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

Кафедра высшей математики

В. А. Липницкий, Н. В. Спичекова

ПРИКЛАДНАЯ МАТЕМАТИКА И ТЕОРИЯ НОРМ СИНДРОМОВ

Методическое пособие
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-45 01 05 «Системы распределения мультимедийной информации»,
1-98 01 02 «Защита информации в телекоммуникациях»
заочной и дистанционной форм обучения

Минск БГУИР 2011

УДК 512(076.1)
ББК 22.144я73
Л61

Рецензент:
заведующий кафедрой информатики учреждения образования
«Белорусский государственный университет
информатики и радиоэлектроники»,
доктор физико-математических наук, профессор Л. И. Минченко

Липницкий, В. А.

Л61 Прикладная математика и теория норм синдромов: метод. пособие для студ. спец. 1-45 01 03 «Сети телекоммуникаций», 1-45 01 05 «Системы распределения мультимедийной информации», 1-98 01 02 «Защита информации в телекоммуникациях» заоч. и дист. форм обуч. / В. А. Липницкий, Н. В. Спичекова. – Минск : БГУИР, 2011. – 76 с.

ISBN 978-985-488-559-9.

Методическое пособие предназначено для практического освоения материала специальных курсов «Прикладная математика» и «Теория норм синдромов». Пособие знакомит с основными криптографическими системами и возможностями применения современной алгебры в теории и практике помехоустойчивого кодирования. Приведены теоретические сведения с примерами, задачи для аудиторной и самостоятельной работы по основам теории чисел, теории групп, теории колец и полей, их приложений для защиты информации от помех и несанкционированного доступа, контрольные работы по каждому разделу.

УДК 512(076.1)
ББК 22.144я73

ISBN 978-985-488-559-9

Содержание

Введение

Переход человечества в конце XX в. в информационную эпоху ознаменовался такими явлениями, как всеобщая компьютеризация, всесторонняя экспансия микро- и нанотехнологий, цифровых телекоммуникационных и инфокоммуникационных систем. Научной базой новых технологий явилась также и иная математика, новая, использующая широкий спектр идей и методов комбинаторики, дискретной математики, математической логики, современной алгебры и геометрии, особенно в аспектах, связанных с так называемой «конечной математикой». Конечно же, знание основ этой математики необходимо современным инженерам, занятым обслуживанием и/или разработкой современных аппаратных информационных или телекоммуникационных средств.

Решению названных задач посвящены новые курсы «Прикладная математика. Математические основы защиты информации от помех и несанкционированного доступа» и «Теория норм синдромов». Данное методическое пособие предназначено для студентов заочной и дистанционной форм обучения для самостоятельного освоения и изучения названных курсов.

Предлагаемое издание знакомит с методами и алгоритмами вычислений в кольцах классов вычетов. На этих алгоритмах строятся системы цифровой обработки сигналов, современные криптографические системы защиты информации от несанкционированного доступа. Учебные модели таких криптосистем можно изучить с помощью данного пособия. Также студенты знакомятся с методами формирования конечных полей (полей Галуа) и вычислений в них. На основе алгоритмов вычислений в полях Галуа функционируют устройства защиты информации от помех в современных телекоммуникационных системах. Студенты на практике осваивают математические алгоритмы работы названных устройств, в частности, моделей действующих систем сотовой связи.

Теория норм синдромов является новейшим результатом белорусской школы кодировщиков XXI в. Для ее освоения требуется четкое владение техникой вычислений в полях Галуа. Предложенный в пособии спектр задач позволяет усвоить основы теории норм синдромов и применять полученные знания на практике.

Каждая из двух частей пособия, соответствующая двум перечисленным курсам, завершается контрольной работой для студентов.

Часть I. Прикладная математика. Математические основы защиты информации от помех и несанкционированного доступа

Глава 1. Основы теории чисел

Теорема 1.1.1 (теорема о делении с остатком). *Для любых целых чисел* a *и* $b \neq 0$ *существуют единственные целые числа* q *и* r, $0 \le r < |b|$, *такие, что выполняется равенство:* $a = b \cdot q + r$.

Пример 1.1.1. а) пусть $a = -20,\ b = 3;$ тогда $q = -7,\ r = 1;$

б) пусть $a = -17,\ b = -5;$ тогда $q = 4,\ r = 3.$

Определение 1.1.1. Если целые числа $a_1, a_2, \ldots, a_n$ делятся на целое число d, то d называют их общим делителем. Максимальный из общих делителей целых чисел $a_1, a_2, \ldots, a_n$ называется их наибольшим общим делителем и обозначается как $НОД(a_1, a_2, ..., a_n)$.

Теорема 1.1.2. *Если* $a = b \cdot q + c$, *то* $\text{НОД}(a, b) = \text{НОД}(b, c)$.

Теорема 1.1.2 позволила Евклиду (примерно 2300 лет тому назад) обосновать следующий факт.

Теорема 1.1.3. *Наибольший общий делитель целых чисел* a *и* b *совпадает с последним, отличным от нуля, остатком следующей цепочки равенств, получаемых последовательным применением теоремы о делении с остатком*:

$$\begin{cases} a = b \cdot q_1 + r_1, \\ b = r_1 \cdot q_2 + r_2, \\ \ldots\ldots\ldots\ldots\ldots \\ r_{n-2} = r_{n-1} \cdot q_n + r_n,\ m.e.\ \ r_n = \text{НОД}\ \ (a,b), \\ r_{n-1} = r_n \cdot q_{n+1}. \end{cases}$$

Теорема 1.1.3 предоставляет алгоритм нахождения наибольшего общего делителя целых чисел, называемый алгоритмом Евклида. Он легко преобразуется в алгоритм нахождения наибольшего общего делителя трех и более целых чисел. Следует отметить, что алгоритм Евклида до наших дней остается самым быстрым алгоритмом нахождения наибольшего общего делителя целых чисел.

Пример 1.1.2. Найти с помощью алгоритма Евклида $\text{НОД}(72, 26)$.

Решение. $72 = 26 \cdot 2 + 20;\ \ 26 = 20 \cdot 1 + 6;\ \ 20 = 6 \cdot 3 + 2;\ \ 6 = 2 \cdot 3.$ Следовательно, $\text{НОД}(72, 26) = 2$.

Обратным применением цепочки равенств алгоритма Евклида доказывается

Теорема 1.1.4. *Если* $d = \text{НОД}(a, b)$, *то существуют такие целые* $\boldsymbol{u}$ *и* $\boldsymbol{v}$, *что выполняется следующее соотношение* (*Безу*): $d = a \cdot u + b \cdot v.$

Пример 1.1.3. Цепочка равенств алгоритма Евклида из решения примера 2 позволяет построить соотношение Безу для $\text{НОД}(72, 26) = 2$.

$$2 = 20 + 6\cdot(-3) = 20 + \big(26 + 20\cdot(-1)\big)\cdot(-3) = 20\cdot 4 + 26\cdot(-3) = (72 + 26\cdot(-2))\cdot\big(4 + 26\cdot(-3)\big) = 72\cdot 4 + 26\cdot(-11).$$

Определение 1.1.2. Целые числа a и b называются взаимно простыми, если их наибольший общий делитель $\text{НОД}(a,b) = 1$.

