1 \pmod{p}$. Отсюда $(p-1)/2$ делится на 2^{t+1}, т. е. $p = k \cdot 2^{t+2} + 1$.

Возможные простые делители числа F_5 имеют вид $128k + 1$ и теперь легко найти делитель $641 = 5 \cdot 128 + 1$. Делители F_{73} имеют вид $N_k = k \cdot 2^{75} + 1$, $k = 1, 2, 3, 4$. Для k, равного 1, 2, 3, 4, число N_k делится на 3, 17, 5, 3 соответственно. Легко видеть, что F_{73} не делится на эти числа, так что первым делителем F_{73} может быть лишь N_5.

Последовательность чисел F_t всегда дает новые простые делители, так как F_t взаимно просто со всеми предшествующими F_s $(s < n)$. Это тотчас следует из соотношения $F_0F_1F_2 \ldots F_{n-1} = 2^{2^n} - 1 = F_n - 2$, которое выводится перемножением n тождеств $(2^{2^l} - 1)(2^{2^l} + 1) = 2^{2^{l+1}} - 1$ $(l = 0, 1, 2, \ldots, n-1)$.

Таким образом, теорема доказана. Из составных чисел Ферма наибольший практический интерес для задач ЦОС имеют первых два составных числа Ферма: F_5 $(b = 32)$ и F_6 $(b = 64)$. Из теоремы 8.1 следует, что каждый простой сомножитель F_t имеет вид $k \cdot 2^{t+2} + 1$. Поэтому 2^{t+2} делит $N_{\max}(F_t) = k \cdot 2^{t+2}$. Из этой же теоремы следует, что 2 принадлежит показателю 2^{t+1}, т. е. $N(2) = 2^{t+1}$, а значит, $N(\sqrt{2}) = 2^{t+2}$. Поэтому для любых чисел Ферма F_t $(t \geqslant 2)$ $N(\sqrt{2}) = 2^{t+2} = 4b$, а для F_5 и F_6 может быть показано, что $N_{\max}(F_t) = 2^{t+2}$. Элемент ε, имеющий порядок $4b$ в Z_{F_t} $(t \geqslant 2)$, $\varepsilon = \sqrt{2} = 2^{b/4}(2^{b/2} - 1)$. Любая нечетная степень $\sqrt{2}$ будет также иметь порядок 2^{t+2}.

Если $m = 2^{s2^t}$, где s — нечетное число, то в этом случае для $\varepsilon = 2^s$ имеем $N(2^s) = 2^{t+1}$. При выборе ε в виде $\varepsilon = \sqrt{2^s} = 2^{[(s-1)/2 + s2^{t-2}]} \times (2^{s2^{t-1}})$ получим $N = (\sqrt{2^s}) = 2^{t+2} = 4b$.

И наконец, составные числа вида $2^n + 1$ также представляют интерес, в силу того что из них можно получить числа вида $2_n + 1/k$, где k — делитель $2^n + 1$.

Рассмотренные выше модули имеют двухбитовые двоичные представления. Можно рассмотреть трехбитовые модули $m_1 = 2^{2q} - 2^q + 1$ и $m_2 = 2^m - 2^q + 1$. Для первого и второго модулей, если они простые, имеем следующие порядки для мультипликативных групп MG_{m_1}, MG_{m_2} и колец Z_{m_1}, Z_{m_2}:

$$[\mathrm{MG}_{m_1} : 1] = m_1 - 1 = 2^q(2^q - 1) = t;$$
$$[\mathrm{MG}_{m_2} : 1] = m_2 - 1 = 2^q(2^{m-q} - 1) = t.$$

Присутствие множителя 2^q в t говорит о том, что можно построить χ-преобразование на группе Z_N, где $N = 2^n$, $1 \leqslant n \leqslant q$.

Если $m_{1,2}$ не простое, то нужно знать его каноническое разложение на множители. Табл. 39 дает некоторое представление об этом для чисел $m_1 = 2^{2q} - 2^q + 1$. Отметим, что $(2^{3q} + 1) = (2^q + 1) \times$

Таблица 39. **Характеристики ТЧП по модулям $(2^{2q}+2^q+1)/d$**

q	$2^{2q}-2^q+1$	Сомножители числа $2^{2q}-2^q+1$	$N(2)$	$N\sqrt{(2)}$
8	$2^{16}-2^8+1$	97·673	48	96
9	$(2^{18}-2^9+1)/3$	3·87 211	54	—
10	$(2^{20}-2^{10}+1)/13$	13·61·1321	60	—
11	$(2^{22}-2^{11}+1)/3$	3·67·20 857	66	—
12	$2^{24}-2^{12}+1$	433·38 737	72	144
13	$(2^{26}-2^{13}+1)/3$	3·22·366 891	78	—
14	$(2^{28}-2^{14}+1)/13$	13·1429·14 449	84	—
15	$(2^{30}-2^{15}+1)/3\cdot 19$	3·19·18 837 001	90	—
16	$2^{32}-2^{16}+1$	22 253·377·193	96	192
18	$2^{36}-2^{18}+1$	246241·279 073	108	
20	$(2^{40}-2^{20}+1)/241$	241·4562 284 561	120	240
24	$2^{48}-2^{24}+1$	577·487 824 887 233	144	288
27	$(2^{54}-2^{27}+1)/3$	3·163·135 433·272 010 961	162	—

$\times (2^{2q}-2^q-1)$. Поэтому, зная разложение на множители чисел 2^q+1 (см. табл. 38), очень просто можно построить таблицу разложения чисел $2^{2q}-2^q+1$ на множители.

Рассмотрим кольцо Z_m с $m=2^{2q}-2^q+1$ и найдем в этом кольце период элементов $+2$ и -2.

Теорема 8.2 [188]. Пусть ± 2 имеет порядок $6q$ по модулю $m=2^{2q}-2^q+1$.

Теорема 8.3 [188]. Если q делится на 4, то $\sqrt{2}=2^{9q/4}-2^{3q/4}$ имеет порядок $12q$ по mod m.

Доказательство. $(\sqrt{2})^2=2^{9q/2}-2\cdot 2^{3q}+2^{3q/2}\equiv 2 \bmod m$:

$$
\begin{array}{l|l}
2^{9q/2}-2\cdot 2^{3q}+2^{3q/2} & 2^{2q}-2^q+1 \\
\underline{2^{5q/2}-2^{7q/2}+2^{5q/2}} & 2^{5q/2}+2^{3q/2} \\
2^{7q/2}-2\cdot 2^{3q}+2^{3q/2}-2^{5q/2} & \\
\underline{2^{7q/2}-2^{5q/2}+2^{3q/2}\cdot} & \\
-2\cdot 2^{3q}\equiv(-2)(-1)=2 \ mod\ m. &
\end{array}
$$

Если $\sqrt{2}$ имеет порядок n, то $n \mid 12q$; $(\sqrt{2})^{2n}\equiv 1$ означает, что $2^n=1$ и, следовательно, $6q \mid n$, так что n — четно; $(\sqrt{2})^n=2^{n/2}=1$, так что $6q \mid (n/2)$ или $12q \mid n$ и, следовательно, $n=12q$. Пусть m имеет каноническое разложение $m=p_1^{d_1}p_2^{d_2}\ldots p_n^{d_n}$. Теперь рассмотрим порядок элемента 2 по модулю каждой простой степени $p_i^{d_i}$ из разложения m. Так как

$$
\left.\begin{array}{l} 2^{6q}\equiv 1 \bmod m \\ 2^{3q}\equiv -1 \bmod m \end{array}\right\},\ \text{то}\ \left.\begin{array}{l} 2^{6q}\equiv 1 \bmod p_i^{d_i} \\ 2^{3q}\equiv -1 \bmod p_i^{d_i} \end{array}\right\}.
$$

Допустим, что $q = s \cdot 2^t$ и s — нечетно. Тогда если 2 имеет порядок n по mod $p_i^{d_i}$, то $n \mid 6q$ и $n \nmid 3q$. Так если $q = s \cdot 2^t$, то последние условия будут иметь следующий вид: $n \mid 3 \cdot s \cdot 2^{t+1}$ и $n \nmid 3s \times \times 2^t$, так что $n = 3^j r \cdot 2^{t+1}$, где $r \mid s$ и j равно 0 или 1. Остановимся на некоторых конкретных случаях.

Теорема 8.4 [188]. Если $m = 2^{2q} - 2^q - 1$, где $q = 2^t$ или $q = 3 \cdot 2^t$, $t > 0$, то 2 имеет порядок $6q$ по модулю каждой простой степени множителя m.

Доказательство. Пусть 2 имеет порядок n по mod p^d. Из сказанного выше следует, что $n = s^j r \cdot 2^{t+1}$, где $r \mid s$ и j равно 0 или 1.

1. В случае $s = 1$ $r = 1$ и n равно 2^{t+1} или $3 \cdot 2^{t+1}$. Предположим, что $n = 2^{t+1} = 2q$. Тогда $2^{2q} \equiv 1 \bmod p^d$. Но $2^{2q} \equiv 2^q - 1 \bmod m \equiv \equiv 2^q - 1 \bmod p^d$, так что $2^q - 1 \equiv 1 \pmod{p^d}$ или $2^q \equiv 2 \bmod p^d$, но так как p — нечетно, то $2^{q-1} \equiv 1 \pmod{p^d}$. Поскольку 2 имеет порядок $2q$, выражение $2q \mid q - 1$ приводит к противоречию. Таким образом, $n = 3 \cdot 2^{t+1} = 6q$.

2. В случае $s = 3$ возможными значениями n являются 2^{t+1}; $3 \cdot 2^{t+1}$ и $9 \cdot 2^{t+1}$. Значение $n = 3 \cdot 2^{t+1} = 2q$ можно исключить, так как это случай 1. Предположим, что $n = 2^{t+1}$. Тогда $2^{2q} = 2^{3 \cdot 2^{t+1}} \equiv \equiv 1 \bmod p^d$. Но $2^{2q} \equiv 2^q - 1 \pmod{p^d}$, поэтому вновь $2^{q-1} \equiv \equiv 1 \bmod p^d$, тогда $2^{t+1} \mid q - 1$, т. е. $2^{t+1} \mid 3 \cdot 2^t - 1$, что невозможно, если $t > 0$. Таким образом, $n = 9 \cdot 2^{t+1} = 6q$.

Следствие 1. Если q делится на 4, то $\sqrt{2} = 2^{9q/4} - 2^{3q/4}$ имеет порядок $12q$ по модулю каждого сомножителя m.

Доказательство. Отметим, что $(\sqrt{2})^{12q} = 1$ и $(\sqrt{2})^{6q} = = -1$, так что $n \mid 12q$, но $h \nmid 6q$ и таким образом $n = 3^j r \cdot 2^{t+2}$, где $r \mid s$ и j равно 0 или 1. Оставшаяся часть доказательства аналогична предыдущему доказательству.

Следствие 2. Над кольцом Z_m возможно ТЧП длиной $6q$ с $\varepsilon = 2$, а если q делится на 4, то длиной $12q$ с $\varepsilon = \sqrt{2}$.

Доказательство. Необходимо показать, что $6q$ и $12q$ обратимы по модулю m. Это справедливо, если ни 2, ни 3 не делят m. Так как m нечетно, то первое очевидно. Найдем значение m по модулю 3: $2^{2q} - 2^q + 1 = (-1)^{2q} - (-1)^q + 1 \equiv 1 \bmod 3$. Оно справедливо, так как q четно. Таким образом, 3 не делит m.

Теорема 8.5. Если $m = 2^{2q} - 2^q + 1$, где $q = s \cdot 2^t$, $t > 0$, s — простое, то 2 имеет порядок $6q$ или $6q/s$ по модулю каждой простой степени множителя p^d из m.

Доказательство. Пусть 2 имеет порядок n по mod p^d. Из предыдущего следует, что n равно 2^{t+1}, $s \cdot 2^{t+1}$, $3 \cdot 2^{t+1}$ или $3 \cdot s \cdot 2^{t+1}$, как и в случае 2 из теоремы 8.4. Случаи, когда $s \cdot 2^{t+1} = = 2q$ и $2^{t+1} = 2q$, невозможны. Поэтому $3 \cdot 2 \cdot 2^{t+1} = 6q \mid s$ и $3s \times \times 2^{t+1} = 2q$.

В табл. 39 приведены некоторые из полученных результатов. Для q, равного 8, 12, 16, 24, 32, применено следствие 2, и преобразования длин $6q$ и $12q$ имеют место при d, равном 2 и $\sqrt{2}$ соответственно. Остальные модули в таблице получаются с помощью деления 2^{2q} —

-2^q+1 на множители, по модулю которых 2 имеет порядок, меньший, чем $6q$. Отметим, что теорема 8.5 применима к дополнительным значениям q, равным 10, 11, 12, 14, 20.

Найдем теперь вид первообразного корня степени T из 1. Пусть s — некоторое положительное число. Тогда

$$[(\pm 2)^{s/2}]^2 = 2^s \bmod q; \tag{8.4}$$

$$[\pm 2^{(3q+s)/2}]^2 = 2^{3q+s} = 2^q \cdot 2^{2q} \cdot 2^s = 2^q(2^q-1)\cdot 2^s \equiv -2^s \bmod q. \tag{8.5}$$

Выражения (8.4) и (8.5) позволяют решить следующие два сравнения:

$$x^2 \equiv 2^s \bmod q; \quad x^2 \equiv -2^s \bmod q.$$

Их решения имеют вид $x \equiv \pm 2^{s/2} \bmod q$. Пусть теперь $\varepsilon = \sqrt[T]{1}$, где $T = 2^l$, $1 \leqslant l \leqslant n$. Тогда

$$\varepsilon^{T/2} = (\varepsilon^{T/4})^2 \equiv -1 \bmod q.$$

Поэтому

$$\varepsilon^{T/4} = (\varepsilon^{T/8})^2 \equiv \pm 2^{3n/2} \bmod q.$$

Комбинируя (8.4) и (8.5), имеем

$$\varepsilon^{T/8} = (\varepsilon^{T/16})^2 = \pm 2^{k\cdot 3n/4} \bmod q,$$

где k равно 1 или 3. Итерационно продолжая этот процесс, получаем

$$\varepsilon^{T/2i} = \pm 2^{k\cdot 3n/2^{i-1}} \bmod q,$$

где $2 \leqslant i \leqslant \alpha+1$, $k = 1, 3, \ldots, 2^{i-1}-1$. Поэтому $n = 2^\alpha \cdot \beta$, где β — нечетное число.

Рассмотрим еще одну арифметику, которая была предложена в работе [192], из которой приведем без доказательства ряд теорем.

Пусть $A_n = 3 \cdot 2^n + 1$ — последовательность чисел, получаемая при изменении $n \in Z$. По отношению к этой последовательности все простые числа делятся на два типа. К первому типу относятся числа, являющиеся делителями целых вида A_n, ко второму — не являющиеся такими делителями.

Теорема 8.6. Простое число q принадлежит к первому типу, если для некоторого k справедливо сравнение $-3 \equiv 2^k \bmod q$.

Теорема 8.7. Если $q = 17;\ 23 \pmod{24}$, то q принадлежит ко второму типу.

Теорема 8.8. Если $q = 13;\ 19 \pmod{24}$, то q принадлежит к первому типу для A_{2n+1}.

Теорема 8.9. Если q является простым делителем A_{2n+1}, то q равно 1; 5; 7 и 11 (mod 24).

Теорема 8.10. Если q — простой делитель A_{2n}, то $q \equiv 1 \bmod 6$.

Теорема 8.11. Если q принадлежит к первому типу чисел и n_0 — наименьшее целое, большее 0, такое, что $q \mid A_{n_0}$, то q является делителем A_n, если и только если $n = n_0 \bmod l$, где l — индекс числа 2 по модулю q.

Если $A_n = p$ — простое число и так как $\varphi(p) = 3 \cdot 2^n$, то порядок любого элемента мультипликативной группы кольца Z_p имеет вид $3^j \cdot 2^k$, где $0 \leqslant j \leqslant 1$ и $0 \leqslant k \leqslant n$.