Критерий взаимной простоты чисел. Целые числа a и b взаимно просты тогда и только тогда, когда существуют такие целые u и v, что $a\cdot u + b\cdot v = 1$.

Определение 1.1.3. Натуральное число $p > 1$ называется простым, если его положительными делителями являются только 1 и само число p.

Простые числа обладают многими интересными свойствами. Очевидно, всякое натуральное число $n > 1$ либо является простым числом, либо имеет простой делитель. Из школьного курса математики мы знаем, что простых чисел бесконечно много.

Заметим, что из соотношения $n = p\cdot q$ натуральных чисел следует, что либо сомножитель p, либо число q принадлежит отрезку $\left[1;\sqrt{n}\right]$. Другими словами, если есть предположение, что исследуемое число n составное, но делители его не известны, то найти их можно на указанном отрезке. На этом заключении и базируется «решето Эратосфена» – исторически первый метод проверки натурального числа $n > 1$ на простоту: он заключается в последовательном делении числа n на простые числа, не превосходящие $\sqrt{n}$, если ни на одно из простых чисел отрезка $\left[1;\sqrt{n}\right]$ рассматриваемое число не делится, то n – простое число.

Главное назначение простых чисел в том, чтобы быть составными «кирпичиками» всех натуральных чисел. Об этом свидетельствует

Основная теорема арифметики. *Всякое целое число $n > 1$ однозначно, с точностью до порядка следования сомножителей раскладывается в произведение простых чисел* $n = p_1\cdot p_2\cdot\ldots\cdot p_s$.

Если в разложении произвольного натурального числа n в произведение простых множителей собрать в одну степень одинаковые множители, то получим равенство $n = {p_1}^{r_1}\cdot {p_2}^{r_2}\cdot\ldots {p_t}^{r_t}$. Его называют каноническим разложением целого числа n.

Пример 1.1.4.

а) $196 = 2\cdot 98 = 2\cdot 2\cdot 49 = 2^2\cdot 7^2$;

б) $2^{12} - 1 = 4095 = 3^2\cdot 5\cdot 7\cdot 13$.

Каноническое разложение числа дает практически полную характеристику этого числа, определяет все его базовые свойства. По каноническому разложению целых чисел легко находится их наибольший общий делитель, наименьшее общее кратное, решаются иные задачи.

Следует, однако, отметить, что факторизация, т. е. разложение целого числа в произведение простых – алгоритмически трудная задача, особенно для больших чисел, не решенная удовлетворительно и до сегодняшнего дня, несмотря на значительные усилия многих поколений математиков. На сложности задачи

факторизации базируются многие современные криптографические системы. Более подробно об этом мы будем вести речь в третьей главе первой части данного пособия.

Глава 2. Классы вычетов – арифметика остатков

Пусть $n > 1$ – фиксированное натуральное число. Множество $Z/nZ = \{0, 1, ..., n-1\}$ всевозможных остатков от деления целых чисел на n называется кольцом классов вычетов по модулю n. На множестве Z/nZ определены операции сложения $\oplus$ и умножения $\otimes$ по правилам: суммой (произведением) классов $a, b \in Z/nZ$ называется класс, равный остатку от деления $a+b$ $(a \cdot b)$ на n. Ввиду такой специфики операций элементы Z/nZ будем обозначать символами $\overline{a}$ вместо a. Оказывается, операции такого остаточного сложения и умножения наследуют основные свойства сложения и умножения целых чисел. Ввиду конечности количества элементов Z/nZ остаточное сложение и умножение можно задавать в виде таблиц.

Пример 1.2.1. Запишем таблицы сложения и умножения элементов в кольце классов вычетов $Z/3Z$:

$\oplus$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Таблицы ярко демонстрируют экзотичность операций в кольце классов вычетов. Здесь, как видим, сумма ненулевых классов может равняться нулю, а «дважды два» далеко не четыре, а 1. Это означает, что класс $\overline{2}$ является обратным самому себе.

Определение 1.2.1. Элемент $\overline{k} \in Z/mZ$ называется обратимым, если найдется такой класс $\overline{l} \in Z/mZ$, что $\overline{k} \otimes \overline{l} = \overline{l} \otimes \overline{k} = \overline{1}$. Тогда класс вычетов $\overline{l}$ называют обратным к классу вычетов $\overline{k}$ и его обозначают символом $\overline{k}^{-1}$.

Пример 1.2.2. Приведем таблицу умножения в кольце $Z/8Z$

$\otimes$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

В данном примере, как видим из таблицы умножения, обратимыми являются 4 класса вычетов (половина элементов кольца): $\overline{1}, \overline{3}, \overline{5}, \overline{7}$. Классы $\overline{0}, \overline{2}, \overline{4}, \overline{6}$ не являются обратимыми. В кольце Z мы наблюдали однозначность разложения на множители и существование простых чисел. Здесь эти свойства теряются: $\overline{2} = \overline{3} \cdot \overline{6} = \overline{2} \cdot \overline{5} = \overline{6} \cdot \overline{7}$; $\overline{4} = \overline{2} \cdot \overline{2} = \overline{2} \cdot \overline{6} = \overline{4} \cdot \overline{7} = \overline{4} \cdot \overline{3}$; $\overline{6} = \overline{2} \cdot \overline{3} = \overline{2} \cdot \overline{7} = \overline{5} \cdot \overline{6}$. Неоднозначность разложения на множители налицо, при этом ни один из необратимых классов нельзя отнести к разряду простых: $\overline{2}$ делится и на себя и на $\overline{6}$, $\overline{4}$ делится и на $\overline{2}$ и на $\overline{6}$, $\overline{6}$ делится и на себя и на $\overline{2}$.

Эмпирически определить наличие обратных элементов у данного класса $\overline{k}$ можно по таблице умножения: если в $\overline{k}$ -й строке этой таблицы найдется элемент $\overline{1}$, то первый элемент столбца, в котором находится найденный класс $\overline{1}$, и есть обратный к классу $\overline{k}$.

Разумеется, реально построить таблицу умножения можно лишь для небольших значений m. Отметим свойства строк таблиц умножения в общем случае.

Лемма 1.2.1. Пусть $\overline{k}$ – такой класс кольца Z / mZ, что $\text{НОД}(k, m) = 1$. Тогда: 1) для каждого $\overline{l} \neq \overline{0}$ произведение $\overline{k} \otimes \overline{l} \neq \overline{0}$, 2) $\overline{k} \otimes \overline{l} \neq \overline{k} \otimes \overline{s}$, если $\overline{l} \neq \overline{s}$; 3) отображение $\varphi_k : Z / mZ \to Z / mZ$, действующее по правилу $\varphi_k(\overline{x}) = \overline{k} \otimes \overline{x}$, является взаимно однозначным; 4) $\overline{k}$ – обратимый класс в кольце Z / mZ.

Лемма 1.2.2. Пусть $\overline{k} \in Z / mZ$, такой, что $\text{НОД}(k, m) = d > 1$. Тогда:

1) существует такой ненулевой класс $\overline{l} \in Z / mZ$, что $\overline{k} \otimes \overline{l} = \overline{0}$;

2) найдутся ненулевые классы $\overline{l}_1, \overline{l}_2 \in Z / mZ$, такие, что $\overline{k} \otimes \overline{l}_1 = \overline{k} \otimes \overline{l}_2$;

3) $\overline{k} \otimes \overline{l} \neq \overline{1}$ для всех классов $\overline{l} \in Z / mZ$, следовательно, класс $\overline{k}$ необратим в кольце Z / mZ.

Из лемм 1.2.1 и 1.2.2 вытекает

Критерий обратимости классов вычетов. Класс $\overline{k} \in Z / mZ$ обратим в этом кольце тогда и только тогда, когда $\text{НОД}(k, m) = 1$. Если обратный к данному классу $\overline{k} \in Z / mZ$ существует, то он также обратим. Произведение обратимых классов кольца Z / mZ есть также обратимый класс. В частности, если $m = p$ – простое число, то в кольце Z / mZ каждый ненулевой класс обратим.

Определение 1.2.2. Множество Z / mZ^* всех обратимых элементов кольца Z / mZ называется мультипликативной группой этого кольца.

Из критерия вытекает следующий алгоритм нахождения обратного класса к данному классу $\overline{k} \in Z / mZ$. Вычисляем по алгоритму Евклида $\text{НОД}(k, m)$. Если $\text{НОД}(k, m) = d > 1$, то класс $\overline{k}$ необратим. Пусть $\text{НОД}(k, m) = 1$. Для чисел k и m с помощью расширенного алгоритма Евклида строим соотношение Безу $ku + mv = 1$. Это равенство влечет соответствующее равенство классов

вычетов: $\overline{k} \otimes \overline{u} \oplus \overline{m} \otimes \overline{v} = \overline{1}$. Мы знаем, что $\overline{m} = \overline{0}$. Следовательно, имеем равенство $\overline{k} \otimes \overline{u} = \overline{1}$, которое и означает, что $\overline{k}^{-1} = \overline{u}$. При этом часто оказывается, что $u \notin \{0, 1, ..., m-1\}$. Поэтому формальная запись $\overline{k}^{-1} = \overline{u}$ требует доработки. Если $u > m$, то следует подобрать такое целое $t \geq 1$, что $u - tm \in \{0, 1, ..., m-1\}$. Тогда $\overline{k}^{-1} = \overline{u - tm}$. Если же $u < 0$, то следует подобрать такое целое $t \geq 1$, что $u + tm \in \{0, 1, ..., m-1\}$. Тогда $\overline{k}^{-1} = \overline{u + tm}$.

Пример 1.2.3. В кольце $Z / 201Z$ найдем $\overline{37}^{-1}$.

Решение. С помощью алгоритма Евклида найдем НОД$(37, 201)$. $201 = 37 \cdot 5 + 16;\ 37 = 16 \cdot 2 + 5;\ 16 = 5 \cdot 3 + 1$. Таким образом, НОД$(37, 201) = 1$ и $\overline{37}^{-1}$ существует. Из полученных равенств алгоритма Евклида построим соотношение Безу для чисел 201 и 37: $1 = 201 \cdot 7 + 37 \cdot (-38)$. Следовательно, $\overline{37}^{-1} = \overline{-38} = \overline{201 - 38} = \overline{163}$. Проверка: $163 \cdot 37 = 6031 = 201 \cdot 30 + 1 \equiv 1 (\mathrm{mod}\, 201)$. Значит, действительно $\overline{37} \otimes \overline{163} = \overline{1}$.

Малая теорема Ферма. *Пусть p – простое число и целое число a не делится на p. Тогда $\overline{a}^{p-1} = \overline{1}$ в кольце Z / pZ.*

Определение 1.2.3. Функция Эйлера – функция $\varphi(m)$ натурального аргумента m, которая каждому натуральному числу $m > 1$ ставит в соответствие количество натуральных чисел, меньших m и взаимно простых с m.

Функция Эйлера определяет количество обратимых элементов в кольце Z / mZ, т. е. порядок группы Z / mZ^*. Эта функция обладает рядом мультипликативных свойств, облегчающих вычисление ее значений.

Свойство 1. $\varphi(p) = p - 1$ для каждого простого числа p. Для каждого составного n значение $\varphi(n) < n - 1$.

Свойство 2. $\varphi(p^n) = p^n - p^{n-1}$ для каждого простого числа p и произвольного натурального $n \geq 1$.

Свойство 3. Если НОД$(n, m) = 1$, то $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.

Свойство 4. Если $n = p_1^{s_1} p_2^{s_2} ... p_t^{s_t}$ – каноническое разложение числа n, то

$$\varphi(n) = \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot ... \cdot \left(1 - \frac{1}{p_t}\right).$$

Пример 1.2.4. Вычислим $\varphi(48)$. Поскольку $48 = 3 \cdot 2^4$, то согласно свойству 4 $\varphi(48) = 48 \cdot (1 - 1/3) \cdot (1 - 1/2) = 16$.

Пример 1.2.5. Из критерия обратимости классов вычетов следует, что в кольце Z / mZ имеется в точности $\varphi(m)$ обратимых классов. Например, $\varphi(12) = 4$. Значит, в кольце $Z / 12Z$ имеется именно 4 обратимых элемента. Непосредственная проверка показывает, что этими классами являются $\overline{1}, \overline{5}, \overline{7}, \overline{11}$.

Теорема Эйлера. *Если для целого числа* a *и натурального* m $\text{НОД}(a,m)=1$, *то* $\overline{a}^{\varphi(m)} \equiv \overline{1}$ *в кольце* Z/mZ. *В частности, обратным к классу* $\overline{a}$ *является класс* $\overline{a}^{\varphi(m)-1}$.

Теорема 1.2.1. *Мультипликативная группа* Z/pZ^* *для простого числа* p *является циклической, т. е. в ней существуют примитивные элементы – такие классы вычетов* $\overline{b} \neq \overline{0}$, *что* $Z/pZ^* = \left\{\overline{b}, \overline{b}^2, ..., \overline{b}^{p-1} = \overline{1}\right\}$.

Глава 3. Элементы теории групп

§3.1. Базовые понятия теории групп

В математике теория множеств является базовым, но очень небольшим разделом. Чаще всего здесь исследуются множества, наделенные какими-то дополнительными свойствами или структурами, и отношения между такими множествами. Так, математический анализ изучает взаимосвязь числовых множеств. Это ничтожно малый класс множеств, но всеобщее внимание к нему объясняется широчайшими приложениями в науке и жизни.