Таблица 40. **Разложение чисел A_n на сомножители**

n	$3 \cdot 2^n + 1$	Сомножители	n	$3 \cdot 2^n + 1$	Сомножители
1	7	7	22	12 582 913	7·313·5443
2	13	13	23	25 165 825	5^2·1 006 633
3	25	5^2	24	50 331 649	61·825 109
4	49	7^2	25	100 663 297	7^3·269·1091
5	97	97	26	201 326 593	13·1567·9883
6	193	193	27	402 653 185	5·11·1399·5233
7	385	5·7·11	28	805 306 369	7·37·139·22 369
8	769	769	29	1 610 612 737	79·20 387 503
9	1537	29·53	30	3 221 225 473	3 221 225 473
10	3073	7·439	31	6 442 450 945	5·7·184 070 027
11	6145	5·1229	32	12 884 901 889	19·35 692 249
12	12 289	12 289	33	25 769 803 777	13 613·1 893 029
13	24 577	7·3511	34	51 539 607 553	7·181·406 784 459
14	49 153	13·19·199	35	103 079 215 155	5·823·25 059 622
15	98 305	5·19 661	36	206 158 430 209	206 158 430 209
16	196 609	7·28 087	37	412 316 860 417	7·11·29·59·3 129 611
17	393 217	11·35 747	38	824 633 720 833	13·829·1063·71 983
18	786 433	786 433	39	1 649 267 441 665	5·316 133·1 043 401
19	1 572 865	5·7·44 939	40	3 298 534 883 329	7·10 243·46 004 029
20	3 145 729	727·4327	41	6 597 069 776 657	6 597 069 776 657
21	6 291 457	347·18 131	42	13 194 139 533 313	103·12 809 844 207

Теорема 8.12. Если $p = 3 \cdot 2^n + 1$ — простое, то число 2 не является примитивным первообразным элементом, за исключением случая $p = 13$; $T(2)$ делит $3 \cdot 2^{n-1}$ во всех случаях, кроме $p = 17$; $T(2)$ не может быть кратным 3, если p делит некоторое число Ферма.

Теорема 8.13. Если $p = 3 \cdot 2^{2m} + 1$ — простое число, то $T_p(2)$ должно быть кратным 3.

Для примера в табл. 40 представлены числа A_n и их разложение на сомножители, а в табл. 41 — периоды первообразного элемента $\varepsilon = 2$ по модулю простых $p = A_n$.

Рассмотренные арифметики получаются при выборе модуля в виде некоторой функции $f(n)$ натурального аргумента $n \in Z$. Многие математики старались найти такую элементарную функцию $f(n)$, которая для всех $n \in Z$ давала бы различные простые числа. При помощи такой функции можно было бы вычислить большие простые числа, если только имеется возможность найти $f(n)$ для каждого n.

Эйлер в 1772 г. нашел сравнительно длинные последовательности простых чисел, пользуясь квадратичными функциями. Так, например, выражение $n^2 + n + 17$ при $n = 0, 1, 2, \ldots, 15$, а $n^2 + n + 41$ при $n = 0, 1, 2, \ldots, 40$ дают только простые числа [178]. Аналогичным свойством обладают многочлены $2n^2 + 29$ при $n = 0, 1, 2, \ldots, 28$, $n^2 + n + 41$ при $n = 0, 1, 2, \ldots, 39$, $n^2 - 79n + 1601$ при $n = 0, 1, 2, \ldots, 79$. Если поставить вопрос, для каких простых чисел A функция $f(n) = n^2 + n + A$ принимает простые значения при $0 \leqslant n \leqslant A - 2$, то легко можно найти малые значения A, равные

Таблица 41. **Периоды первообразного элемента $\varepsilon = 2$ по модулю простых $p = A_n$**

n	$3 \cdot 2^n + 1 = p$	N_p (2)
1	7	$3 = 3 \cdot 2^{n-1}$
2	13	$12 = 3 \cdot 2^{n-1}$
5	97	$48 = 3 \cdot 2^{n-1}$
6	193	$96 = 3 \cdot 2^{n-1}$
8	769	$384 = 3 \cdot 2^{n-1}$
12	12 289	$6144 = 3 \cdot 2^{n-1}$
18	786 433	$393\,216 = 3 \cdot 2^{n-1}$
30	3 221 225 473	$805\,306\,368 = 3 \cdot 2^{n-1}$
36	206 158 430 209	$103\,079\,215\,104 = 3 \cdot 2^{n-1}$
41	6 597 069 766 657	$1\,649\,267\,441\,664 = 3 \cdot 2^{n-1}$

3; 5; 11 и 17. Несмотря на значительный объем проведенных вычислений, не найдено никаких $A > 41$. Найдены также другие многочлены $f(n)$, принимающие значения простых чисел, но все они при некоторых значениях n «перестают действовать». Вот еще интересный пример [22]. Если в выражении

$$N = (2^p + 1)/3 \quad (8.6)$$

вместо p подставлять различные простые нечетные числа от 31, то значения N также будут простыми числами. Приведем значения p и соответствующие им значения N (табл. 42). Формула (8.6) «отказывается служить» при $p = 37$. В этом случае 45 812 984 491 — составное число. Оно разлагается на два простых сомножителя: $45\,812\,984\,491 = 1\,777 \cdot 25\,781\,083$.

Попытка построить функцию, охарактеризованную выше в виде показательной функции $f(n) = a^n \pm b^n$, где a и b — целые числа, приводит в простейшем случае, когда $a = 2$ и $b = 1$, к простым числам Мерсенна и Ферма. Заменив в выражении

$$f(n) = a^n \pm b^n \quad (8.7)$$

a и b соответственно на a^m и b^m, увидим, что, кроме тривиальных исключений, число $a^{m \cdot n} - b^{m \cdot n}$ является составным. Простые числа могут появиться только лишь при $a - b = 1$ и простом показателе степени. Простейший случай $a = 2$, $b = 1$ приводит к простым числам вида $2^n - 1$ (простые числа Мерсенна).

Из (8.7) следует, что $a^m + b^m$ может быть простым числом лишь тогда, когда m не имеет нечетных простых делителей, т. е. является степенью числа 2. Для $a = 2$, $b = 1$ получаем простые числа вида $F_n = 2^{2^n} + 1$ (простые числа Ферма). Новые простые числа можно найти, подставляя другие значения a и b в (8.7):

Таблица 42. **Числа вида $N = (2p + 1)/3$**

p	N	$N - 1$	T_N (2)
3	3	2	2
5	11	$2 \cdot 5$	10
7	43	$2 \cdot 3 \cdot 7$	14
11	683	$2 \cdot 11 \cdot 31$	11
13	2731	$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	13
17	43 691	$2 \cdot 5 \cdot 17 \cdot 257$	17
19	174 763	$2 \cdot 7 \cdot 19 \cdot 73$	19
23	2 796 903	$3 \cdot 23 \cdot 89 \cdot 681$	23
29	178 956 971	$2 \cdot 5 \cdot 29 \cdot 13 \cdot 113 \cdot 187$	29
31	715 827 883	$2 \cdot 7 \cdot 11 \cdot 31 \cdot 151 \cdot 331$	31

Таблица 43. Десять наибольших простых чисел, меньших N ($N - a_1$, $N - a_2$, $N - a_3$, ..., $N - a_{10}$)

N	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8	a_9	a_{10}
2^4	3	5	—	—	—	—	—	—	—	—
2^5	1	3	9	—	—	—	—	—	—	—
2^6	3	5	11	17	—	—	—	—	—	—
2^7	1	15	19	21	25	27	31	—	—	—
2^8	5	15	17	23	27	29	33	45	57	—
2^9	3	9	13	21	25	33	45	49	51	55
2^{10}	3	5	11	15	27	33	41	47	53	77
2^{11}	9	19	21	31	37	45	49	51	55	61
2^{12}	3	5	17	23	39	45	47	69	75	77
2^{13}	1	13	21	25	31	45	69	75	81	91
2^{14}	3	15	21	23	35	45	51	65	83	111
2^{15}	19	49	51	55	61	75	81	115	121	135
2^{16}	15	17	39	57	87	89	99	113	117	123
2^{17}	1	9	13	31	49	61	63	85	91	99
2^{18}	11	17	23	33	35	41	65	75	75	93
2^{19}	1	19	27	31	45	57	67	69	85	87
2^{20}	3	5	17	27	59	69	129	143	153	185

$$ {}_2M_p = 2^p - 1,\ {}_3M_p = 3^p - 2,\ {}_4M_p = 4^p - 3,\ \ldots,\ {}_mM_p = $$
$$ = (m+1)^p - m; \qquad (8.8) $$

$$ {}^1_2F_n = 2^{2^n} + 1,\ {}^3_2F_n = 2^{2^n} + 3^{2^n},\ {}^5_2F_n = 2^{2^n} + 5^{2^n},\ \ldots; \qquad (8.9) $$

$$ {}^1_3F_n = 3^{2^n} + 1,\ {}^2_3F_n = 3^{2^n} + 2^{2^n},\ \ldots,\ {}^\beta_\alpha F_n = \alpha^{2^n} + \beta^{2^n}. \qquad (8.10) $$

Упражнение 8.4. По выражениям (8.8) — (8.10) построить таблицы простых чисел.

Охота за формулами, которые позволяли бы получать только простые числа, началась в классической древности и до сих пор не увенчалась успехом. Приведем еще таблицу простых чисел вида $p_m = 2^n - a_m$, где a_m — целые числа (табл. 43). Но аппаратурная реализация арифметических операций конечных полей GF (p_m) затруднена.

Очевидно, новые результаты в плане поиска удобных значений модулей M, применяемых для задач ЦОС, можно получить, переходя к системам счисления с основанием, большим 2. Фактически это уже использовалось в выражениях (8.8) — (8.10). Для сравне-

Таблица 44. Разложение чисел $M = 3^n \pm \nu$ на простые сомножители при $\nu = 2$

n	$3^n - \nu$	$3^n + \nu$
2	7	11
3	5^2	29
4	79	83
5	241	$5 \cdot 7^2$
6	727	$17 \cdot 43$
7	$5 \cdot 19 \cdot 23$	$11 \cdot 199$
8	$7 \cdot 937$	6563
9	19 683	$5 \cdot 31 \cdot 127$
10	$137 \cdot 431$	59 051
11	$5 \cdot 71 \cdot 499$	$7 \cdot 25\,307$
12	$113 \cdot 1703$	$11 \cdot 48\,313$
13	$197 \cdot 8093$	$5^3 \cdot 63\,773$
14	$7 \cdot 17 \cdot 40\,193$	4 782 971

ния приведем таблицы разложения чисел вида $M = k^n \pm \nu$ на простые множители при $k = 3 \div 10$ (см. табл. 44—51). Разложение четных M не приводится.

Из данных табл. 44—51 видно, что с возрастанием k число практически интересных модулей M увеличивается. И это только в рамках чисел вида $M = k^n \pm \nu$. Значит, усложнять выражение для значения модуля M, что приведет к увеличению аппаратурных затрат при реализации, нет необходимости.

Преимущества более высоких оснований систем счисления (больше 2) показаны наглядно. Заметим, что реализация соответствующих устройств, работающих с такими основаниями систем счисления, наиболее эффективна с помощью многозначной элементной базы. По мнению авторов, в некоторых случаях были бы эффективными даже двоично-кодированные многозначные устройства. Однако ясно, что применение многозначной элементной базы будет всегда эффективнее.

3. Принципы построения и свойства многозначных структур

Исследования устройств ИВТ, использующих многозначное (недвоичное) представление информации, ведутся в нашей стране и за рубежом на протяжении многих лет. За эти годы

Таблица 45. **Разложение чисел $M = 4^n \pm \nu$ на простые сомножители**

n	$4^n - \nu$		$4^n + \nu$	
	$\nu = 1$	$\nu = 3$	$\nu = 1$	$\nu = 3$
2	$3 \cdot 5$	13	17	19
3	$3^2 \cdot 7$	61	$5 \cdot 13$	67
4	$3 \cdot 5 \cdot 17$	$11 \cdot 23$	257	$7 \cdot 37$
5	$3 \cdot 11 \cdot 31$	1021	$5^2 \cdot 41$	$13 \cdot 79$
6	$3^2 \cdot 5 \cdot 7 \cdot 13$	4093	$17 \cdot 241$	4099
7	$3 \cdot 43 \cdot 127$	16 381	$5 \cdot 29 \cdot 113$	$7 \cdot 2341$
8	$3 \cdot 2731 \cdot 8191$	$13 \cdot 71^2$	65 537	65 539
9	$3^3 \cdot 7 \cdot 19 \cdot 73$	$11 \cdot 23\,831$	$5 \cdot 13 \cdot 37 \cdot 109$	262 147

Таблица 46. **Разложение чисел $M = 5^n \pm \nu$ на простые сомножители**

n	$5^n - \nu$		$5^n + \nu$	
	$\nu = 2$	$\nu = 4$	$\nu = 2$	$\nu = 4$
2	23	$3 \cdot 7$	3^3	29
3	$3 \cdot 41$	11^2	127	$3 \cdot 43$
4	$7 \cdot 89$	$3^3 \cdot 23$	$3 \cdot 11 \cdot 191$	$17 \cdot 37$
5	$3^2 \cdot 347$	3121	$53 \cdot 59$	$3 \cdot 7 \cdot 149$
6	$17 \cdot 919$	$3 \cdot 41 \cdot 127$	$3 \cdot 5209$	15 629
7	$3 \cdot 26\,041$	78 121	$7 \cdot 11\,161$	$3^2 \cdot 8681$

Таблица 47. **Разложение чисел $M = 6^n \pm \nu$ на простые сомножители**

n	$6^n - \nu$			$6^n + \nu$		
	$\nu = 1$	$\nu = 3$	$\nu = 5$	$\nu = 1$	$\nu = 3$	$\nu = 5$
2	$5 \cdot 7$	$3 \cdot 11$	31	37	39	41
3	$5 \cdot 43$	$3 \cdot 71$	211	$7 \cdot 31$	$3 \cdot 73$	$13 \cdot 17$
4	$5 \cdot 7 \cdot 37$	$3 \cdot 431$	1291	1297	$3 \cdot 433$	1301
5	$5^2 \cdot 311$	$3 \cdot 2591$	$19 \cdot 409$	$7 \cdot 11 \cdot 101$	$3 \cdot 2593$	$31 \cdot 251$
6	$5 \cdot 7 \cdot 31 \cdot 43$	$3 \cdot 15\,551$	$11 \cdot 4241$	$13 \cdot 37 \cdot 97$	$3 \cdot 103 \cdot 151$	$29 \cdot 1609$
7	$5 \cdot 55\,987$	$3 \cdot 93\,311$	$157 \cdot 1783$	$7^2 \cdot 29 \cdot 197$	$3 \cdot 11 \cdot 17 \cdot 499$	$279\,941$

Таблица 48. **Разложение чисел $M = 7^n \pm \nu$ на простые сомножители**

n	$7^n - \nu$			$7^n + \nu$		
	$\nu = 2$	$\nu = 4$	$\nu = 6$	$\nu = 2$	$\nu = 4$	$\nu = 6$
2	47	$3^2 \cdot 5$	43	$3 \cdot 17$	53	$5 \cdot 11$
3	$11 \cdot 31$	$3 \cdot 113$	337	$3 \cdot 5 \cdot 23$	347	349
4	2399	$3 \cdot 17 \cdot 47$	$5 \cdot 479$	$3^4 \cdot 89$	$5 \cdot 13 \cdot 37$	$29 \cdot 83$
5	$5 \cdot 3361$	$3 \cdot 3 \cdot 1867$	$53 \cdot 317$	$3 \cdot 13 \cdot 431$	16 811	$17 \cdot 23 \cdot 43$
6	$71 \cdot 1657$	$3 \cdot 5 \cdot 11 \cdot 23 \cdot 31$	117 643	$3^2 \cdot 19\,739$	$29 \cdot 4057$	$5 \cdot 23\,531$

Таблица 49. **Разложение чисел $M = 8^n \pm \nu$ на простые сомножители**

n	$8^n - \nu$				$8^n + \nu$			
	$\nu = 1$	$\nu = 3$	$\nu = 5$	$\nu = 7$	$\nu = 1$	$\nu = 3$	$\nu = 5$	$\nu = 7$
2	$3^2 \cdot 7$	61	59	$3 \cdot 19$	$2^2 \cdot 3 \cdot 5$	67	$3 \cdot 23$	71
3	$7 \cdot 73$	509	$3 \cdot 13^2$	$5 \cdot 101$	$3^3 \cdot 19$	$5 \cdot 103$	$11 \cdot 47$	$3 \cdot 173$
4	$3^2 \cdot 5 \cdot 7 \cdot 13$	4093	4091	$3 \cdot 29 \cdot 47$	$17 \cdot 241$	4099	$3 \cdot 1367$	$11 \cdot 373$
5	$7 \cdot 31 \cdot 151$	$5 \cdot 6553$	$3 \cdot 67 \cdot 163$	181^2	$3^2 \cdot 11 \cdot 331$	32 771	$13 \cdot 2521$	$3 \cdot 5^2 \cdot 19 \cdot 23$

Таблица 50. **Разложение чисел $M = 9^n \pm \nu$ на простые сомножители**

n	$9^n - \nu$				$9^n + \nu$			
	$\nu = 2$	$\nu = 4$	$\nu = 6$	$\nu = 8$	$\nu = 2$	$\nu = 4$	$\nu = 6$	$\nu = 8$
2	79	$7 \cdot 11$	$3 \cdot 5^2$	73	83	$5 \cdot 17$	$3 \cdot 29$	89
3	727	$5^2 \cdot 29$	$3 \cdot 241$	$7 \cdot 103$	$17 \cdot 43$	733	$3 \cdot 5 \cdot 7^2$	$11 \cdot 67$
4	$7 \cdot 937$	$79 \cdot 83$	$3 \cdot 5 \cdot 19 \cdot 23$	6553	6563	$5 \cdot 13 \cdot 101$	$3 \cdot 11 \cdot 199$	6569
5	$137 \cdot 431$	$5 \cdot 7^2 \cdot 241$	$3 \cdot 19\,681$	$17 \cdot 23 \cdot 151$	59 051	59 053	$3 \cdot 54 \cdot 31 \cdot 127$	$73 \cdot 809$

Таблица 51. **Разложение чисел $M = 10^n \pm \nu$ на простые сомножители**

n	$10^n - \nu$					$10^n + \nu$				
	$\nu = 1$	$\nu = 3$	$\nu = 5$	$\nu = 7$	$\nu = 9$	$\nu = 1$	$\nu = 3$	$\nu = 5$	$\nu = 7$	$\nu = 9$
2	$3^2 \cdot 11$	97	$5 \cdot 19$	$3 \cdot 31$	$7 \cdot 13$	101	103	$3 \cdot 5 \cdot 7$	107	109
3	$3^3 \cdot 37$	997	$5 \cdot 199$	$3 \cdot 331$	991	$7 \cdot 11 \cdot 13$	$17 \cdot 59$	$3 \cdot 5 \cdot 67$	$19 \cdot 53$	1009
4	$3^2 \cdot 11 \cdot 101$	$13 \cdot 769$	$5 \cdot 1999$	$3 \cdot 3331$	$97 \cdot 103$	$73 \cdot 137$	$7 \cdot 1429$	$3 \cdot 5 \cdot 23 \cdot 29$	10 007	10 009
5	$3^3 \cdot 7 \cdot 11 \cdot 13 \cdot 37$	$757 \cdot 1321$	$5 \cdot 7 \cdot 2857$	$3 \cdot 33\,331$	$17 \cdot 59 \cdot 997$	$11 \cdot 9091$	100 003	$3 \cdot 5 \cdot 59 \cdot 113$	$97 \cdot 1031$	$7^2 \cdot 13 \cdot 157$

неоднократно и довольно существенно изменялись задачи, которые возникали перед разработчиками средств ИВТ, в том числе — многозначной ИВТ.

Первоначально основной задачей считалось снижение числа активных элементов, в последнее время с учетом резкого снижения стоимости отдельных транзисторов, изготавливаемых методами интегральной технологии,— решение проблемы внешних и внутренних связей (соединений). Проблема соединений является одной из актуальных проблем современной вычислительной техники, носит принципиальный характер [164] и особенно ярко проявляется при создании современных БИС и СБИС. Если принять, что линейные размеры кристалла составляют n единиц длины (рис. 39), то с ростом размеров кристалла параметр, определяющий допустимое число внешних выводов, возрастает с увеличением n линейно, тогда как площадь кристалла s, предназначенная для размещения схемы, возрастает пропорционально n^2. В то же время число связей на самом кристалле (для схемы с общим характером соединений) возрастает как $(n^2)!$

Попытка решить проблему внутренних соединений выделением на кристалле отдельных слабо связанных функциональных модулей приводит к новой версии исходной задачи, в которой проблема соединений сохраняется внутри укрупненных модулей [212].

Таким образом, число внешних соединений L_e, активных элементов N и внутренних соединений L_i связаны с размерами кристалла следующими оценочными соотношениями, свидетельствующими о недостаточности числа внешних выводов и чрезвычайно быстром росте внутренних связей:

$$L_e \equiv n;\ N \equiv s \equiv n^2;\ L_i \equiv (n^2)!$$

Образно говоря, с увеличением степени интеграции и размера кристаллов БИС может «задохнуться» вследствие невозможности организации внешнего обмена или из-за того, что внутренние связи занимают большую часть кристалла. По данным работы [185], в современных двоичных СБИС внутренние связи и изоляция занимают до 90 % площади кристалла, тогда как на долю активных элементов остается всего 10 % площади. Проблема соединений характерна не только для схем микроэлектроники, но и для других устройств ИВТ. В частности, в некоторых специализиро-

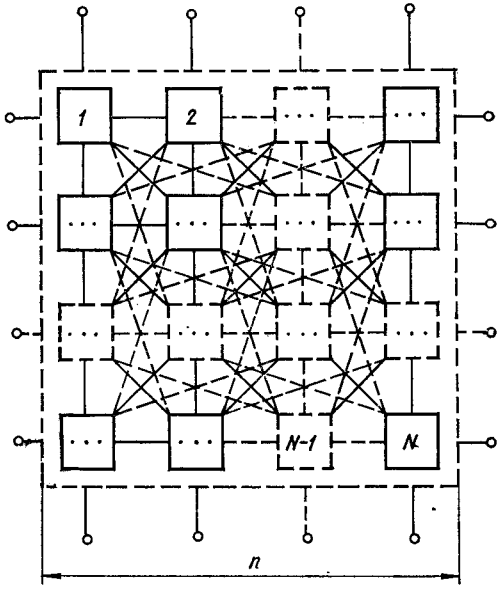


Рис. 39. Схема кристалла БИС,

ванных устройствах ИВТ масса кабельных соединений достигает 70 % общей массы устройства.

Одним из возможных и, по-видимому, наиболее радикальных способов решения проблемы соединений является использование многозначного представления информации и многозначной элементной базы. Использование многозначности позволяет создавать структуры, оптимальные по аппаратурным затратам, быстродействию, точности, и легко осуществлять «размен» одних параметров на другие. При этом если непосредственный размен, например, быстродействия на сложность при фиксированной значности может быть затруднен тем, что каждый из этих параметров задан жестко исходными техническими требованиями, то при выборе оптимальной (с точки зрения соотношения параметров) значности конструктор имеет значительную свободу. Что касается вопроса соединений, то здесь выигрыш от многозначности (с основанием k) представления информации по сравнению с двоичным определяется известным соотношением $L_2/L_k = \log_2 k$. Этот выигрыш определяется возможностью передачи больших объемов информации по каждому из соединений между функциональными элементами и модулями.

Распространяя приведенное выше выражение на крайний случай $k \to \infty$, т. е. на случай бесконечнозначных (или аналоговых) структур, можно по-новому оценить тот известный факт, что для них проблемы сложности соединений практически не существует. Естественно предположить, что эта проблема присуща именно двоичным устройствам ИВТ и обусловлена в основном сравнительно низкими функциональными возможностями двоичных элементов и структур по отношению к требуемому количеству сигнальных и вспомогательных соединений. Для аналоговых систем это отношение существенно лучше. В то же время современные цифровые (двоичные) системы существенно превосходят аналоговые системы по точности и стабильности. Можно, однако, с уверенностью сказать, что это превосходство не является привилегией только двоичных устройств и что во многих случаях использование двоичного представления является неоправданной перекомпенсацией отрицательных свойств аналоговых устройств ИВТ. Комплексное решение проблемы числа соединений, точности, сложности, быстродействия и т. п. должно приводить к выбору оптимальной значности k, частными крайними случаями которой могут являться 2 и ∞. В то же время оперирование только двумя этими крайними значениями k невольно напоминает систему счета примитивных племен: «один, два, много».

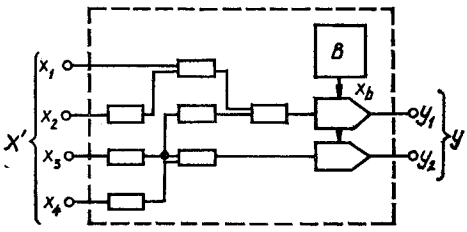


Рис. 40. Схема типового элемента многозначной структуры.

Возрастающий интерес к многозначным элементам и структурам обусловлен рядом причин. Использование принципов многозначного кодирования позволяет добиваться существенной экономии оборудования и уве-

личения надежности систем. При реализации в интегральном исполнении многозначные структуры характеризуются малым количеством межэлементных связей и могут быть собранными из весьма ограниченного числа типов интегральных схем. Присущая многозначным элементам высокая универсальность обеспечивает однородность структур, построенных на основе этих элементов. Перечисленные причины предопределяют в качестве ближайшей области применения многозначных элементов системы ИВТ. Наличие этих и других положительных качеств (в частности, принципиальной возможности значительного повышения быстродействия) позволяет широко использовать многозначную элементную базу в современных ЦВМ, особенно при построении аппаратных средств ЦОС.

Попытки оптимизации параметров средств ИВТ с использованием многозначного представления информации, в частности сокращения числа соединений в БИС и СБИС, предпринимаются относительно недавно. В работах [128, 191], где рассматривается задача сокращения внешних соединений, предложено решение указанной задачи использованием для организации внешнего обмена АЦП и ЦАП (или, точнее, двоично-многозначных кодеров и декодеров) при сохранении двоичной организации внутри самой БИС. Такой подход не устраняет проблему внутренних соединений, решение которой возможно только при наличии многозначной элементной базы во всех частях БИС, удовлетворяющей требованиям современной микроэлектроники. Рассмотрим некоторые общие принципы организации и свойства многозначных элементов и структур, сформулированные в первоначальной форме в работах [137, 140, 142, 144, 145] и успешно реализуемые в настоящее время.

Характерной чертой современных многозначных структур является гибридность, заключающаяся в возможности представления сигналов как в аналоговой, так и в цифровой форме. Перспективность гибридных устройств такого типа отмечена, в частности, в [24]. Широкое использование гибридности позволяет создавать структуры и системы, сочетающие в себе достоинства аналоговых (высокое быстродействие, малое число соединений) и цифровых (высокая точность и стабильность) устройств и являющиеся оптимальными по соотношению этих параметров. Рационально построенные гибридные многозначные структуры являются, кроме того, оптимальными

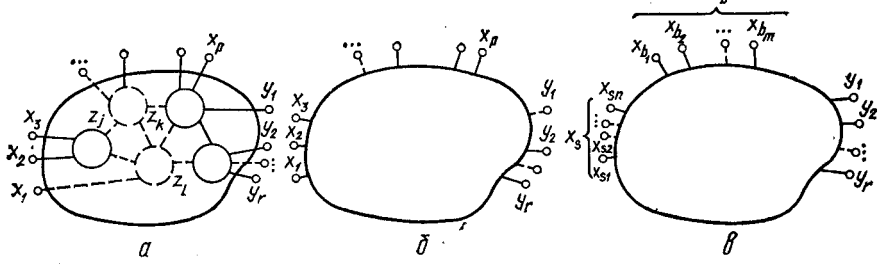


Рис. 41. Схема перехода от электронной модели к многозначной логической схеме.

также по аппаратурным затратам и, как следствие этого,— по надежности.

В отличие от известных гибридных вычислительных машин и комплексов, представляющих собой отдельные аналоговые и цифровые части, связанные между собой с помощью АЦП и ЦАП, гибридность многозначных структур проявляется в представлении сигналов на уровне отдельных компонент (вентилей, резисторов и т. п.). Типовой элемент многозначной структуры содержит как аналоговые, так и цифровые компоненты (рис. 40). На рисунке первые из них изображены прямоугольниками, вторые — неправильными пятиугольниками. (Конкретная схема элемента выбрана произвольно.) Поскольку выходы элемента соединены со входами других элементов, в многозначной структуре имеет место непрерывное чередование аналоговой и цифровой форм представления информации.

Цифровые компоненты соединены с источником базисных величин B. Использование системы базисных величин, являющееся основой принципа базиса, обеспечивает работоспособность и высокую функциональную надежность элементной базы при изменениях параметров компонент и внешних факторов. Сущность принципа базиса в современной трактовке [138, 143] заключается в том, что сигналам с погрешностями из множества $\{X'\}$ периодически ставятся в соответствие точные (или, во всяком случае, значительно более точные) значения сигналов из множества $\{x_b\}$.

Рассмотрим реализацию принципа базиса в современной трактовке в связи с задачами построения и математического исследования гибридных многозначных структур. Любое реальное многозначное устройство представляет собой некоторую электронную схему (рис. 41, *а*), описываемую в общем случае системой дифференциальных уравнений. Это представление является наиболее полным и позволяет детально исследовать все аспекты поведения устройства, включая погрешности передачи входных сигналов. Описывая и исследуя многозначное устройство с помощью системы дифференциальных уравнений, мы не накладываем никаких ограничений на диапазон изменения входных и выходных сигналов, рассматривая эти сигналы в общем случае как непрерывные, а саму схему — как аналоговую (x, y, $z \in Q$). Положение не изменяется принципиально и при переходе к макромодели, описывающей терминальное поведение устройства (рис. 41, *б*). Здесь происходит снижение порядка системы уравнений, описывающих устройство, за счет сокращения множества внутрисхемных сигналов, но сам характер уравнений и сигнальных величин остается неизменным (x, $y \in Q$).

Ситуация изменяется радикально при переходе от макромодели к многозначной логической схеме устройства (рис. 41, *в*). Прежде всего, общее множество $\{x\}$ входов разбивается на два подмножества — сигнальных $\{x_s\}$ и базисных $\{x_b\}$ входов, причем $\{x_b\}$ при выбранной значности k принадлежит по определению множеству E_k. Входные сигнальные $\{x\}$ и выходные величины $\{y\}$ характеризуются, вообще говоря, наличием погрешностей, определяющих их отклонение от значений множества E_k. Если значения этих погрешностей

не превосходят нигде половины интервала квантования, то их можно не принимать во внимание и полагать, что множества $\{x\}$ и $\{y\}$ также принадлежат E_k.

Периодические обращения к множеству базисных величин, обладающих гарантированной точностью задания, существенным образом отличают цифровые многозначные структуры от аналоговых структур. В аналоговых структурах имеет место непрерывное накопление погрешности e по мере увеличения числа элементарных преобразований:

$$x_1 \to x_2 = y_2 + e_1 \to x_3 = y_2 + e_2 \to x_4 = y_3 + e_3, \ \ldots, \qquad (8.11)$$

причем $e_1 < e_2 < e_3 < \ldots$.

В многозначных структурах картина существенно изменяется:

$$x_1 \to x_2 = y_1 + e_1' \upharpoonright\downarrow x_{b_1} \to x_3 = y_2 + e_2' \upharpoonright\downarrow x_{b_2}, \ \ldots, \qquad (8.12)$$

где $e_1', e_2', \ldots, < e_{\max}$.

В выражении (8.12) знаком $\to$ обозначен некоторый функциональный оператор, а знаком $\upharpoonright\downarrow$ — обращение к множеству базисных величин, осуществляемое цифровыми компонентами структуры — квантователями. В (8.12) представлен крайний случай обращения к множеству базисных величин после каждого функционального преобразования. На практике эта операция восстановления сигналов может осуществляться после нескольких функциональных преобразований, число которых между последовательными обращениями к базису определяется точностью преобразования и выбранной значностью. Операции восстановления сигналов могут сочетаться в цифровых элементах с функциональными преобразованиями.

Базисные величины неизбежно характеризуются определенными разбросами и отклонениями от номинальных значений. Это обстоятельство особенно характерно при использовании принципа базиса при создании многозначных БИС, где по соображениям снижения числа вводов и внутренних соединений базисные величины могут формироваться в каждом отдельном элементе структуры. Принцип базиса соблюдается в полной мере и в том случае, если приняты меры к тому, чтобы максимальная суммарная погрешность $e_{\max}$ формирования базисных величин и воспроизведения их отдельными элементами многозначной структуры заведомо не превышала половины интервала квантования, определяемого выбранной значностью.

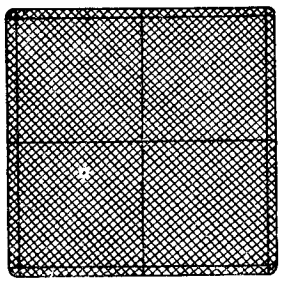
Остановимся более подробно на различиях между аналоговыми и цифровыми структурами, а также на механизме образования фиксированных состояний и преобразования сигналов в цифровых многозначных структурах. В аналоговой системе все состояния являются равновероятными; состояния, соответствующие целочисленным значениям, ничем не отличаются от любых других состояний системы. Пространство состояний аналоговой системы показано на рис. 42, *а* (для наглядности это пространство принято двухмерным). Целочисленным значениям условно соответствуют точки пересечения горизонтальных и вертикальных прямых, а вероятность пребывания системы в определенном состоянии отображена интенсивностью

штриховки (в данном случае равномерной по всей площади). На пространство состояний наложено пространство помех, осуществляющих перевод системы из одних точек пространства состояний в другие по некоторому случайному закону.