Потребности практики вызвали необходимость изучения современной алгебры специалистами инфокоммуникационных направлений. С формальной точки зрения алгебра изучает алгебраические системы, т. е. множества с алгебраическими операциями на них. С алгебраическими операциями сложения, вычитания, умножения, деления чисел мы знакомы с раннего детства. В вузе многообразие рассматриваемых алгебраических операций стремительно растет. Здесь и умножение матриц, и сложение векторов, и векторное умножение векторов, и композиция функций, т. е. процедура образования сложных функций. Выше к этому списку мы добавили сложение и умножение классов вычетов. Эти и другие примеры давно привели к необходимости абстрактного определения алгебраической операции.

Определение 1.3.1. Бинарной алгебраической операцией на множестве X называется всякое правило, по которому каждой упорядоченной паре (x, y) элементов $x, y \in X$ ставится в соответствие один вполне определенный элемент z из X.

Обычно операции обозначаются знаками $*$, $\bullet$, $\times$, $^{\circ}$, $+$, $-$, скобками и т. п. В конкретных ситуациях бинарные алгебраические операции называют сокращенно или сложением, или умножением, или, наконец, композицией. Тот факт, что элемент z множества X является результатом бинарной операции $*$ над элементами $x, y \in X$ в указанном порядке обозначают равенством: $z = x * y$.

Пример 1.3.1. $(Z,+,\cdot)$ – алгебраическая система целых чисел с операциями сложения и умножения, называемая кольцом целых чисел. $(M_n(R),+,\cdot)$ – матричная алгебра – алгебраическая система квадратных матриц порядка n с

вещественными коэффициентами относительно операций матричного сложения и матричного умножения.

Алгебраические системы различают по операциям и свойствам этих операций.

Определение 1.3.2. Алгебраическая система $(X, *)$ с одной алгебраической операцией на множестве X называется группоидом.

Если у группоида $(X, *)$ операция ассоциативна $a*(b*c)=(a*b)*c$ для произвольных a, b, $c \in X$, то такой группоид называют полугруппой.

Моноидом $(X, *)$ называют полугруппу с единицей или нейтральным элементом, т. е. таким элементом n, что $n*x=x*n=x$ для каждого элемента $x \in X$.

Пример 1.3.2. $(N, \cdot)$ – множество натуральных чисел с операцией умножения – моноид; $(N, +)$ – множество натуральных чисел с операцией сложения – полугруппа, а алгебраическая система $(N, -)$ – группоид.

Пример 1.3.3. R_3 – множество всех свободных векторов трехмерного пространства с операцией векторного умножения – группоид, но не полугруппа, поскольку операция векторного умножения, как известно, не ассоциативна.

Определение 1.3.3. Группой называется непустое множество G с определенной на нем бинарной алгебраической операцией $\bullet$, которая обладает свойствами:

1) ассоциативность: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ для любых $a, b, c \in G$;

2) в G существует нейтральный элемент, т. е. такой элемент $e \in G$, что $g \bullet e = e \bullet g = g$ для каждого $g \in G$;

3) каждый элемент $g \in G$ имеет обратный, т. е. такой элемент $h \in G$, что $g \bullet h = h \bullet g = e$.

Несложно доказывается, что в любой группе нейтральный элемент – единственный, и что элемент, обратный к каждому элементу, определен однозначно.

Пример 1.3.4. $(Q, +)$; $(R, +)$; $(C, +)$ – группы всех рациональных, вещественных и соответственно комплексных чисел с операцией сложения. Это так называемые аддитивные группы.

Определение 1.3.4. Абелевыми, или коммутативными называют группы $(G, \bullet)$ со свойством 4): $a \bullet b = b \bullet a$ для произвольных $a, b \in G$.

Исторически сложилось, что все аддитивные группы являются коммутативными. Нейтральный элемент аддитивной группы называют нулем и обозначают 0, а обратный элемент к данному элементу a – противоположным и обозначают через $-a$. К аддитивным относятся группы: $(M_{m\times n}(R), +)$ – множество прямоугольных $m \times n$ матриц с вещественными коэффициентами с операцией сложения матриц, $(P[x], +)$ – множество всех полиномов с вещественными коэффициентами и с операцией сложения, V_n – множество всех n-мерных векторов с вещественными коэффициентами и с операцией векторного сложе-

ния. Всякий линейный код является абелевой группой относительно определенной на нем операции сложения.

Если множество с операцией умножения является группой, то такую группу обычно называют мультипликативной.

Пример 1.3.5. Продолжая пример 1.3.4, заметим, что к мультипликативным абелевым группам относятся следующие числовые группы с обыкновенной операцией умножения чисел: $(Q^*,\cdot)$; $(R^*,\cdot)$; $(C^*,\cdot)$ и т. д., где $C^* = C \setminus \{0\}$, $R^* = R \setminus \{0\}$, $Q^* = Q \setminus \{0\}$.

Свойство 4 делит группы на два класса: на абелевы и неабелевы группы.

Пример 1.3.6. $GL_n(R)$ – множество квадратных матриц порядка $n > 1$ с вещественными коэффициентами и ненулевым определителем относительно операции матричного умножения является неабелевой группой. Она называется полной линейной группой (матриц порядка n над полем R). Полную линейную группу можно рассматривать над любым полем P, например, над полем комплексных чисел C или рациональных чисел Q. А можно в качестве P взять конечное поле, в частности, Z / pZ – поле классов вычетов по простому модулю p.

По количеству элементов группы делятся на два типа: конечные группы и бесконечные.

Определение 1.3.5. Порядком конечной группы называется количество элементов этой группы. Если G – конечная группа, то $|G|$ – ее порядок.

Пример 1.3.7. Группа $(Z / nZ, \oplus)$ является конечной абелевой аддитивной группой из n элементов; в силу критерия обратимости классов множество $(Z / nZ)^*$ обратимых относительно умножения классов вычетов по модулю n, где n – натуральное число, большее единицы, образует группу порядка $\varphi(n)$. Алгебраическая система $(M_{m\times n}(Z / kZ), +)$ из $m \times n$-матриц с операцией матричного сложения являются конечной абелевой группой порядка k^{mn}. Группа $GL_n(Z / pZ)$, p – простое, является конечной некоммутативной группой. Известно, что ее порядок $|GL_n(Z / pZ)| = (p^n - 1)(p^n - p) \cdot \ldots \cdot (p^n - p^{n-1})$.

Отметим, что для каждого натурального числа n существует абелева группа порядка n. Для каждого натурального $n > 1$ множество C_n комплексных корней n-й степени из 1, т. е. чисел $Z_n = e^{\frac{i2\pi k}{n}}$ для $k = 0, 1, \ldots, n-1$, образует коммутативную группу порядка n. Такой же является группа $(Z / nZ, \oplus)$ из примера 1.3.7.

В дальнейшем, если не оговорено противное, операцию в группе будем считать умножением, нейтральный элемент обозначать через e и называть единицей.