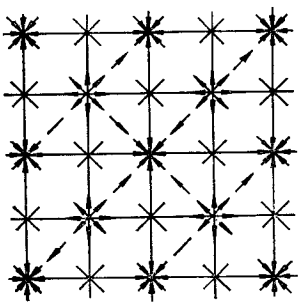
Преобразование исходной аналоговой системы в цифровую многозначную осуществляется введением в ее состав специальных преобразователей — квантователей с характеристиками $y = f(x)$ особого типа (рис. 43). Эти характеристики формируются следующим образом. Вначале выбираются k состояний, соответствующих целым числам (0, 1, ..., $k - 1$) и отвечающих номинальным значениям сигналов $x_н$. Определяются также k промежуточных значений (1′, 2′, ..., $(k - 2)'$), лежащих посередине между номинальными значениями, и принимается, что во всех этих $2k$ точках для входного и выходного сигналов выполняется условие $y = x$. Тем самым принимается, что статистический коэффициент передачи $K_{ст}$ в этих точках равен единице. Затем через эти $2k$ точек проводится кривая (или ломаная) таким образом, чтобы динамический (дифференциальный) коэффициент передачи $K_д$ имел значение $K'_д > 1$ в точках $x = 0, 1, ...$ ..., $k - 1$ и $K'_д > 1$ — в промежуточных точках (в предельном случае $K'_д = 0$, $K''_д \to \infty$). Номинальные сигналы передаются этими преобразователями со статическим коэффициентом передачи $K_{ст} = 1$, а отклонения от номинальных сигналов (в определенных пределах) — с динамическим коэффициентом $K'_д < 1$:

$$y = K_{ст}x_н + K'_д e = x_н + K'_д e.$$

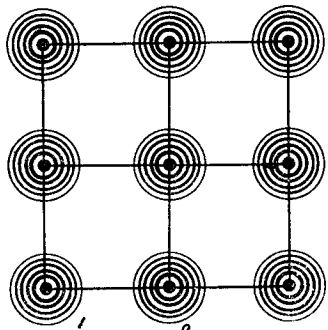
В предельном случае отклонения передаются с коэффициентом передачи, равным нулю. В результате воздействия операторов квантования (рис. 42, *б*) на пространство состояний исходной системы в окрестностях номинальных сигналов имеет место уменьшение значений отклонений, т. е. снижение уровня



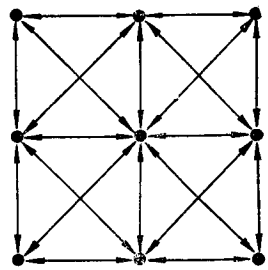
а



б



в



г

Рис. 42. Условная схема пространства состояний аналоговых и цифровых схем.

накопившихся погрешностей, и сигналы начинают группироваться в окрестностях номинальных целочисленных значений. В реальной многозначной системе устанавливается своего рода «динамическое равновесие между группирующим действием квантующих операторов и рассеивающим действием пространства «операторов» помех, в итоге образуется ряд размытых подмножеств состояний, соответствующих уже не аналоговой, а реальной цифровой многозначной системе (рис. 42, *в*). Центры этих подмножеств располагаются в точках, соответствующих номинальным значениям. Исследование поведения системы в окрестности каждой из этих точек составляет задачу моделирования. Переход к идеальному пространству состояний, на которые воздействуют функциональные операторы, приводит к задачам логического анализа и синтеза (рис. 42, *г*).

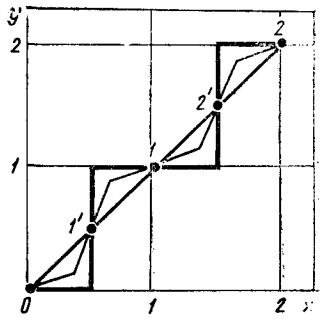


Рис. 43. Характеристика квантователя при $k = 3$.

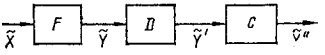


Рис. 44. Представление многозначной структуры.

Приведенные выше соображения позволяют предпринять попытку создания единого аппарата исследования реальных многозначных структур, учитывающего аналого-цифровой характер преобразуемых ими сигналов. Многозначную структуру всегда можно представить в виде последовательной цепочки преобразователей (рис. 44). На рис. 44 обозначены: F — функциональный преобразователь; D — «преобразователь» искажений (или рассеяния); C — корректирующий (или квантующий) преобразователь. Процесс преобразования информации в реальной k-значной структуре имеет вид последовательности отображений:

$$\tilde{X} \xrightarrow{F} \tilde{Y} \xrightarrow{D} \tilde{Y}' \xrightarrow{C} \tilde{Y}''.$$

Рассмотрим вначале первое отображение F, соответствующее функциональному преобразованию. Идеальные (свободные от погрешностей) входной вектор X и выходной вектор Y для структуры с n входами являются n-векторами в n-мерном линейном пространстве E_k^n. Само функциональное преобразование описывается $k^n \times k^n$ матрицей $\{F\}$. Однако в реальных структурах функциональные преобразования выполняются не над точными (идеальными) значениями сигналов x_i, а над реальными их значениями $\tilde{x}_i = x_i + e_i$, содержащими погрешности (отклонения) e_i. Тогда $\tilde{X} = X + E$, где $X = (x^i)$ и $E = (e_i)$ — $n \times k^n$ — матрицы аналогичного вида. Значения реальных сигналов не являются целыми числами (точнее, не находятся в целочисленном отношении). При надлежащем выборе значности k и достаточно малых погрешностях входного сигнала реальные значения функций, составляющих матрицу выходных сигналов, отличаются от идеальных меньше чем наполовину интервала квантования.

При анализе преобразований сигналов в многозначных структурах удобно считать, что функциональное преобразование не вносит дополнительных погрешностей, а внесение и коррекцию погрешностей можно описывать с помощью двух других преобразований, входящих в общую цепочку и выражаемых соответственно матрицей искажений $\{D\}$ и матрицей коррекции (квантования) $\{C\}$. Первая из них представляет собой диагональную матрицу вида

$$D = \begin{bmatrix} d_{11} & 0 & \dots & 0 \\ 0 & d_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & d_{ll} \end{bmatrix},$$

где $d_{ii} = 1 \pm \delta_{ii}$ — коэффициенты, характеризующие дополнительные отклонения сигналов от номинальных значений, возникающие в структуре до выполнения операции квантования.

Число l является условной размерностью матрицы. Получаемая после воздействия матрицы $\{D\}$ матрица значений сигналов $\{\tilde{Y}'\}$ подобно $\{\tilde{X}\}$ представляет собой сумму матриц номинальных значений и погрешностей, которые, вообще говоря, превышают соответствующие значения погрешностей во входных сигналах вектора $\{\tilde{X}\}$, а следовательно, и в сигналах вектора $\{\tilde{Y}\}$. Эта матрица далее взаимодействует с матрицами корректирующих коэффициентов:

$$\{C\} = \begin{bmatrix} K_{\text{ст}_{11}} & 0 & \dots & 0 \\ 0 & K_{\text{ст}_{22}} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & K_{\text{ст}_{ll}} \end{bmatrix} + \begin{bmatrix} K'_{\text{д}_{11}} & 0 & \dots & 0 \\ 0 & K'_{\text{д}_{22}} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & K'_{\text{д}_{ll}} \end{bmatrix}. \quad (8.13)$$

Как отмечалось, в предельном случае первая из двух матриц (8.13), сумма которых образует $\{C\}$, обращается в единичную, а вторая — в нулевую матрицу. Практически и элементы матрицы выходных сигналов $\{\tilde{Y}''\}$ всегда содержат свои погрешности, не превышающие при нормальном функционировании структуры половины интервала квантования.

Из приведенных рассуждений видны взаимосвязь и отличия аналоговых и цифровых устройств, а также методов анализа непрерывных и дискретных систем. В первом случае переменные принимают значения из множества рациональных чисел Q (на установленной шкале измерения), во втором — только из конечного множества целых чисел E_k. Практически во втором случае значения переменных не обязательно в точности соответствуют значениям из E_k, но отклонения можно не принимать во внимание ввиду их гарантированной ограниченности и отсутствия накопления погрешностей. Таким образом, различие между аналоговыми и цифровыми многозначными системами состоит в использовании принципа базиса. (Заметим, что

и двоичные системы представляют собой простейший случай многозначных систем с базисными значениями, соответствующими 0 и 1.) Вместе с тем можно широко использовать в составе многозначных структур аналоговые операции и аналоговую схемотехнику, добиваясь существенного уменьшения общей сложности структур, в первую очередь — числа соединений.

4. Многозначная логика, схемотехника, технология

Две специфические особенности рассматриваемой элементной базы — гибридность и универсальность — определяют круг возможностей и задач, возникающих при построении многозначных структур. Наличие этих особенностей позволяет проводить организацию структур в соответствии с одним из двух существенно различающихся вариантов [141].

Гибридность, т. е. способность многозначных элементов к обработке как дискретных, так и непрерывных сигналов, позволяет вводить в состав многозначной дискретной структуры ряд элементарных непрерывных преобразователей при сохранении цифровой формы переработки информации. Такие преобразователи могут, в частности, выполнять операции суммирования и перемножения, реализация которых для непрерывных величин существенно проще, чем реализация построением соответствующих дискретных функциональных преобразователей.

Располагая такими преобразователями и одновходовыми элементами, выполняющими операции непрерывно-дискретного преобразования, можно строить дискретные сумматоры и умножители, а также произвольные многозначные структуры, используя одно из удобных представлений многозначной логики — многозначный аналог алгебры Жегалкина. Практическое применение этого представления ограничивалось именно трудностями построения соответствующей элементной базы на чисто дискретных принципах.

Гибридность элементов позволяет дополнить методы анализа и синтеза за счет привлечения хорошо разработанного аппарата непрерывных групп, который можно использовать при определении условий групповой инвариантности множества многозначных функций относительно преобразований входных переменных. Выявленные при этом свойства симметрии можно применить для упрощения процедуры синтеза. Группы непрерывных преобразований можно использовать также для получения неприводимых представлений при решении некоторых задач функциональной декомпозиции. Таким образом, гибридность обусловливает наряду с технологическим упрощением также возможность применения при решении задач синтеза новых и эффективных алгебраических методов.

Универсальность многозначных элементов обеспечивает значительную свободу при выборе системы базисных операций. Поскольку функционально полные системы в многозначной логике обладают несравненно большим разнообразием по сравнению с двоичной, серьез-

ное значение приобретает задача выбора способа аналитического представления многозначных переключательных функций, обеспечивающего эффективность методов синтеза цифровых автоматов в многозначном структурном алфавите. В этом плане значительный интерес представляют работы по классификации функций многозначной логики и исследование возможностей введения избыточности в логические базисы. Наиболее перспективными представляются здесь декомпозиционные методы синтеза в базисе бинарных операций. Принципиальная возможность выполнения многовходовых универсальных логических модулей может радикально изменить саму постановку задачи комбинационного синтеза.

Целесообразно также выделение наборов простейших логических сетей, накрывающих все функции из P_k^n, и разработка эффективных алгоритмов синтеза (декомпозиции) для различных классов функций. Немалый интерес представляет возможность построения структур с неоднородными основаниями счисления, непосредственно вытекающая из особенностей рассматриваемых многозначных элементов.

Обеспечение высокой функциональной надежности и серийной пригодности многозначных структур — важное, но не единственное следствие применения принципа базиса. Дополнительным результатом, как отмечалось, является многофункциональность элементной базы. Это качество позволяет осуществить разумный компромисс между требованиями специализации БИС и стремлением уменьшить их номенклатуру и стоимость за счет увеличения тиражирования. Преимущества использования многозначного представления информации и многозначной элементной базы наиболее полно раскрываются при совместном выполнении требований многофункциональности и однородности.

Многофункциональность достигается благодаря тому, что при реализации современных многозначных элементов базисные векторы могут задавать не только уровни состояний, но и саму выполняемую элементом функцию. Смета базисного вектора приводит к изменению такой функции при неизменности структуры элемента. Поскольку базисные векторы могут (в случае одновходового элемента) задаваться k^k способами, получаемые элементы будут универсальными. Аналогично обстоит дело с n-входовыми k-значными элементами, где общее число выполняемых функций составляет k^{k^n}. Это число соответствует мощности множества всех функций k-значной логики от n переменных P_k^n.

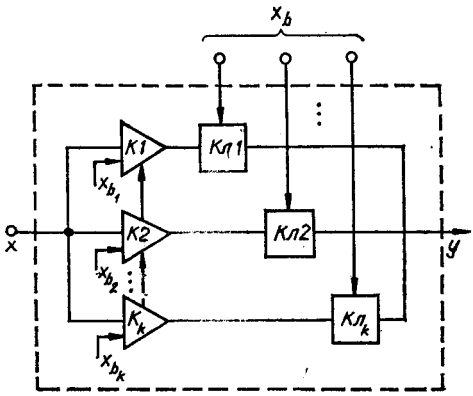


Рис. 45. Схема одновходового универсального элемента.

Структурная схема одно-

входового универсального многозначного элемента с пространственным промежуточным преобразованием показана на рис. 45.

Элемент содержит преобразователь входного сигнала x в пространственный код, выполненный на связанных между собой компараторах (схемах сравнения) $К1 - К_k$, и обратный преобразователь пространственного кода в выходной сигнал y, реализованный на ключах $Кл1 - Кл_k$. Связь между компараторами обеспечивает срабатывание только того из них, в зоне действий которого находится входной сигнал. В свою очередь, компаратор осуществляет активизацию соответствующего ключа. Элементы этого типа имеют параллельную структуру и отличаются высоким быстродействием. Выполняемая элементом функция определяется видом базисного вектора x_b и изменяется при его изменении. Аналогичным образом строятся многовходовые (в частности, двухвходовые) элементы. Практически проблема построения элементов и структур с числом входов, больше двух, решается последовательным применением процедуры построения n-входовых элементов из $(n - 1)$-входовых элементов. В конечном итоге задача построения универсальной n-входовой структуры может быть приведена к реализации и соответствующему соединению одновходовых универсальных многозначных элементов типа описанных выше. Одновходовые элементы могут быть настроены на выполнение операции квантования, а при введении обратной связи могут служить также запоминающими элементами.

Практическая реализация универсальных элементов и структур оказывает существенное влияние на логический синтез. Это влияние определяется в первую очередь возможностью использования избыточных и сверхизбыточных логических базисов и, как отмечалось ранее, в пределе — базиса всех функций от заданного числа переменных. В этом предельном случае синтез может заменяться настройкой структуры на выполнение требуемой функции. Целесообразность применения логических базисов с высокой избыточностью обусловливается в первую очередь соотношением возрастания аппаратурных затрат (включая связи) и увеличения логических возможностей, а также умением использовать эти возможности.

Многофункциональность элементов тесно связана с однородностью, которая достигается сочетанием одинакового включения однотипных элементов с регулярностью структуры. Требование соблюдения однородности диктуется практикой создания современных БИС и непосредственно связано с задачей построения матричных БИС.

Анализ различных вариантов построения матричных схем [20, 21] показал особенности логических устройств, построенных на основе одноканальных бесповторных каскадов из универсальных элементов. Такие каскады способны полностью

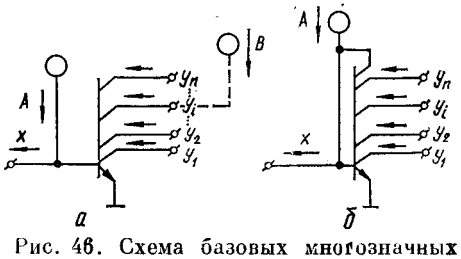


Рис. 46. Схема базовых многозначных интегральных инжекционных элементов.

использовать достоинства многозначного представления информации в схемах. В частности, при увеличении значности связей и элементов вдоль каскада по показательному закону можно синтезировать абсолютно минимальные по числу элементов схемы логических n, m-полюсников.

Практически значность элементов ограничена сверху, в силу чего бесповторные каскады из универсальных элементов не универсальны, т. е. не способны реализовать произвольную функцию от заданного числа переменных. Однако они полностью удовлетворяют требованиям однородности и фактически являются элементарным узлом для построения универсальных однородных матриц.

Многозначная однородная матрица, способная выполнить любую логическую функцию от заданного числа переменных, представляет собой набор параллельно включенных одноканальных каскадов. Для универсальной матрицы число каскадов находится в степенной зависимости от числа переменных реализуемой функции.

Отличительной чертой многозначных схем, и в особенности многозначных однородных схем, является возможность оптимизации значения одних характеристик за счет использования избыточности по другим характеристикам. Вместе с тем избыточность (в первую очередь по аппаратурным затратам), характерная для однородных универсальных схем, определяет интерес к схемам с меньшей степенью функциональной избыточности, крайним случаем которых являются схемы с фиксированной логикой, построенные в функционально полном или слабо избыточном логическом базисе [184, 186, 187, 194, 197].

При определении базисного набора важно, чтобы входящие в его состав функции допускали простую реализацию в соответствии с данной технологией. В набор часто входят аналоговые операции, широкое использование которых позволяет добиться существенного снижения аппаратурных затрат и числа внутренних соединений [169, 184]. Базовый элемент инжекционных интегральных БИС — многоколлекторный транзистор, который может включаться по схеме порогового детектора (рис. 46, *а*) или по схеме отражателя тока (рис. 46, *б*). Информация кодируется уровнями тока. Функции, выполняемые пороговым детектором и отражателем тока, определяются выражениями

$$y_i = \begin{cases} 0, & \text{если } x > A; \\ B, & \text{если } x < A; \end{cases} \qquad (8.14)$$

$$y_i = \begin{cases} A - X, & \text{если } x \leqslant A; \\ 0, & \text{если } x > A, \end{cases} \qquad (8.15)$$

где A, $B \in E_k$.

Если к этому добавить еще весовое суммирование токов

$$y = rx_1 + sx_2, \; rs = 0, 1, 2, \ldots, \qquad (8.16)$$

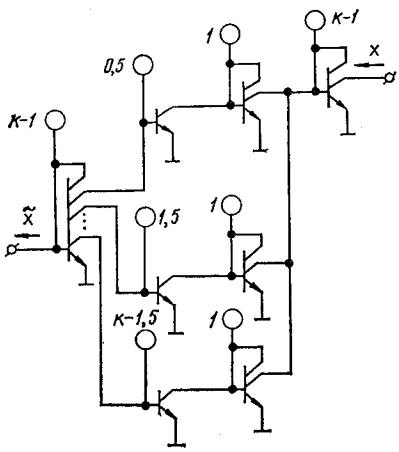


Рис. 47. Схема дискретизатора.

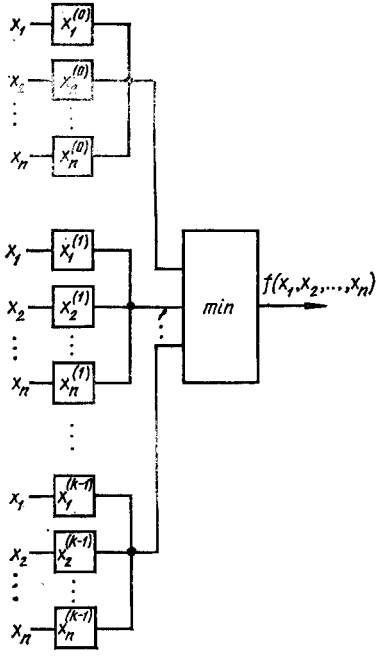


Рис. 48. Схема параллельной многозначной структуры.

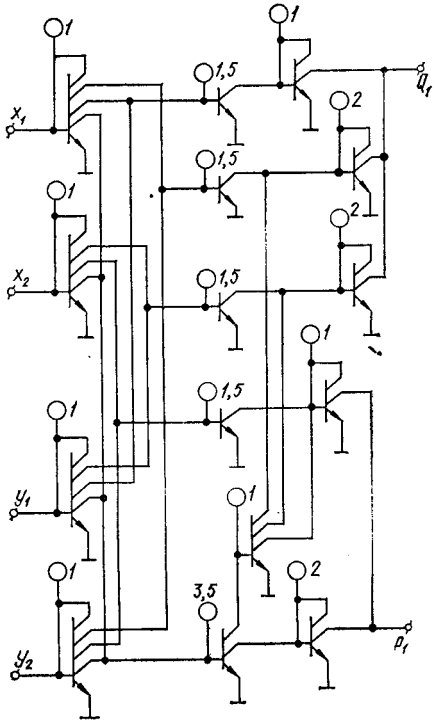


Рис. 49. Схема умножителя двухразрядных двоичных чисел с четверичным выходом.

реализуемое простым соединением коллекторов, то получится избыточная функциональная система, через элементы которой можно выразить любую k-значную функцию. В эту систему входят одна цифровая операция (8.14), а также две аналоговые — (8.15) и (8.16). В ряде случаев в систему вводятся еще некоторые функции, которые реализуются с помощью нескольких отражателей тока и пороговых детекторов и могут облегчать как процедуру формального синтеза, так и практическую реализацию многозначных структур. Одной из таких схем является схема дискретизатора (рис. 47), соответствующая структурной схеме, показанной на рис. 45. В связи с относительно высокой сложностью этой схемы выбирать базисные функции можно таким образом, чтобы их аппаратурная реализация с помощью отражателей тока и пороговых детекторов могла быть осуществлена без дополнительной установки дискретизаторов. В этом случае в каждой цепочке схем, реализующих базисные функции, находится пороговый детектор, который и обрывает цепочку накопления погрешностей, а число последовательно включенных отражателей тока не превосходит допустимой величины с учетом значения максимальной погрешности, обусловленного возможностями технологии [186].

При выборе системы базисных функций можно ставить определен-

Таблица 52. Функция умножения по модулю 4

y_2	y_1	$x_2=0$		$x_2=1$	
		$x_1=0$	$x_1=1$	$x_1=0$	$x_1=1$
0	0	0	0	0	0
	1	0	1	2	3
1	0	0	2	0	2
	1	0	3	2	1

Таблица 53. Функция переноса при умножении

y_2	y_1	$x_2=0$		$x_2=1$	
		$x_1=0$	$x_1=1$	$x_1=0$	$x_1=1$
0	0	0	0	0	0
	1	0	0	0	0
1	0	0	0	1	1
	1	0	0	1	2

ные наперед заданные условия, которым должна удовлетворять реализуемая структура. Таким условием может быть, например, максимальное быстродействие схемы, что особенно важно при разработке устройств, предназначенных для ЦОС. Ниже приведена функционально полная система базисных функций для синтеза параллельных структур. В эту систему входят характеристические функции

$$x^{(G)} = \begin{cases} 0, & \text{если } x = G; \\ \infty, & \text{если } x = G\,(G \in E_k), \end{cases} \tag{8.17}$$

а также функция минимума $x_1 \wedge x_2 = \min(x_1, x_2)$ и суммы $x_1 + x_2$.

На практике вместо ∞ в выражении (8.17) можно взять любое значение $\nu > k - 1$, удовлетворяющее неравенству $\nu \geqslant (k-1) + \frac{\Delta}{2}$, где Δ — интервал квантования. Любая k-значная функция n переменных записывается в виде

$$f(\vec{x}) = \bigwedge_{\vec{\alpha}} f(\vec{\alpha}) + x_1^{(\alpha_1)} + x_2^{(\alpha_2)} + \cdots + x_n^{(\alpha_n)}, \tag{8.18}$$

где $f(\vec{\alpha})$ — значение функции $f(\vec{x})$ на наборе $\vec{\alpha}$ $(f(\vec{\alpha}) \neq k-1)$.

Функцию минимума $x_1 \wedge x_2$ можно реализовать с помощью инжекционных элементов таким образом, что с увеличением числа переменных не увеличивается задержка схемы. Функция суммы реализуется простым соединением проводников и, следовательно, задержки не вносит (если пренебречь временем распространения электромагнитного поля). Минимизация k-значных функций, представленных в виде (8.18), может осуществляться известными способами. Конфигурация быстродействующих параллельных структур, получающихся в результате синтеза, показана на рис. 48.

Создание и внедрение многозначной элементной базы не может пройти скачком за короткий промежуток времени. Неизбежен переходный период, когда многозначные устройства будут работать наряду с двоичными. В этой связи существенное значение приобретают вопросы стыковки многозначных устройств с двоичными, для чего разрабатываются специальные устройства с целью преобразования многозначного кода в двоичный и двоичного — в многозначный. При синтезе эти устройства можно совмещать с другими многозначными узлами и блоками, на входы которых поступают входные данные (двоичный код). Таким образом, в частности, построен умножитель двух-

разрядных двоичных чисел [34]. Выход этого умножителя четверичный (рис. 49), и дальнейшая обработка данных производится в четверичном алфавите. Значения уровней токов инжекторов заданы в относительных единицах и обозначены цифрами *1—3, 5*.

Умножитель реализует функции $f_1 : E_2 \times E_2 \to E_4$ и $f_2 : E_2 \times E_2 \to E_3$, где f_1 — функция умножения по модулю 4 (табл. 52) и f_2 — функция переноса при умножении (табл. 53). На выходе имеем двухразрядное четверичное число, представляющее собой результат умножения двоичных чисел x_2x_1 и y_2y_1. Так как в результате умножения максимальное значение старшего разряда произведения (переноса) равно $k - 2 = 4 - 2 = 2$, то формально значение этого разряда принадлежит алфавиту E_3. По такому же принципу построен и сумматор [39], но выходы у этого сумматора, как и входы, двоичные. Обработка данных внутри схемы производится в многозначном алфавите. Это обусловливает более высокое быстродействие и низкие аппаратурные затраты по сравнению с известными двоичными инжекционными сумматорами [1].

Возможно построение чисто k-значных умножителей, т. е. умножителей с k-значными входами и k-значными выходами. Примером такого множителя для $k = 4$ может служить схема, приведенная в работе [35]. На основе такого умножителя может строиться ячейка параллельного многоразрядного матричного умножителя [36, 80] основного узла устройств и систем, предназначенных для ЦОС.

Наряду с многозначными И^{2}Л схемами, в которых переменные представляются значениями токов, все более широко начинают исследоваться и применяться многозначные устройства с представлением информации в виде зарядов и напряжений. Заряды используются в качестве носителя информации в приборах с зарядовой связью (ПЗС), удобных для построения многозначных устройств, особенно последовательностного типа. Представление сигналов в виде уровней напряжения используется в многозначных устройствах, использующих МОП-технологию [212], а смешанное представление в виде токов и напряжений — в системе эмиттерно-связанной логики (ЭСЛ).

5. Передача сигналов в многозначных структурах и системах

Успехи в создании многозначных БИС вызывают повышенный интерес к информационно-вычислительным устройствам, работающим в многозначном структурном алфавите. Построение таких устройств на современных БИС с высокой степенью интеграции требует решения важного вопроса передачи сигналов в многозначных структурах и системах и связи их с системами другой значности (в частности, двоичными).

Как отмечалось, сигналы в многозначных элементах, входящих в некоторую структуру, имеют гибридный характер. Передача сигналов в пределах одного узла такой структуры обеспечивается единством базисных (а следовательно, и информационных) сигналов в данном узле, обычно представляющем собой конструктивно оформленное

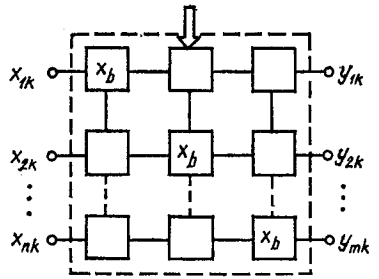


Рис. 50. Схема многозначной БИС.

устройство — БИС (рис. 50). Многозначная БИС содержит n входов и m выходов значности k, а также вход питания. Базисные величины формируются внутри БИС или даже в каждом отдельном ее элементе, а их единство является следствием одинаковости геометрических и технологических характеристик компонент и элементов, расположенных на одном кристалле.

Наряду с вопросами преобразования и передачи сигналов от элемента к элементу внутри узла многозначной структуры (БИС) при организации обмена между различными многозначными БИС возникает ряд проблем. Основная из них заключается в том, что ввиду неизбежных технологических разбросов сигналы отдельных БИС могут отличаться больше чем наполовину интервала квантования, что неизбежно приведет к сбоям и невозможности организации обмена. Существует несколько вариантов решения этой проблемы. Один из них является характерным для современного этапа. Однако, поскольку структуры этого типа не реализуют возможность уменьшения числа выводов, интересно рассмотреть вопрос передачи сигналов в структурах, где многозначными являются внутренние и внешние сигналы. Многозначная структура, содержащая ряд последовательно соединенных узлов (многозначных БИС), показана на рис. 51.

Специфика изменения уровней сигналов в многозначных БИС заключается в том, что в то время как абсолютные значения этих уровней могут изменяться довольно значительно, отношение их выдерживается обычно с достаточно высокой точностью. Это обстоятельство может быть использовано для согласования уровней сигналов в соответствии со схемой, изображенной на рис. 52. Из рисунка видно, что обычная многозначная БИС дополнена здесь двумя звеньями — эталонным элементом (обозначен звездочкой) и нормализатором N.

На эталонный элемент подается внешний базисный сигнал x_b', а выход эталонного элемента используется для управления нормализатором. В свою очередь, нормализатор осуществляет изменение питающего напряжения, поступающего на элементы (в том числе и на эталонный элемент) таким образом, чтобы свести до минимума разницу между x_b' и наибольшим значением внутриэлементного базисного сигнала x_b. При этом, если один и тот же внешний базисный сигнал поступает на все БИС многозначной структуры, изображенной на рис. 51, то первоначальная картина уровней сигналов на микросхемах с номерами i, j, l (рис. 53, *а*) трансформируется в нормализованную картину (рис. 53, *б*), т. е. происходит их выравнивание. Хотя выравнивание осуществляется только в отношении верхних уровней сигналов, ввиду соблюдения пропорциональности отношения оно выполняется одновременно и для всех остальных уровней. Тем самым оказывается возможным осуществлять обмен сигналами между различными БИС

многозначной структуры. Недостатком данного способа является необходимость регулирования по цепи питания, связанного с потерями мощности и, что наиболее существенно, с необходимостью ввода в состав каждой БИС (или в дополнение к ней) специального устройства — нормализатора. Это устройство должно быть достаточно мощным, так как питание всех отдельных элементов многозначной структуры проходит через него и, по всей видимости, конструктивно должно выполняться в виде отдельной вспомогательной микросхемы (рис. 52). Вообще говоря, нормализация может осуществляться не обязательно путем воздействия на напряжение питания, но и за счет изменения какого-либо другого параметра. Нужно только, чтобы влияние этого параметра было одинаковым для всех элементов БИС.

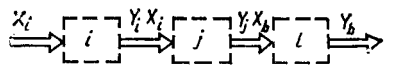


Рис. 51. Схема многозначной структуры, состоящей из последовательных узлов.

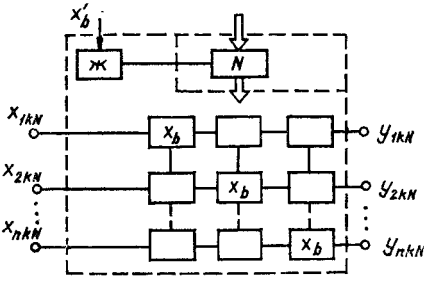


Рис. 52. Схема согласования уровней сигналов.

На примере описанной структуры мы впервые сталкиваемся с двумя типами базисных величин — внутренним базисом X_b, благодаря которому обеспечивается передача сигналов между элементами БИС, и внешним базисом X'_b, обеспечивающим обмен сигналами между БИС. В системе с эталонным элементом и нормализатором осуществляется выравнивание двух этих типов базисов, и таким образом значения сигналов как внутри БИС, так и на ее внешних выводах совпадают.

Рассмотрим другой вариант организации передачи сигналов в многозначных структурах в соответствии со схемой, показанной на рис. 54. Особенностью этой схемы является то, что в ней существуют две группы элементов — внутренние (функциональные) и внешние (на рисунке заштрихованы). Функция внешних элементов — согласование сигналов отдельных БИС многозначной структуры. Каждая из этих групп элементов имеет собственные базисные сигналы (соответственно x_b и x'_b). Связь между ними должна осуществляться по пространственному признаку p. В отличие от предыдущего случая здесь не происходит выравнивания базисов x_b и x'_b, внутренние сигналы в каждой из БИС могут, вообще говоря, отличаться как друг от друга, так и от внешних сигналов, общих для всех узлов многозначной структуры. Общая картина сигналов в многозначной структуре показана на рис. 55. Внешние сигналы представлены в промежутках между внутренними сигналами (i, j, l) каждой БИС. Поскольку для введения всех значений базисных сигналов потребовалось бы 2 (k^n — 1) вводов, здесь целесообразно ввести лишь максимальный базисный сигнал x'_b. Все остальные должны получаться из этого максимального сигнала делением с учетом оговоренного ранее обстоятельст-

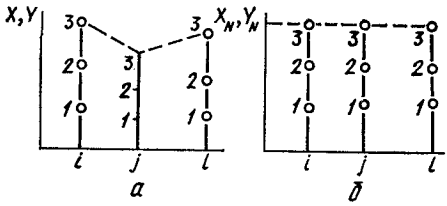
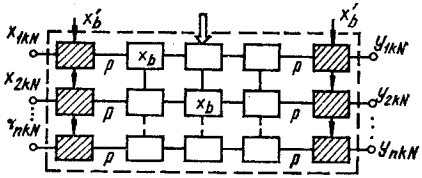
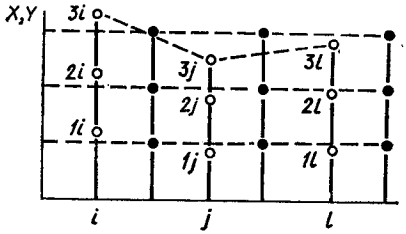


Рис. 53. Графическое изображение уровней сигналов в микросхеме.

Рис. 54. Схема передачи сигналов в многозначной структуре.

Рис. 55. Графическое изображение уровней сигналов в многозначной структуре.