§3.2. Подгруппы

Определение 1.3.6. Подгруппой в группе $(G,\cdot)$ называется всякое непустое подмножество H элементов множества G, *которое в свою очередь является группой относительно той же операции.*

Тот факт, что H есть подгруппа группы G, отмечают так: $H \le G$ или $H < G$, если включение $H \subset G$ строгое.

Пример 1.3.8. Аддитивные группы целых, рациональных, вещественных и комплексных чисел образуют систему подгрупп: $(Z,+) < (Q,+) < (R,+) < (C,+)$. Подмножество всех целых чисел, делящихся на натуральное число $n > 1$, образует подгруппу $(nZ,+)$ в группе $(Z,+)$. Следовательно, имеют место бесконечные цепочки аддитивных подгрупп типа $(Z,+) > (2Z,+) > (4Z,+) > \ldots$.

Пример 1.3.9. Мультипликативные группы рациональных, вещественных и комплексных чисел из примера 1.3.8 образуют свою цепочку подгрупп: $Q^* < R^* < C^*$. Каждая из этих групп имеет и иные свои подгруппы. Так, Q^* и R^* содержат подгруппы Q_+^* и R_+^* положительных рациональных и положительных вещественных чисел соответственно, $\{\pm 1\}$ – подгруппа мультипликативной группы Q^*. Множество U всех комплексных чисел, модуль которых равен 1, т. е. единичная окружность с центром в начале координат на комплексной плоскости является подгруппой относительно умножения в группе C^*. Пусть n и k – произвольные натуральные числа, большие 1. Имеется цепочка подгрупп: $C_n < C_{kn} < U < C^*$.

Теорема 1.3.1 (критерий подгруппы). *Непустое подмножество H группы $(G,\cdot)$ является подгруппой тогда и только тогда, когда для произвольных элементов $a, b \in H$ имеет место включение $a \cdot b^{-1} \in H$.*

Пример 1.3.10. В любой группе G подмножество $\{e\}$ из одного единственного нейтрального элемента $e \in G$ является самой маленькой подгруппой.

Определение 1.3.7. Подгруппа H группы G называется собственной, если $H \neq G$ и $H \neq \{e\}$.

Пример 1.3.11. С помощью критерия подгруппы легко убедиться, что $SL_n(R)$ – подмножество квадратных матриц порядка n с определителем, равным 1, – образует подгруппу в полной линейной группе $GL_n(R)$. Действительно, для произвольных матриц $A, B \in SL_n(R)$ по свойствам определителей $\det(B^{-1}) = 1$ и $\det(AB^{-1}) = \det A \cdot \det(B^{-1}) = 1$. Следовательно, $AB^{-1} \in SL_n(R)$ и согласно критерию $SL_n(R)$ является подгруппой в группе $GL_n(R)$. Она носит название специальной линейной группы. $SL_n(R)$ содержит подгруппу $SL_n(Q)$ с рациональными коэффициентами, а та в свою очередь содержит достаточно

мощную (при $n \geq 2$) подгруппу $SL_n(Z)$ с целыми коэффициентами.

§3.3. Циклические подгруппы

Теорема 1.3.2. *Пусть a – фиксированный элемент произвольной группы G. Пусть* $< a >= \{a^0 = e, a, a^2, ..., a^{-1}, a^{-2}, ...\}$ *– множество всевозможных степеней элемента a. Тогда* $< a >-$ *подгруппа группы* G*, причем абелева.*

Доказательство следует из критерия подгруппы: для произвольных $a^k, a^l \in < a >$ произведение $a^k \cdot a^{-l} = a^{k-l}$ принадлежит множеству $< a >$.

Определение 1.3.8. Подгруппа $< a >$ из теоремы 1.3.2 называется циклической подгруппой группы G, порожденной элементом a. Если в группе G найдется такой элемент b, что $G =< b >$, то такую группу называют циклической.

При этом элемент b называют примитивным, или образующим элементом группы.

Пример 1.3.12. Следующие группы являются циклическими: а)$(Z,+) = <1>$; б) $(Z/nZ,+) =< \overline{1} >$; в) $C_n =< e^{i2\pi/n} >$.

Теорема 1.3.3. Пусть элемент $a \in G$ обладает свойствами $a^n = e$ для некоторого целого n, и $a^k \neq e$ для всех целых k, $1 \leq k < n$. Тогда циклическая подгруппа $< a >$ имеет порядок n и $< a >= \{a, a^2, ..., a^n = e\}$.

Доказательство. Заметим, что для целых k, $1 \leq k < n$, $(a^k)^{-1} = a^{n-k}$.

Определение 1.3.9. Величина n из теоремы 1.3.3 называется порядком элемента $a \in G$. Если же для элемента $a \in G$ такого n не существует, то говорят, что элемент имеет бесконечный порядок.

Пример 1.3.13. Любое ненулевое целое число имеет бесконечный порядок в аддитивной группе целых чисел. В примере 1.3.12 элементы $\overline{1}$ и $e^{i2\pi/n}$ имеют одинаковый порядок n.

Пример 1.3.14. Возьмем матрицу $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(R)$. Здесь $A^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$; $A^3 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}$. Степени матрицы A попарно различны и образуют бесконечную последовательность. Определитель матрицы A равен $1 \neq 0$. Следовательно, матрица A обратима: $A^{-1} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$, $A^{-2} = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$,… . Таким образом, циклическая подгруппа, порожденная матрицей A в группе $GL_2(R)$, является бесконечной.

Матрица $H \in GL_2(R)$ вида $H = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ имеет степени $H^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$;

$H^3 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$; $H^4 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = E$ – единичная матрица. Согласно теореме 1.3.3 подгруппа $< H >$ есть конечная подгруппа 4-го порядка.

Из определения циклической группы следует, что она содержит счетное или конечное множество элементов и во втором случае имеет четкую структуру, выражаемую теоремой 1.3.3. Отметим еще одно свойство циклических групп.

Теорема 1.3.4. *Всякая подгруппа циклической группы является циклической.*

Итак, в любой группе много циклических подгрупп: каждый элемент порождает свою циклическую подгруппу. Тем не менее следует заметить, что чаще группы циклическими не являются. Например, все некоммутативные группы не могут быть циклическими в силу теоремы 1.3.2. Циклическими не являются аддитивные и мультипликативные группы вещественных и комплексных чисел в силу их несчетности. Множество рациональных чисел является счетным, т. е. равномощно множеству целых чисел. Однако абелева группа (Q,+) в отличие от группы $(Z,+)$ не циклична. Существует много конечных коммутативных и нециклических групп. Можно показать, что мультипликативная группа $Z/8Z^*$ абелева, но не циклична, а $Z/9Z^*$ – циклична. В отличие от составного модуля n группы Z/pZ^* для простых p в определенном смысле одинаковы.

Теорема 1.3.5. *Для каждого простого числа p мультипликативная группа Z/pZ^* содержит $p-1$ элементов и является циклической.*

Когда в конкретном случае спрашивают о цикличности данной группы Z/pZ^*, то при этом неявно предполагают, что следует найти такое натуральное число b, $1 < b < p$, что $< b > = Z/pZ^*$.

Глава 4. Исторические шифры. Современные теоретико-числовые криптосистемы

§4.1. Исторические методы шифрования

Криптография, или тайнопись, существует практически столько же, сколько существует и письменность, и имеет длительную и славную историю. Рассмотрим наиболее популярные системы шифрования.

1. Шифр Цезаря. Суть данного шифра в том, что в тексте каждая буква заменяется отстоящей от нее в алфавите на фиксированное число позиций по циклу. Так, Юлий Цезарь в I веке новой эры в деловой переписке заменял в сообщении первую букву латинского алфавита (A) на четвертую (D), вторую (B) – на пятую (E), наконец, последнюю – на третью. Иными словами, замена производилась в соответствии с таблицей, которая для русского алфавита имеет следующий вид:

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С

П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Пример 1.4.1. Знаменитое донесение Юлия Цезаря римскому сенату об очередной победе выглядит (в русском переводе) следующим образом:

ТУЛЫИО ЦЕЛЖЗО ТСДЗЖЛО

Приложив достаточно серьезные усилия по расшифровке, можно убедиться, что истинный текст гласит: «Пришел, увидел, победил».

2. Тарабарская грамота. Известна в России с XIII в. На уровне разговорного языка ею владели и Стенька Разин, и Емельян Пугачев. Известный журналист В. Гиляровский, автор ряда очерков о нравах и обычаях старой Москвы, еще в 30-х гг. XX в. встречал на московских рынках странных лиц, переговаривавшихся между собой на «тарабарском». Тарабарская грамота проста. В ней согласные буквы заменяются по схеме:

Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

При шифровании буквы, расположенные на одной вертикали, заменяют одну на другую. Остальные буквы остаются без изменения.

Пример 1.4.2. Попробуйте прочитать следующее «исключительно секретное» сообщение: РАРА РЫСА МАРУ.

3. Криптосистема Тритемиуса. Данная система шифрования впервые была опубликована в 1518 г. в трактате, принадлежащем перу религиозного деятеля аббата Тритемиуса (1462 – 1516). Система Тритемиуса представляет собой дальнейшее усовершенствование системы шифрования Цезаря и базируется на идее применения девизов. Под текстом подписывался девиз (в дальнейшем его стали называть «ключом») с повторением, затем происходило постолбцовое суммирование букв текста и девиза («ключа» по новой терминологии), в результате получался шифротекст.

Пример 1.4.3. Зашифруем текст «Над Парижем небо синее» с помощью девиза «Роза». Как сказано выше, для этого выпишем две строки – строку текста и строку ключа с повторением. Сверху и снизу добавим по строке номеров соответствующих букв в русском алфавите. Получим следующую таблицу:

15	1	5	17	1	18	10	8	6	14	15	6	2	16	19	10	15	6	6
Н	*А*	*Д*	*П*	*А*	*Р*	*И*	*Ж*	*Е*	*М*	*Н*	*Е*	*Б*	*О*	*С*	*И*	*Н*	*Е*	*Е*
Р	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*	*А*	*Р*	*О*	*З*
18	16	9	1	18	16	9	1	18	16	9	1	18	16	9	1	18	16	9

Для получения шифротекста суммируем числа каждого столбца полученной таблицы. Если сумма оказывается больше 33, то вычитаем из нее 33. После этих вычислений от числа вновь переходим к букве. Так, в первом столбце получаем число 15 + 18 = 33, т. е. букву «Я». Продолжив процедуру, получим следующее шифрованное сообщение:

Я П М Р С А С З Ц Ь Ц Ё Т Ю Ъ И Я Ф Н

4. Постолбцовая транспозиция. В данный прямоугольник размером $[n \times m]$ вписывается «змейкой» сообщение по строкам. Шифрованный текст найдем, если будем выписывать буквы в порядке следования столбцов. Следующий пример демонстрирует шифрование методом «постолбцовой транспозиции».

Пример 1.4.4. Текст, состоящий из 30 букв, записан построчно змейкой в таблицу или матрицу размером 5×6:

М	*И*	*Н*	*С*	*К*	*С*
А	*Ц*	*И*	*Л*	*О*	*Т*
Р	*Е*	*С*	*П*	*У*	*Б*
Е	*Б*	*И*	*К*	*И*	*Л*
Л	*А*	*Р*	*У*	*С*	*Ь*

Шифрованный текст получается в результате последовательной записи столбцов этой таблицы в строку, также «змейкой», начиная с последнего:

МАРЕЛ АБЕЦИ НИСИР УКПЛС КОУИС ЬЛБТС .

Конечно, возможны и другие способы-маршруты записи текста в таблицу и выписки столбцов. Например, такой, более естественный:

М	*И*	*Н*	*С*	*К*	*С*
Т	*О*	*Л*	*И*	*Ц*	*А*
Р	*Е*	*С*	*П*	*У*	*Б*
Л	*И*	*К*	*И*	*Б*	*Е*
Л	*А*	*Р*	*У*	*С*	*Ь*

→ *МТРЛЛ ИОЕИА НЛСКР СИПИУ КЦУБС САБЕЬ*

Пример 1.4.5. Попробуйте прочитать еще одно сообщение, зашифрованное методом «постолбцовой транспозиции»:

МАСТ АЕРР ЕШРН ОЕРМ ИУПВ КЙТР ПНОИ.

§4.2. Современная криптография. Криптосистема RSA

Современная криптография существует с последней четверти XX в. и базируется на рассмотренной выше «остаточной» арифметике. Толчком к ее созданию послужили исследования ученых У. Диффи и М. Хелмана по так называемым «односторонним функциям», достаточно легко вычислимым, но обращение которых без знания необходимых ключей реализуется крайне сложно.

Эти же авторы предложили гипотетический пример такой односторонней «функции» – функцию Эйлера: $\varphi(n)$ легко вычисляется, если известно каноническое разложение числа n, но вычисление φ становится практически невозможным для больших значений n. Для таких значений n поиск больших делителей также становится почти неразрешимой проблемой. Вскоре на основе этой идеи американские исследователи Р. Ривест, А. Шамир и Л. Адлеман предложили свою криптографическую систему [1].