ва о возможности получения с высокой точностью их отношений. Как отмечалось выше, можно также вводить все значения базисных сигналов x_b' последовательно во времени. Однако, поскольку такой вариант связан с необходимостью запоминания точных уровней этих сигналов внутри БИС, он представляется менее перспективным.

Организация передачи сигналов в многозначных (и смешанных двоично-многозначных) системах — сравнительно слабо отработанный вопрос. Определенный опыт накоплен по использованию многозначного алфавита для связи между двоичными системами с целью снижения числа соединений (рис. 56, *а*). Разработанные к настоящему времени преобразователи двоичных сигналов в k-значные ($2 \to k$) и k-значные в двоичные ($k \to 2$) могут быть использованы и для организации связи между системами разных значностей (рис. 56, *б*).

Реализацию преобразователей $2 \to k$ и $k \to 2$ можно осуществить с помощью многозначных элементов с пространственным промежуточным преобразованием. Например, преобразователь $2 \to k$ является преобразователем $p \to s$ с дешифратором $Д$, осуществляющим преобразование двоичного слова x в унитарный пространственный код, который с помощью преобразователя $p \to s$ преобразуется в многозначный код (рис. 57) [33].

Как отмечалось, один из переходных этапов при создании многозначных структур — сочетание многозначного и двоичного представления информации, которое может быть осуществлено, в частности, в соответствии со схемой рис. 58, где преобразователи $k \to 2$ и $2 \to k$ обрамляют логическую схему *2*. Последняя, являясь двоичной, функционирует в специфических условиях, в которых обычные ограничения двоичных схем не действуют или проявляются слабо. Это обусловлено в первую очередь малой длиной связей и как следствие снижением занимаемой ими площади кристалла. При создании многозначных БИС, совместимых с существующими двоичными, возможна и обратная конфигурация, когда входной и выходной преобразователи меняются местами. В этом случае логическая схема *2*

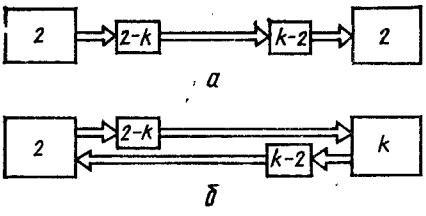


Рис. 56. Схема многозначной системы передачи сигналов.

Рис. 57. Схема преобразователя кодов.

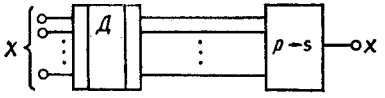
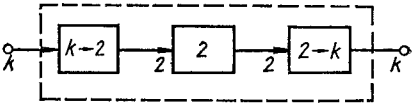


Рис. 58. Блок-схема многоуровневой системы передачи данных.



будет k-значной со всеми вытекающими последствиями в отношении внутренних соединений.

Многозначная вычислительная техника, возникающая как внутри цифровой двоичной, так и внутри аналоговой вычислительной техники, не только воспринимает лучшие качества каждой из них, но и служит важным методологическим средством, обеспечивающим понимание их диалектического единства, которое может быть обеспечено или по крайней мере облегчено при использовании языка многозначной логики. Полученные реальные выигрыши в 2—3 раза по числу соединений и быстродействию, несомненно, будут превзойдены по мере совершенствования технологии, разработки «естественных» систем синтеза, устраняющих излишние промежуточные преобразования, и накопления необходимого опыта построения многозначных структур и систем. Появление БИС для ЦОС, содержащих как аналоговые (АЦП и ЦАП), так и цифровые функциональные преобразователи, можно считать началом гибридной многозначной интегральной схемотехники, развитие которой будет сопровождаться внедрением многозначного ($\infty > k > 2$) представления информации и многозначных функциональных преобразователей.

6. Векторный процессор для ЦОС

Рассмотрим примерную архитектуру векторного процессора, ориентированного на решение задач ЦОС в реальном времени. С учетом результатов анализа реализуемых математических моделей в процессоре предусмотрена параллельная аппаратурная реализация следующих функций и операций: умножение вектора на скаляр; покомпонентное перемножение двух векторов; сумма n компонент вектора (векторно-скалярная операция); табличное функциональное преобразование данных; скалярная операция вида $y = ax + b$.

Процессор состоит из пяти основных блоков (рис. 59): входного и выходного буферных запоминающих устройств (*БЗУД1* и *БЗУД2*); непосредственно векторного процессора, включающего в себя блоки векторного оперативного запоминающего устройства (*ВОЗУ*), векторных (*БВО*), векторно-скалярных (*БВСО*) операций; устройства управления (*УУ*) и запоминающего устройства программ (*ЗУП*).

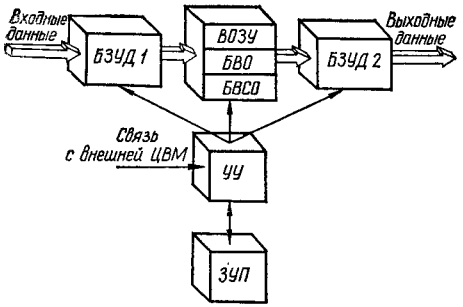


Рис. 59. Укрупненная блок-схема процессора.

Блок *БЗУД1* предназначен для согласования скорости поступления входных данных и скорости обмена данными в векторном процессоре. Причем скорость поступления входных данных может быть выше скорости обработки и обмена данными в процессоре. Однако отсчеты входных данных поступают в блок *БЗУД1* последовательно, а обработка их производится параллельно с помощью n арифметических устройств. Функция блока *БЗУД2* — обратная функции блока *БЗУД1* и заключается в параллельном считывании обработанных данных и последовательном выводе их со скоростью, равной скорости поступления.

Оперативная память и память программ разделены. Это позволяет проводить параллельно считывание или запись данных в *ВОЗУ* и считывание кода команд.

Управление осуществляется с помощью устройства управления, а также предусмотрена связь с внешней *ЦВМ* для управления процессом вычислений в рамках системы ЦОС. На рис. 59 связи управления показаны тонкими стрелками в отличие от потоков данных, которые показаны объемными стрелками.

Непосредственно векторный процессор состоит из n одинаковых блоков (n — размерность обрабатываемых векторов). Каждый блок представляет собой скалярный процессор, конфигурация которого повторяет конфигурацию векторного процессора. Для того чтобы избежать путаницы, будем векторный процессор без буферных запоминающих устройств *БЗУД1* и *БЗУД2* называть просто процессором, так как термином «векторный процессор» названо все устройство в целом, блок-схема которого показана на рис. 59; n-мерная структура процессора показана на рис. 60. Обмен данными между блоками осуществляется с помощью интерфейса, названного «*Скоростная шина*». Обмен данными между «слоями» процессора может осуществляться с помощью блока *БВСО*, может быть также предусмотрено специальное устройство.

Функциональная схема блока векторных операций (рис. 61) состоит из n устройств, каждое из которых реализует функцию $y = a \odot x \oplus b$, где $\oplus$ и $\odot$ — соответственно операция суммы и умножения по модулю $p = 2^m - 1$ (p — простое число; возможные значения $p = 2^7 - 1$, $p = 2^{13} - 1$, $p = 2^{17} - 1$ и др.), а также n логических блоков (*ЛБ*), выполняющих операции сравнения, инверсии кодов и другие логические операции. Каждое устройство, реализующее функцию вида $y = a \odot x \oplus b$, имеет входные регистры коэффициентов a, x, b и выходной регистр y, которые соединены с шинами интерфейса. Точно также каждое устройство сравнения имеет входные регистры a, b (для обозначения регистров мы употребляем

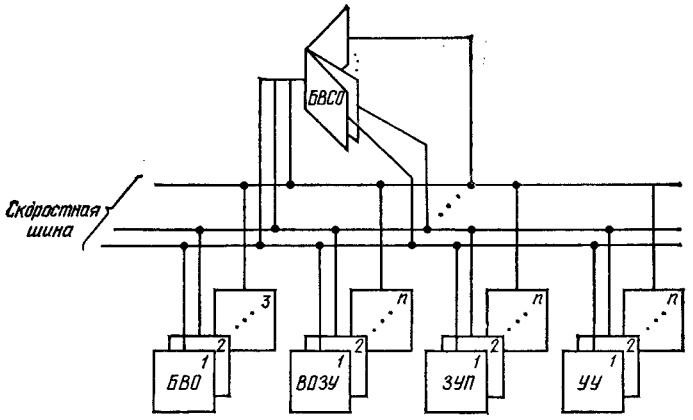


Рис. 60. Блок-схема n-мерной структуры процессора.

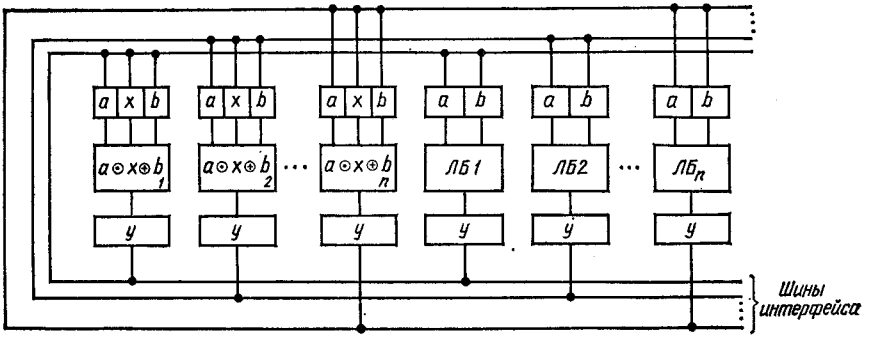


Рис. 61. Схема блока векторных операций.

те же буквы, что и для обозначения слов данных) и выходной регистр y, которые тоже соединены с шинами интерфейса. Наличие входных и выходных регистров позволяет организовать конвейерные вычисления.

Блок векторных операций можно дополнить и другими устройствами, выполняющими различные функции, что позволит более эффективно реализовать алгоритмы и упростить разработку программного обеспечения. Выбор устройств этого блока, описанный выше, обусловлен задачей эффективной реализации ортогональных преобразований (в том числе ортогональных преобразований, определенных над конечным полем или конечным кольцом) и операций над векторами в n-мерном векторном пространстве.

Блок векторно-скалярных операций представляет собой n-входовой сумматор m-разрядных слов по модулю p. С помощью n устройств, реализующих функцию вида $y = a \odot x \oplus b$ и блока векторно-скалярных операций, удобно вычислять скалярное произведение двух векторов. В этом случае перемножение n пар координат векторов осуществляется с помощью устройств, реализующих функцию

вида $y = a \odot x \oplus b$; суммирование результатов перемножения производится с помощью блока векторно-скалярных операций.

Обычные арифметические операции выполняются с помощью модульных устройств, поскольку результат модульной операции совпадает с результатом обычной арифметической операции при соответствующем масштабировании входных операторов. Сдвиги и округления осуществляются с помощью логических блоков.

Векторное *ОЗУ* состоит из n одинаковых секций, куда записываются результаты промежуточных вычислений.

Описанное архитектурное решение можно отнести к типу «один поток команд — множество потоков данных» [55, 105]. Других особенностей архитектура векторного процессора не имеет. Таким образом, введение модульных арифметических устройств вместо обычных не приводит к каким-нибудь существенным изменениям архитектуры процессоров ЦОС. Однако расширяются их функциональные возможности за счет эффективной реализации математических моделей ЦОС, определенных над конечными полями и кольцами.

* * *

В плане аппаратурной реализации математические модели, определенные над конечными полями или кольцами, не являются альтернативой классическим моделям и могут быть реализованы с помощью обычных ЦВМ, ориентированных на решение задач ЦОС. Однако реализация моделей будет более эффективной, если в ЦВМ арифметические операции конечных полей или колец (модульные операции) реализуются не программным, а аппаратурным путем. Для этого нет необходимости снабжать ЦВМ еще одним арифметическим устройством. Потребуется только расширение функциональных возможностей имеющегося арифметического устройства за счет реализации модульных операций, так как обычные арифметические операции и модульные можно совместить при реализации в одном устройстве. Оказалось, что характеристики модульных устройств улучшаются при переходе к системам счисления, в которых представляются элементы конечных полей или колец и сам модуль, с более высоким основанием (бóльшим двойки). В этой связи особый интерес для ЦОС представляют многозначные элементы и структуры, так как аппаратурная реализация будет наиболее эффективной, когда значность (число устойчивых состояний) элементной базы совпадает с основанием системы счисления.

Современные многозначные структуры являются существенно гибридными, реализующими одновременное использование аналоговых и цифровых (в том числе двоичных) элементарных операций. Многозначное представление информации дает возможность добиться оптимального соотношения между стабильностью квантованных цифровых и высокой информационной плотностью аналоговых сигналов. В результате получаются выигрыши по быстродействию и числу межсхемных соединений, что позволит поднять аппаратные средства для ЦОС на качественно более высокую ступень.

СПИСОК ЛИТЕРАТУРЫ

1. *Аваев Н. А., Дулин В. Н., Наумов Ю. Е.* Большие интегральные схемы с инжекционным питанием.— М. : Сов. радио, 1977.— 248 с.
2. *Агарвал Р. С., Баррас Ч. С.* Теоретико-числовые преобразования для быстрого вычисления цифровой свертки.— ТИИЭР, 1975, 63, № 4, с. 6—20.
3. *Агарвал Р. К., Кули Дж. У.* Новые алгоритмы для цифровой свертки.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 91—117.
4. *Агарвал Р. С., Баррас Ч. С.* Алгоритм быстрого вычисления цифровой одномерной свертки на основе многомерных методов.— Там же, с. 172—186.
5. *Агарвал Р. С., Баррас Ч. С.* Быстрая свертка, использующая преобразования с числами Ферма, и ее применение в цифровой фильтрации.— Там же, с. 156—172.
6. *Акушский И. Я., Амербаев В. М., Пак И. Т.* Основы машинной арифметики комплексных чисел.— Алма-Ата : Наука, 1970.— 248 с.
7. *Акушский И. Я., Юдицкий Д. И.* Машинная арифметика в остаточных классах.— М. : Сов. радио, 1968.— 439 с.
8. *Александров П. С.* Введение в теорию групп.— М. : Наука, 1980.— 144 с.
9. *Алексеенко В. И.* Реализация функционально-полной системы операций алгебры многозначной логики (Айзенберга — Рабиновича).— В кн.: Теория кодирования и оптимизация сложных систем. Алма-Ата : Наука, 1977, с. 41—47.
10. *Алексеенко В. И.* Функции алгебры многозначной логики, реализующие модульные операции над кодами в остатках.— Там же, с. 33—41.
11. *Аллен Дж.* Архитектура ЭВМ для обработки сигналов.— ТИИЭР, 1975, 63, № 4, с. 96—107.
12. *Ахмед Н., Рао К. Р.* Ортогональные преобразования при обработке цифровых сигналов.— М. : Связь, 1980.— 248 с.
13. *Ахо А., Хопкрофт Дж., Ульман Дж.* Построение и анализ вычислительных алгоритмов.— М. : Мир, 1979.— 536 с.
14. *Беллман Р.* Введение в теорию матриц.— М. : Наука, 1976.— 352 с.
15. *Белоглазова О. В., Лабунец В. Г.* Теория и применение преобразований Гаусса — Рейдера.— Изв. АН СССР. Техн. кибернетика, 1981, № 2, с. 193—200.
16. *Бендат Дж., Пирсол А.* Применение корреляционного и спектрального анализа.— М. : Мир, 1983.— 312 с.
17. *Березенко А. И., Ланнэ А. А., Осокин Ю. В., Страутманис Г. Ф.* Современное состояние разработок СБИС для цифровой обработки сигналов.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 243—246.
18. *Билинский И. Я., Микелсон А. К.* Стохастическая цифровая обработка непрерывных сигналов.— Рига : Зинатне, 1983.— 292 с.
19. *Блейксли Т. Р.* Проектирование цифровых устройств с малыми и большими интегральными схемами.— Киев : Вища шк., 1981.— 336 с.