Суть криптосистемы RSA в следующем. Находятся два больших простых числа p и q. Для серьезной криптосистемы, способной противостоять атакам всей современной компьютерной «рати», эти числа должны содержать по 60 – 70 десятичных знаков. Каким образом подобрать такие большие простые числа – это отдельный разговор. Вычисляется их произведение $n = pq$. Тогда значение функции Эйлера: $\varphi(n) = (p-1)(q-1)$. Фиксируется натуральное число e, $0 < e < n$, $\text{НОД}(e, \varphi(n)) = 1$. Пара (e, n) называется открытым ключом. Передаваемая информация первоначально преобразуется в цифровую форму – в некоторое десятичное число c (это обозначение происходит от слова «сообщение»), данный этап шифрованием, собственно, и не считается. Авторы криптосистемы предложили самый немудрёный способ перевода словесной информации в числовую: букву «а» заменяем числом 01, букву «б» – числом 02,…, «я» – числом 33. Предполагается, что $0 < c < n$. Тогда c можно интерпретировать как ненулевой элемент кольца классов вычетов Z/nZ. А если потребовать дополнительно выполнения условия: $\text{НОД}(c, n) = 1$, то $c \in Z/nZ^*$, т. е. c – обратимый элемент кольца Z/nZ. Конечно, целое число c и класс вычетов $\bar{c}$, порожденный этим числом в кольце Z/nZ, представляют собой, как говорят одесские юмористы, две большие разницы, особенно при операциях над ними. Сообщение шифруется и передается в виде числа $m = \bar{c}^e$, вычисленного в кольце Z/nZ. Теория групп гарантирует, что возведение в e-ю степень является взаимно однозначной и, следовательно, обратимой операцией в группе Z/nZ в отличие, например, от возведения в квадрат, потому, что $n-1$ делится на 2 для нечетного n. Итак, зашифрованное сообщение m есть e-я степень числа c в кольце Z/nZ. Отметим, что требование $\text{НОД}(c, n) = 1$ вовсе не обременительно, поскольку в кольце Z/nZ имеется лишь $p+q$ необратимых элементов. Адресату отправляется тройка чисел: (m, e, n).

Адресат получает сообщение (m, e, n). Он также должен знать и секретный ключ – такое целое число $d < n$, что $\bar{e} \cdot \bar{d} = \bar{1}$ в кольце $Z/\varphi(n)Z$. Впрочем, достаточно знать разложение $n = pq$. Тогда адресат знает, что $\varphi(n) = (p-1)(q-1)$. Величина d является обратным к классу вычетов $\bar{e}$ в кольце $Z/\varphi(n)Z$ и находится, как мы знаем, стандартным расширенным алгоритмом Евклида. В силу теоремы Эйлера $\bar{c}$, как элемент группы Z/nZ^*, обла-

дает свойством $\bar{c}^{\varphi(n)} = \bar{1}$. Тогда $\bar{m}^d = \bar{c}^{ed} = \bar{c}^{\varphi(n)\cdot r+1} = \left(\bar{c}^{\varphi(n)\cdot}\right)^r \cdot \bar{c} = \bar{1}\cdot\bar{c} = \bar{c}$. Таким образом, чтобы расшифровать сообщение m, адресату достаточно возвести m в d -ю степень по модулю n. Это относительно простая задача.

Пример 1.4.6. Пусть $p = 3,\ q = 11$. Тогда $n = pq = 33,\ \varphi(n) = 2\cdot 10 = 20$. Возьмем $e = 7$. Ясно, что тогда $d = 3$. В качестве сообщения возьмем букву «С» = 19. Тогда шифровка есть число $m = c^e (\mathrm{mod}\, n) = 19^7 (\mathrm{mod}\, 33)$. Эту величину вычислим поэтапно.

$$19^2 = 361 \equiv 31(\mathrm{mod}\, 33).\ 19^4 \equiv 31^2(\mathrm{mod}33) = 961 \equiv 4(\mathrm{mod}33).$$

Тогда $19^7 \equiv 4\cdot 31\cdot 19(\mathrm{mod}\, 33) \equiv 13(\mathrm{mod}\, 33)$. Таким образом, $m = 13$. Адресату отправляется сообщение $(m, e, n) = (13, 7, 33)$.

Принявший сообщение реализует его дешифрацию по правилу $c = m^d (\mathrm{mod} n) = 13^3 (\mathrm{mod}33) = 13^2\cdot 13(\mathrm{mod}33) \equiv 4\cdot 13(\mathrm{mod}33) = 52(\mathrm{mod}33) = 19.$ Истинное сообщение определено полностью и правильно.

Злоумышленник, чтобы расшифровать перехваченное сообщение m, должен найти $\varphi(n)$. Тогда он сможет найти решение сравнения $ex \equiv 1(\mathrm{mod}(\varphi(n))$, т. е. найти секретный ключ d. После этого при расшифровке у него возникнут такие же трудности, как и у адресата. Но для нахождения $\varphi(n)$ в математике существует единственный путь – разложение числа n на простые множители. А это алгоритмически очень сложная задача, особенно в случае, когда оба простых числа p и q достаточно велики, т. е. относительно близки к $\sqrt{n}$.

Чтобы продемонстрировать стойкость данной криптосистемы, изобретатели в своей первой публикации о ней предложили читателям расшифровать следующую криптограмму:

n = 114 381 625 757 888 867 669 325 779 976 146 612 010 218 296 721 242 362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058 989 075 147 599 290 026 879 543 541;

e = 9007;

m = 96 869 613 754 622 061 477 140 922 254 355 882 905 759 991 124 574 319 874 695 120 930 816 298 225 145 708 356 931 476 622 883 989 628 013 391 990 551 829 945 157 815 154

Всемирно известный специалист по всевозможным головоломкам М. Гарднер опубликовал этот криптотекст в журнале «Scientific American» еще в августе 1977 г., предложив 100$ первому, кто его расшифрует. В нем используется n – 129-значное число и e – 4-значное число. Зашифрованное сообщение является 128-значным десятичным числом. Текст был расшифрован лишь через 17 лет, в апреле 1994 г. Авторы данного шифротекста ожидали его расшифровки как минимум через 50 лет. Однако известный в мире специалист по факторизации целых чисел, один из соавторов наиболее эффективного на сегодняшний день метода разложения целых чисел на множители – метода квадратичного решета, воспринял поставленную задачу как вызов собственному достоинству. Он с тремя единомышленниками – Д. Аткинсоном, М. Граффом, П. Лейлендом возглавил проект Free Software Foundation, в котором на доброволь-

ных началах участвовало примерно 600 человек. Была проведена колоссальная теоретическая и организационная проработка организации всех аспектов работы по расшифровке данного криптотекста. Для этого через Internet были задействованы ресурсы 1600 компьютеров из более 20 стран. Организаторы расшифровки использовали суперкомпьютер – MasPar. Данные были занесены в 0-1 матрицу из 188346 строк и 188146 столбцов. Файл с этой матрицей превосходил 4 Гб, причем каждый бит был существенным. Непосредственные вычисления проводились непрерывно в течение 220 дней. 129-значное число было разложено на 64- и 65- значные множители:

p = 3 490 529 510 847 650 949 147 849 619 903 898 133 417 764 638 493 387 843 990 820 577;

q = 32 769 132 993 266 709 549 961 988 190 834 461 413 177 642 967 992 942 539 798 288 533.

После этого достаточно быстро было восстановлено зашифрованное сообщение: «The magic words are squeamish ossifrage».

§4.3. Криптосистема Эль Гамаля

Данная криптосистема, предложенная Таиром Эль Гамалем, появилась в 1985 г. как реакция на излишнюю сложность криптосистемы RSA. Ее криптографическая стойкость базируется на иной проблеме – проблеме дискретного логарифма: решение уравнения $\bar{a}^x = \bar{b}$ в кольце Z/pZ с простым p на сегодняшний день осуществляется единственным способом – последовательным перебором степеней $\bar{a}$ до получения требуемого класса вычетов $\bar{b}$. Проблема и состоит в нахождении иного, не переборного метода определения степени x в данном уравнении.