20. *Бобров А. Е., Кметь А. Б., Костянко Н. Ф. и др.* О многозначных логических сетях.— В кн.: Многозначные машины и системы. Киев : Наук. думка, 1976, с. 21—51.
21. *Бобров А. Е.* Многозначные многофункциональные структуры.— Там же, с. 75—84.
22. *Боревич З. И., Шафаревич И. Г.* Теория чисел.— М. : Наука, 1972.— 495 с.
23. *Бриллинджер Д.* Временные ряды : Обраб. данных и теория.— М. : Мир, 1980.— 536 с.
24. *Букатова И. Л., Елинсон М. И., Крапивин В. А. и др.* Некоторые вопросы развития ЭВМ будущих поколений.— М., 1976.— 32 с.— (Препринт / АН СССР. Ин-т ИРЭ; № 11/217).
25. *Вайнштейн, Оппенгейм А.* Сравнение шумов округления цифровых фильтров при их реализации по методу с плавающей запятой и по методу с фиксированной запятой.— ТИИЭР, 1969, 57, № 7, с. 72—74.
26. *Вандер Варден Б. Л.* Алгебра.— М. : Наука, 1980.— 624 с.
27. *Вариченко Л. В.* Ортогональные разложения булевых функций над полем комплексных чисел и полями Галуа.— Львов, 1979.— с. 23—26. Рукопись деп. в ВИНИТИ, № 993—79 Деп.
28. *Вариченко Л. В.* Повышение точности алгоритмов цифровой обработки сигналов с помощью вычислений в конечных полях.— В кн.: Применение ортогональных методов при обработке сигналов и анализа систем. Свердловск : УПИ, 1981, с. 111—117.
29. *Вариченко Л. В.* Разработка и исследование высокоэффективных специализированных многозначных устройств для цифровой обработки сигналов : Автореф. дис. ... канд. техн. наук.— Львов, 1982.— 24 с.
30. *Вариченко Л. В., Дунец Р. Б., Раков М. А., Томин Ю. А.* Принципы построения процессоров для цифровой обработки сигналов.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 270—273.
31. *Вариченко Л. В., Жабин В. И., Коноплянко З. Д. и др.* А. с. 1016779 (СССР). Вычислительное устройство.— Опубл. в Б. И., 1983, № 17.
32. *Вариченко Л. В., Коноплянко З. Д.* Параллельное вычисление степенных полиномов с помощью специализированных вычислительных устройств.— В кн.: Методы распараллеливания в применении к задачам отбора и параллельной обработки информации в реальном времени. Докл. Всесоюз. шк.-семинара по распараллеливанию обраб. информ. (Львов, февр. 1981 г.) : Тез. докл. Львов : 1981, с. 22—24. (Препринт / АН УССР. Ин-т. ФМИ; № 43).
33. *Вариченко Л. В., Коноплянко З. Д., Раков М. А.* Вопросы построения многоуровневой системы передачи данных.— В кн.: Всесоюз. конф. по измерит. информ. системам (Львов, окт. 1981 г.) : Тез. докл. Львов : ВНИИМИУС, 1981, с. 24—25.
34. *Вариченко Л. В., Коноплянко З. Д., Раков М. А.* А. с. 894704 (СССР). Умножитель двухразрядных двоичных чисел инжекционного типа.— Опубл. в Б. И., 1981, № 48.
35. *Вариченко Л. В., Коноплянко З. Д., Раков М. А.* А. с. 928651 (СССР). Умножитель четверичный инжекционного типа.— Опубл. Б. И., 1982, № 18.
36. *Вариченко Л. В., Лапшинов О. Н.* Элементарная ячейка параллельного многозначного умножителя И²Л-типа.— Микроэлектроника, 1980, 9, вып. 5, с. 423—432.
37. *Вариченко Л. В., Раков М. А.* Исследование изоморфизмов спектральных разложений функций k-значной логики над бесконечными и конечными полями.— В кн.: Многозначная информационно-вычислительная техника. Киев : ИК АН УССР, 1979, с. 3—12.
38. *Вариченко Л. В., Раков М. А.* К исследованию изоморфизмов спектральных разложений функций алгебры логики.— В кн.: Моделирующие системы с многозначным и гибридным кодированием. Киев : Наук. думка, 1980, с. 34—38.
39. *Вариченко Л. В., Раков М. А. А.* с. 892730 (СССР). Полный одноразрядный сумматор инжекционного типа.— Опубл. Б. И., 1981, № 47.

40. *Вариченко Л. В., Раков М. А.* Принципы построения многозначных процессоров для параллельной обработки данных.— В кн.: Параллельные машины : Тез. докл. Киев, 1980, с. 23—24. (Препринт / АН УССР. Ин-т ИЭД; 223).
41. *Вариченко Л. В., Раков М. А.* Спектральный синтез многозначных вычислительных структур над конечными и бесконечными полями.— Автоматика и вычисл. техника, 1981, № 1, с. 25—28.
42. *Введение* в кибернетическую технику : Обработка физической информации / Под ред. Б. Н. Малиновского.— Киев : Наук. думка, 1979.— 256 с.
43. *Вейцман К.* Распределенные системы мини- и микро-ЭВМ.— М. : Финансы и статистика, 1982.— 332 с.
44. *Виленкин С. Я.* Статистическая обработка результатов исследования случайных функций.— М. : Энергия, 1979.— 320 с.
45. *Виноград С.* О билинейных формах, мультипликативная сложность которых зависит от поля констант.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 225—233.
46. *Виноград С.* О вычислении дискретного преобразования Фурье.— Там же, с. 117—136.
47. *Виноградов И. М.* Основы теории чисел.— М. : Наука, 1981.— 176 с.
48. *Воеводин В. В.* Линейная алгебра.— М. : Наука, 1980.— 400 с.
49. *Вольперт Л. А., Гуревич М. Х., Кузнецов А. А., Страутманис Г. Ф.* Усовершенствованная структура СБИС цифрового процессора обработки сигналов с аналоговыми устройствами ввода/вывода.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 251—253.
50. *Гаусс К. Ф.* Труды по теории чисел.— М. : Физматгиз, 1959.— 560 с.
51. *Гивенталь А. Б., Кренкель Т. Э.* Теоретико-числовое преобразование Френеля и его применение в цифровой обработке многомерных массивов данных.— В кн.: Цифровая обработка сигналов и ее применения. М. : Наука, 1981, с. 23—32.
52. *Гилл А.* Линейные последовательностные машины.— М. : Наука, 1974.— 288 с.
53. *Глазунов М. Н.* Об одной математической машине, ориентированной на исследование диофантовых уравнений.— В кн.: Вычисления в алгебре, теории чисел и комбинаторике. Киев : ИК АН УССР, 1980, с. 32—40.
54. *Глушков В. М.* Основы безбумажной информатики.— М. : Наука, 1982.— 552 с.
55. *Головкин Б. А.* Параллельные вычислительные системы.— М. : Наука, 1980.— 520 с.
56. *Грибанов Ю. И., Мальков В. Л.* Выборочные оценки спектральных характеристик стационарных случайных процессов.— М. : Энергия, 1978.— 149 с.
57. *Гуд И. Дж.* О взаимоотношении между двумя быстрыми преобразованиями Фурье.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 136—147.
58. *Дадаев Ю. Г.* Теория арифметических кодов.— М. : Радио и связь, 1981.— 272 с.
59. *Демидович Б. П., Марон И. А.* Основы вычислительной математики.— М. : Наука, 1970.— 664 с.
60. *Джайн А. К.* Успехи в области математических моделей для обработки изображений.— ТИИЭР, 1981, 69, № 5, с. 9—39.
61. *Драган Я. П.* Модели сигналов в линейных системах.— Киев : Наук. думка, 1972.— 303 с.
62. *Драган Я. П.* Структура и представление моделей стохастических сигналов.— Киев : Наук. думка, 1980.— 384 с.
63. *Дуда Р., Харт П.* Распознавание образов и анализ сцен.— М. : Мир, 1976.— 512 с.
64. *Евреинов Э. В.* Однородные вычислительные системы, структуры и среды.— М. : Радио и связь, 1981.— 208 с.
65. *Ершов Ю. Л., Палютин Е. А.* Математическая логика.— М. : Наука, 1979.— 320 с.

66. *Игнатов В. А.* Теория информации и передачи сигналов.— М. : Сов. радио 1979.— 280 с.
67. *Каляев А. В., Пузенков Н. А.* Перспективы развития цифровых процессоров обработки сигналов.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 247—250.
68. *Кантор И. Л., Солодовников А. С.* Гиперкомплексные числа.— М. : Наука, 1973.— 144 с.
69. *Карцев М. А.* Арифметика цифровых машин.— М. : Наука, 1969.— 576 с.
70. *Карцев М. А., Брик В. А.* Вычислительные системы и синхронная арифметика.— М. : Радио и связь, 1981.— 360 с.
71. *Каппелини В., Константинидис А. Дж., Эмилиани П.* Цифровые фильтры и их применение.— М. : Энергоатомиздат, 1983.— 360 с.
72. *Касами Т., Токура Н., Ивадари Е., Инагаки Я.* Теория кодирования.— М. : Мир, 1978.— 576 с.
73. *Климова Е. В., Коваленко Л. Г., Кухарев Г. А., Скорняков В. С.* Особенности алгоритмической и аппаратурной реализации дискретных преобразований Фурье в базисе комплексных прямоугольных функций.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 15—18.
74. *Клиффорд А., Престон Г.* Алгебраическая теория полугрупп.— М. : Мир, 1972.— Т. 1. 286 с.
75. *Кметь А. Б., Раков М. А., Ланцов А. Л.* Вопросы построения и организации многозначных элементов и структур.— В кн.: Многозначные элементы и структуры. Киев : Наук. думка, 1976, с. 3—21.
76. *Коксетер Г. С. М., Мозер У. О. Дж.* Порождающие элементы и определяющие соотношения дискретных групп.— М. : Наука, 1980.— 240 с.
77. *Колба Д. П., Паркс Т. У.* Алгоритм БПФ для простых множителей, использующий быструю свертку.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 72—89.
78. *Колмогоров Г. С., Лабунец В. Г.* Новый быстрый алгоритм для косинусного преобразования.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 55—58.
79. *Корн Г. и Корн Т.* Справочник по математике для научных работников и инженеров.— М. : Наука, 1974.— 832 с.
80. *Корнейчук В. И., Тарасенко В. П.* Синтез комбинационных множительных схем из многозначных логических элементов.— Изв. АН СССР. Техн. кибернетика, 1968, № 6, с. 50—54.
81. *Кострыкин А. И.* Введение в алгебру.— М. : Наука, 1977.— 296 с.
82. *Крылов В. В., Херманис Э. А.* Модели систем обработки сигналов.— Рига : Зинатне, 1981.— 212 с.
83. *Кузин А. Т.* Основы кибернетики.— М. : Энергия, 1979.— Т. 2. 584 с.
84. *Кузьмин И. В., Кедрус В. А.* Основы теории информации и кодирования.— Киев : Вища шк., 1977.— 280 с.
85. *Курош А. Г.* Лекции по общей алгебре.— М. : Наука, 1973.— 400 с.
86. *Кэртис Ч., Райнер И.* Теория представлений конечных групп и ассоциативных алгебр.— М. : Наука, 1969.— 668 с.
87. *Лабунец В. Г.* Единый подход к алгоритмам быстрых преобразований.— В кн.: Применение ортогональных методов при обработке сигналов и анализа систем. Свердловск : УПИ, 1980, с. 4—14.
88. *Лабунец В. Г.* Обобщенные преобразования Хаара.— В кн.: Многозначные элементы, структуры, системы. Киев : Наук. думка, 1983, с. 78—85.
89. *Лабунец В. Г.* Теоретико-числовые преобразования над полями алгебраических чисел.— В кн.: Применение ортогональных методов при обработке сигналов и анализе систем. Свердловск : УПИ, 1981, с. 44—54.
90. *Лабунец В. Г.* Фурье — подобные преобразования.— Там же, с. 4—14.
91. *Лабунец В. Г., Ситников О. П.* Гармонический анализ булевых функций и функций *К*-значной логики над конечными полями.— Изв. АН СССР. Техн. кибернетика, 1975, № 1, с. 141—148.

92. *Лабунец В. Н., Ситников О. П.* Обобщенные и быстрые преобразования Фурье на произвольной конечной абелевой группе.— В кн.: Гармонический анализ на группах в абстрактной теории систем. Свердловск : УПИ, 1976, с. 24—43.
93. *Ланнэ А. А., Титов М. А.* Принципы построения реализационного базиса цифровой обработки сигналов.— В кн.: Методы и микроэлектронные средства цифрового преобразования и обработки сигналов : Тез. докл. Рига : ИЭВТ АН ЛатвССР, 1983, ч. 2, с. 4—7.
94. *Ланцов А. Л.* Синтез многозначных потенциальных схем с инжекционным питанием.— Автоматика и вычисл. техника, 1979, № 4, с. 83—88.
95. *Лейбовиц Л. М.* Упрощенная двоичная арифметика для преобразования с числами Ферма.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 202—207.
96. *Ленг С.* Алгебра.— М. : Мир, 1968.— 564 с.
97. *Лиу Б., Канеко Т.* Анализ погрешностей цифровых фильтров, реализуемых арифметическими операциями с плавающей запятой.— ТИИЭР, 1969, **57**, № 10, с. 49—63.
98. *Макклеллан Дж. Х.* Аппаратурная реализация преобразования Ферма.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 186—202.
99. *Макклеллан Дж. Х., Рейдер Ч. М.* Применение теории чисел в цифровой обработке сигналов.— М. : Радио и связь, 1983.— 264 с.
100. *Макс Ж.* Методы и техника обработки сигналов при физических измерениях.— М. : Мир, 1983.— Т. 1. 312 с.
101. *Мальцев А. И.* Алгебраические системы.— М. : Наука, 1970.— 392 с.
102. *Микроэлектронные* цифро-аналоговые и аналого-цифровые преобразователи информации / Под ред. В. Б. Смолова.— Л. : Энергия, 1976.— 336 с.
103. *Многозональные* аэрокосмические съемки Земли.—М. : Наука, 1981.— 304 с.
104. *Моисеев Н. Н.* Математические задачи системного анализа.— М. : Наука, 1981.— 488 с.
105. *Мультипроцессорные* системы и параллельные вычисления / Под ред. Ф. Г. Энслоу.— М. : Мир, 1976.— 383 с.
106. *Мухопад Ю. Ф.* Проектирование специализированных микропроцессорных вычислений.— Новосибирск : Наука, 1981.— 161 с.
107. *Надежность* многозначных структур / В. В. Григорьев, А. Б. Кметь, З. Д. Коноплянко и др.— Киев : Наук. думка, 1981.— 176 с.
108. *Наймарк М. А.* Теория представлений групп.— М. : Наука, 1976.— 560 с.
109. *Нечаев В. И.* Числовые системы.— М. : Просвещение, 1975.— 199 с.
110. *Норкин К. Б.* Специализированные гибридные управляюще-вычислительные устройства.— М. : Энергия, 1980.— 288 с.
111. *Нусбаумер Х.* Цифровая фильтрация с помощью комплексных преобразований Мерсенна.— В кн.: Макклеллан Дж., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 216—225.
112. *Обработка* изображений и цифровая фильтрация / Под ред. Т. Хуанга.— М. : Мир, 1979.— 320 с.
113. *Омельченко В. А.* Основы спектральной теории распознавания сигналов.— Харьков : Вища шк., 1983.— 156 с.
114. *Оппенгейм А., Вайнштейн.* Влияние конечной длины регистра при цифровой фильтрации и быстром преобразовании Фурье.— ТИИЭР, 1972, **60**, № 8, с. 41—65.
115. *Оппенгейм А. В., Шафер Р. В.* Цифровая обработка сигналов.— М. : Связь, 1979.— 416 с.
116. *Оппенгейм А., Шафер Р., Стокхэм Т.* Нелинейная фильтрация сигналов, представленных в виде произведения и свертки.— ТИИЭР, 1968, **56**, № 8, с. 5—34.
117. *Орнатский П. П.* Теоретические основы информационно-измерительной техники.— Киев : Вища шк., 1983.— 455 с.
118. *Отнес Р., Эноксон Л.* Прикладной анализ временных рядов.— М. : Мир, 1982.— 428 с.

119. *Парлетт Б.* Симметричная проблема собственных значений. Численные методы.— М. : Мир, 1983.— 384 с.
120. *Пелед А., Лиу Б.* Цифровая обработка сигналов.— Киев : Вища шк., 1979.— 264 с.
121. *Перестраиваемые* цифровые структуры на основе интегрирующих процессоров / А. Г. Алексеенко, А. В. Каляев, В. И. Лукиенко и др.— М. : Радио и связь, 1982.— 368 с.
122. *Пешель М.* Моделирование сигналов и систем.— М. : Мир, 1981.— 302 с.
123. *Пойа Д.* Математика и правдоподобные рассуждения.— М. : Наука, 1975.— 464 с.
124. *Поллард Дж. М.* Быстрое преобразование Фурье в конечном поле.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 147—155.
125. *Поса Дж.* Цифровые процессоры аналоговых сигналов — новое направление интегральной техники.— Электроника, 1980, № 4, с. 93—96.
126. *Применение* ортогональных методов при обработке сигналов и анализе систем.— Свердловск : УПИ, 1980.— Вып. 1. 128 с.
127. *Применение* цифровой обработки сигналов / Под ред. А. Оппенгейма.— М. : Мир, 1980.— 552 с.
128. *Пролейко В. М.* Развитие микропроцессоров, микро-ЭВМ и систем на их основе.— Электрон. пром-сть, 1979, № 11/12, с. 3—6.
129. *Прэтт У.* Цифровая обработка изображений.— М. : Мир, 1982.— Кн. 1. 312 с.
130. *Прэтт У.* Цифровая обработка изображений.— М. : Мир, 1982.— Кн. 2. 480 с.
131. *Пухов Г. Е., Бардаченко В. Ф., Королев Ю. В.* Вычислительные устройства на скаляторах.— Киев : Техніка, 1983.— 145 с.
132. *Пухов Г. Е.* Построение разрядно-аналоговых функциональных преобразователей из разрядных матриц.— В кн.: Неоднородные вычислительные системы. Киев : Наук. думка, 1975, с. 68—76.
133. *Пчелин Б. К.* Специальные разделы высшей математики.— М. : Высшая шк., 1973.— 461 с.
134. *Рабинер Л. Р., Гоулд Б.* Теория и применение цифровой обработки сигналов.— М. : Мир, 1978.— 848 с.
135. *Рабинер Л. Р., Шафер Р. В.* Цифровая обработка речевых сигналов.— М. : Радио и связь, 1981.—496 с.
136. *Раков М. А.* Вычислительные устройства и многозначное представление информации.— Микроэлектроника, 1984, **13**, вып. 2, с. 99—106.
137. *Раков М. А., Кметь А. Б.* Реализация многозначных систем управления.— В кн.: V Всесоюз. совещ. по пробл. упр. (Москва, май 1971 г.) : Тез. докл. М. : Наука, 1971, ч. 3, с. 56—58.
138. *Раков М. А.* Многозначные структуры и аналого-цифровые методы обработки информации.— В кн.: Исследование в области системных измерений. Львов, 1981, с. 82—95.
139. *Раков М. А.* Многозначные структуры и перспективы развития информационно-вычислительной техники.— Львов, 1982.— 70 с.— (Препринт АН УССР. Ин-т ФМИ; № 66).
140. *Раков М. А.* О путях построения элементов с большим количеством устойчивых состояний.— В кн.: IV Всесоюз. совещ. по автомат. упр. (техн. кибернетике), (Москва, 1968 г.) : Тез. докл. М. : Наука, 1968, ч. 2, с. 18—19.
141. *Раков М. А.* Реалізація багатозначних елементів та структур.— Вісн. АН УРСР, 1976, № 1, с. 26—34.
142. *Раков М. А.* Реализация многозначных элементов и структур.— В кн.: Вычислительная техника и энергетика. Киев : Наук. думка, 1974, с. 64—76.
143. *Раков М. А., Страздинь И. Э.* Преобразование сигналов в цифровых многозначных структурах.— Автоматика и вычисл. техника, 1982, № 4, с. 56—62.
144. *Раков М. А.* Частотно-фазовые многоустойчивые элементы автоматики : Автореф. дис. ... д-ра техн. наук.— М., 1970.— 48 с.
145. *Реализация* многозначных структур автоматики / Под ред. М. А. Ракова.— Киев : Наук. думка, 1976.— 350 с.

146. *Ридер К., Хаббл Л.* Направления развития видеодисплейных систем.— ТИИЭР, 1981, 69, № 5, с. 134—145.
147. *Рид И. С., Троун Т. К.* Применение конечных полей для вычисления сверток.— В кн.: Макклеллан Дж. Х., Рейдер Ч. М. Применение теории чисел в цифровой обработке сигналов. М. : Радио и связь, 1983, с. 207—216.
148. *Розенфельд А.* Распознавание и обработка изображений с помощью вычислительных машин.— М. : Мир, 1972.— 230 с.
149. *Самофалов К. Г., Корнейчук В. И., Тарасенко В. П.* Электронные цифровые вычислительные машины.— Киев : Вища шк., 1976.— 480 с.
150. *Свенсон А. Н., Смердов А. А.* Системы передачи информации со статистическим усреднением.— Киев : Наук. думка, 1967.— 228 с.
151. *Синьков М. В., Ващенко В. Ф., Губарени Н. М.* Фундаментальная теорема для биквадриплексных чисел.— Мат. моделирование и теория электр. цепей, 1978, вып. 16, с. 84—86.
152. *Синьков М. В., Ващенко В. Ф.* Теоретико-числовые свойства биквадриплексных чисел.— Гибрид. вычисл. машины и комплексы, 1979, вып. 1, с. 48—52.
153. *Смолов В. Б., Байков В. Д.* Анализ погрешности вычисления на СЦВМ элементарных функций.— Точность и надежность кибернет. систем, 1974, вып. 2, с. 65—68.
154. *Смолов В. Б.* Функциональные преобразователи информации.— Л. : Энергоиздат, 1981.— 248 с.
155. *Специализированные* многозначные анализаторы / Под ред. М. А. Ракова.— Киев : Наук. думка, 1977.— 172 с.
156. *Специализированные* ЦВМ / Под ред. В. Б. Смолова.— М. : Высш. шк., 1981.— 279 с.
157. *Справочник* по интегральным микросхемам / Под ред. Б. В. Тарабрина.— М. : Энергия, 1980.— 816 с.
158. *Степанов С. А.* Сравнения.— М. : Знание, 1975.— 62 с.
159. *Стокхэм Т., Кэннон Т., Ингебретсен Р.* Цифровое восстановление сигналов посредством неопределенной инверсной свертки.— ТИИЭР, 1975, 63, № 4, с. 160—177.
160. *Трахтман А. М., Трахтман В. А.* Основы теории дискретных сигналов на конечных интервалах.— М. : Сов. радио, 1975.— 208 с.
161. *Ту Дж., Гонсалес Р.* Принципы распознавания образов.— М. : Мир, 1978.— 412 с.
162. *Турмухамбетов Р. Н.* К вопросу о построении непозиционной системы счисления в кольце кватернионов.— В кн.: Теория кодирования и оптимизация ложных систем. Алма-Ата : Наука, 1977, с. 214—218.
163. *Турмухамбетов Р. Н.* Системы счисления с кватернионными основаниями $\pm 1 \pm i$, $\pm 1 \pm j$, $\pm 1 \pm k$.— Там же, с. 211—214.
164. *Файзулаев Б. Н.* Предельное быстродействие и основные закономерности развития БИС ЭВМ.— Микроэлектрон. и полупроводниковые приборы, 1982, вып. 7, с. 12—18.
165. *Фараджев Р. Г.* Аналитические способы вычисления процессов в линейных последовательностных машинах.— Изв. АН СССР. Техн. кибернетика, 1965, № 5, с. 74—80.
166. *Фараджев Р. Г.* Линейные последовательностные машины.— М. : Наука, 1975.— 160 с.
167. *Фараджев Р. Г., Цыпкин Я. З.* Преобразование Лапласа — Галуа в теории последовательностных машин.— Докл. АН СССР, 1966, 166, № 3, с. 45—52.
168. *Федорів Р. Ф.* Статистична радіометрія.— К. : Наук. думка, 1979.— 264 с.
169. *Фирма* Signetics планирует выпуск четырехуровневых логических схем.— Электроника, 1976, 49, № 22, с. 3—5.
170. *Френкс Л.* Теория сигналов.— М. : Сов. радио, 1974.— 344 с.
171. *Фрини Д.* Специализированные аппаратные средства для цифровой фильтрации.— ТИИЭР, 1975, 63, № 4, с. 108—125.
172. *Хармут Х.* Теория секвентного анализа. Основы и применения.— М. : Мир, 1980.— 575 с.
173. *Цикин И. А.* Дискретно-аналоговая обработка сигналов.— М. : Радио и связь, 1982.— 160 с.

174. *Цифровая* обработка сигналов и ее применение.— М. : Наука, 1981.— 223 с.
175. *Цифровые* многозначные элементы и структуры / К. Г. Самофалов, В. И. Корнейчук, А. М. Романкевич, В. П. Тарасенко.— Киев : Вища шк., 1974.— 168 с.
176. *Цыпкин Я. З.* Теория линейных импульсных систем.— М. : Физматгиз, 1963.— 968 с.
177. *Шефер Р., Рабинер Л.* Цифровое представление речевых сигналов.— ТИИЭР, 1975, 63, № 4, с. 141—159.
178. *Эдвардс Г.* Последняя теорема Ферма. Генетическое введение в алгебраическую теорию чисел.— М. : Мир, 1980.— 485 с.
179. *Яблонский С. В.* Введение в дискретную математику.— М. : Наука, 1979.— 272 с.
180. *Ярославский Л. П.* Введение в цифровую обработку изображений.— М. : Сов. радио, 1979.— 312 с.
181. *Ярославский Л. П., Мерзляков Н. С.* Методы цифровой голографии.— М. : Наука, 1977.— 192 с.
182. *Agarwal R. C., Burrus C. S.* Fast one-dimensional digital convolution by multidimensional techniques.— IEEE Trans. Acoust. Speech and Signal Proc., 1974, 22, N 1, p. 1—10.
183. *Briggs F. A., Fu K—S., Hwang K., Wah B. W.* PUMPS architecture for pattern analysis and image database management.— IEEE Trans. Comput., 1982, 31, N 10, p. 969—983.
184. *Dao T. T., McCluskey E. J., Russel L. K.* Multivalued integrated injection logic.— Ibid., 1977, 26, N 12, p. 1233—1241.
185. *Dao T. T.* Recent multivalued circuits.— Proc. IEEE COMPCON, 1981, Spring, p. 194—203.
186. *Davio M., Deschamps J.— P.* Synthesis of discrete function using I^2L technology.— IEEE Trans. Comput., 1981, 30, N 9, p. 653—661.
187. *Davio M., Deschamps J.— P., Thayse A.* Discrete and switching functions.— McGraw — Hill Intern. Book Co. New-York, 1978.— 729 p.
188. *Dubois E., Venetsanopoulos A. N.* Number theoretic transforms with Modulos $2^{2q} - 2^q + 1$.— In: IEEE Intern. conf. acoust., speech and signal proc. record, Tulusa, Okl. Apr. 10—12, 1978, p. 623—627.
189. *Dubois E., Venetsanopoulos A. N.* The discrete fourier transform over finite rings with application to fast convolution.— IEEE Trans. Comput., 1978, 27, N 7, p. 586—593.
190. *Dubois E., Venetsanopoulos A. N.* The generalized discrete fourier transform in rings of algebrais integers.— IEEE Trans. Acoust. Speech and Signal Proc., 1980, 28, N 2, p. 169—175.
191. *Etiemble D.* TTL circuits for a 4-valued bus (a way to reduce package and interconnetions).— In: Proc. 8th Intern. symp. multiple — valued logic, 1978, May. New-York, 1978, p. 7—12.
192. *Golomb S. W.* Propertics of the sequence $3 \cdot 2^n + 1$.— Math. Comput., 1976, 30, N 135, p. 657—663.
193. *Herlestam T., Johannsson R.* On computing logarithms over CF (2^p).— BIT, 1981, 21, p. 326—334.
194. *Ikihiko Ichizuka.* Synthesis of multivalued miltithreshold networks for applying I^2L circuits.— In: Proc. 9th Intern. symp. multiple valued logic. Bath, 1979, p. 67—76.
195. *Martens J.— B., Vanwormhoudt M. C.* Convolution of long integer sequences by means of number theoretic transforms over residue class polynomial rings.— IEEE Trans. Acoust., Speech, and Signal Proc., 1983, 31, N 5, p. 1125—1134.
196. *Martens J.— B., Vanwormhoudt M. C.* Convolution using a conjugate Symmetry property for number theoretic transforms over rings of regular integers.— Ibid., p. 1121—1124.
197. *McCluskey E. J.* Logic design of multivalued I^2L logic circuits.— IEEE Trans. Comput., 1979, 28, p. 546—559.
198. *Miller R. L., Reed I. S., Troung T. K.* A theorem for computing primitive elements in the field of complex integers of characteristic mersenne prime.— IEEE Trans. Acoust., Speech and Signal Proc., 1981, 29, N 1, p. 119—121.

199. *Muzakami H., Reed I. S., Albert A.* Recursive FIR digital filter design using a z-transform on a finite ring.— Ibid., 1983, **31**, N 5, p. 1155—1164.
200. *Noll C., Nichel L.* The 25th and 26th mersenne primes.— Math. Comp., 1980, **35**, N 152, p. 1387—1390.
201. *Nussbaumer H. J.* Digital filtering using complex Mersenne transforms.— IBM. J. Res. Develop., 1976, **20**, N 4, p. 498—504.
202. *Nussbaumer H. J.* Fast multipliers for number theoretic transforms.— IEEE Trans. Comput., 1978, **27**, N 8, p. 764—765.
203. *Nussbaumer H. J.* New algorithms convolution and DET based on polinomial transforms.— In: IEEE Intern. conf. acoust. Speech and Signal Proc. Record. Tulusa, Okl., 1978, Apr. 10—12, p. 638—641.
204. *Pollard J. M.* The fast fourier transform in a finite field.— Math. Comput., 1971, **25**, N 114, p. 365—374.
205. *Rader C. M.* Discrete convolutions via Mersenne transforms.— IEEE Trans. Comput., 1972, **21**, p. 1269—1272.
206. *Rakov M. A., Varichenko L. V.* Principles of organization of the on — ground data processing for remote sensing purposes using finite rings and fields.— In: 34th congr. Intern. Astronaut. Fed. Oct. 10—15, 1983 Budapest, Hungary Budapest, 1983, p. 131—132 (Abstr. Pap; No IAF—83—130).
207. *Reed I. S., Troung T. K.* Complex Integer convolutions over direct sum of galois fields.— IEEE Trans. Intern. Theor., 1975, **21**, p. 657—661.
208. *Reed I. S., Troung T. K.* Fast mersenne — prime transforms for digital filtering.— IEEE, 1978, **125**, N 5, p. 433—440.
209. *Reed I. S., Troung T. K., Lin K. Y.* Fast algorithm for computing complex-number theoretic transforms.— In: National Telecommunications conference, NTC'77 Conf. Record. 1977, vol. 2, p. 29 : 4—1 — 29 : 4—3.
210. *Reed I. S., Troung T. K., Miller R. L.* A new algorithm for computing primitive elements in the field of Gaussian complex integers modulo a Mersenne prime.— IEEE Trans. Acoust. Speech and Signal Proc., 1979, **27**, N 5, p. 561—563.
211. *Schönhage A., Strassen V.* Schnelle multiplication grosser zahlen.— Computing., 1966, **7**, N 3/4, S. 281—292.
212. *Smith K. S.* The prospects for multivalued logic: a technology and applications view.— IEEE Trans. Comput., 1981, **30**, N 9, p. 619—634.
213. *Vander Kraats R. H., Venetsanopuolos A. N.* Two Dimensional Filtering using Fermat number transforms.— IEEE Intern. Conf. Acoust., Speech and Signal Proc., Pecord Tuiusa. Okl. Apr. 10—12, 1978, p. 614—618.
214. *Vegh E., Leibowitz L. M.* Fast complex convolution in finite rings.— IEEE Trans. Acoust., Speech and Signal Proc., 1976, **24**, p. 343—344.

ОГЛАВЛЕНИЕ

Леонид Викторович
ВАРИЧЕНКО

Валерий Григорьевич
ЛАБУНЕЦ

Михаил Аркадьевич
РАКОВ

АБСТРАКТНЫЕ АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ И ЦИФРОВАЯ ОБРАБОТКА СИГНАЛОВ

Утверждено к печати ученым советом Физико-механического института им. Г. В. Карпенко АН УССР

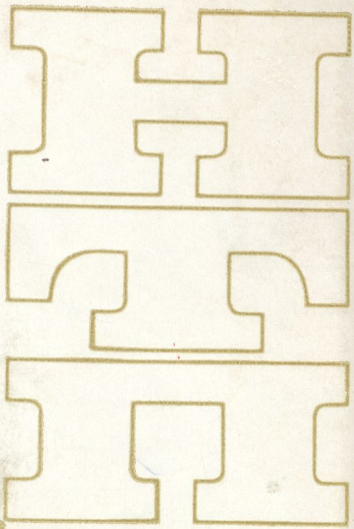
Редактор И. Г. Бобрышева
Художественный редактор И. Т. Лагутин
Технический редактор Т. С. Березяк
Корректоры Л. С. Трилевич,
Л. М. Тищенко, Р. С. Коган

ИБ № 7317

Сдано в набор 05.09.85. Подп. в печ. 18.02.86. БФ 01027
Формат 60×90/16. Бум. тип. № 1. Обыкн. нов. гарн. Выс. печ
Усл. печ. л. 15,875. Усл. кр.-отт. 17,43. Уч.-изд. л. 17,05
Тираж 1750 экз. Заказ 6-99. Цена 3 р. 40 к.

Издательство «Наукова думка».
252601 Киев 4, ул. Репина, 3.

Отпечатано с матриц Головного предприятия республи
канского производственного объединения «Полиграфкни
га». 252057 Киев, ул. Довженко, 3 на книжной фабрик
«Коммунист». 310012 Харьков, ул. Энгельса, 11.



В 1986 г. издательство «Наукова думка» выпускает в серии «Наука и технический прогресс» следующие монографии: «Прогноз и предотвращение выбросов пород и газов»; Г. А. Соколовский, В. И. Гнесин «Нестационарные трансзвуковые и вязкие течения в турбомашинах».