В основе криптосистемы Эль Гамаля лежит большое простое число P. Для реальных, не учебных, криптосистем оно должно содержать от 150 до 300 десятичных знаков. А это означает, что P находится в диапазоне от 2^{512} до 2^{1024}. Как мы знаем, кольцо классов вычетов Z/PZ является полем, т. е. кольцом, в котором все ненулевые элементы обратимы относительно умножения. Согласно теореме 1.3.5 мультипликативная группа Z/PZ^* является циклической, т. е. представляет собой цепочку степеней одного из этих элементов. Пусть g – одна из таких образующих мультипликативной группы Z/PZ^*. Параметры P и g общедоступны, считаются открытыми ключами криптосистемы.

Секретным ключом криптосистемы может быть в принципе любое натуральное число x. Его знают оба пользователя криптосистемы – и отправитель, и адресат. Величина же $h = g^x \pmod P$ является третьим открытым ключом криптосистемы. Информационным сообщением в этой криптосистеме может быть любое число c, интерпретируемое как ненулевой элемент поля Z/PZ. Для передачи сообщения c или нескольких сообщений за короткий промежуток времени отправитель формирует сеансовый ключ k. Адресат его не знает. Сообщение шифруется умножением в поле Z/PZ на $K = h^k \pmod P$. Таким

образом, шифрованное сообщение $m = cK(\mathrm{mod}\,P)$. Адресату отправляется сообщение из двух чисел: (m, O_{sk}), где $O_{sk} = g^k(\mathrm{mod}P)$ – открытый сеансовый ключ.

Получатель знает тройку (P, g, h) открытых ключей. Также он знает и секретный ключ x. Получатель вычисляет величину $O_{sk}^x(\mathrm{mod}\,P)$. Заметим, что $O_{sk}^x(\mathrm{mod}\,P) = g^{kx}(\mathrm{mod}\,P) = h^k(\mathrm{mod}\,P) = K$. Осталось найти K^{-1} в поле Z/PZ. Эта задача аналогична нахождению d в криптосистеме RSA. Теперь остается узнать истинное сообщение по формуле $c = m \cdot K^{-1}(\mathrm{mod}\,P)$.

Пример 1.4.7. Пусть $P = 23$. Непосредственная проверка показывает, что в качестве образующей g в $Z/23Z^*$ можно взять $g = 5$.

Пусть секретный ключ $x = 7$. Тогда

$h = 5^7(\mathrm{mod}23) = 5^2 \cdot 5^2 \cdot 5^2 \cdot 5(\mathrm{mod}23) \equiv 2 \cdot 2 \cdot 2 \cdot 5(\mathrm{mod}23) = 40(\mathrm{mod}23) \equiv 17(\mathrm{mod}23).$

Итак, $h = 17$. Возьмем $k = 3$. Тогда $K = h^k(\mathrm{mod}P) = 17^3(\mathrm{mod}23) \equiv 14(\mathrm{mod}23)$. $O_{sk} = g^k(\mathrm{mod}\,P) = 5^3(\mathrm{mod}\,23) \equiv 10(\mathrm{mod}\,23)$. Осталось выбрать сообщение. Пусть $c = 20$. Тогда $m = cK(\mathrm{mod}\,P) = 20 \cdot 14(\mathrm{mod}\,23) \equiv 4(\mathrm{mod}\,23)$. Адресату отправляется пара чисел $(m, O_{sk}) = (4, 10)$. Величины $(P, g, h, x) = (23, 5, 17, 7)$ он должен знать заранее.

Получатель вычисляет $K = O_{sk}^x(\mathrm{mod}\,P) = 10^7(\mathrm{mod}\,23) = 14$. Легко видеть, что $K^{-1}(\mathrm{mod}\,23) = 5$. Тогда $c = m \cdot K^{-1}(\mathrm{mod}\,P) = 4 \cdot 5(\mathrm{mod}\,23) = 20$.

§4.4. Криптосистема Рабина

Данная криптосистема также явилась результатом переосмысления криптосистемы RSA. М. Рабин заинтересовался вопросом выбора ключа e в криптосистеме RSA. Там e всегда взаимно просто с $\varphi(n)$ и, в частности, всегда нечетно. А что произойдет, если взять e четным, например $e = 2$? В результате подробного рассмотрения и появилась следующая модификация криптосистемы RSA – криптосистема Рабина.

Пусть p и q – два различных простых числа. Пусть $N = pq$. Зафиксируем число B, $0 \le B < N$. Пара $\{N, B\}$ есть пара открытых ключей криптосистемы Рабина. Сообщение c рассматривается как элемент кольца Z/NZ и шифруется формулой $m = c(c + B)(\mathrm{mod}\,N)$. Ясно, что такой способ шифрования реализуется гораздо быстрее, чем в криптосистеме RSA.

Расшифровка здесь представляет гораздо более «вязкую» процедуру даже для законного получателя криптотекста. Фактически сообщение c есть один из корней квадратного уравнения $x^2 + Bx - m = 0$ в кольце Z/NZ. В этом кольце 2 является обратимым элементом. Поэтому для решения квадратного уравнения

вполне пригодны стандартные формулы: $x = \left(\sqrt{\frac{B^2}{4} + m} - \frac{B}{2}\right) (\mathrm{mod}\, N)$. Неудобство здесь в том, что из каждого квадрата в данном кольце Z/NZ извлекаются 4 различных корня.

Пример 1.4.8. Пусть $N = 3 \cdot 7 = 21$. Возьмем $B = 5$. Пусть сообщение $c = 19$. Тогда шифровка $m = c(c + B)(\mathrm{mod}\, N) = 19(19 + 5)(\mathrm{mod}\, 21) = 15$. Адресату отправляется тройка чисел $(N, B, m) = (21, 5, 15)$.

Получатель вычисляет дискриминант квадратного уравнения: $D = \frac{B^2}{4} + m = 25/4 + 15 \equiv (25 \cdot 16 + 15)(\mathrm{mod}\, 21) = 16$. Непосредственная проверка показывает, что в кольце $Z/21Z$ из 16 извлекаются в точности 4 корня: 4, 10, 11, 17. Здесь $2^{-1} = 11$. Поэтому $x_1 = 4 - 5 \cdot 11 \equiv 12 (\mathrm{mod}\ 21)$; $x_2 = 10 - 55 \equiv 18 (\mathrm{mod} 21)$; $x_3 = 11 - 55 \equiv 19 (\mathrm{mod}\ 21)$; $x_4 = 17 - 55 \equiv 4 (\mathrm{mod} 21)$. Отправитель знает, какой ответ является нужным, но как на него указать адресату – дополнительная проблема.

Глава 5. Кольца и поля

§5.1. Кольца

Определение 1.5.1. Кольцом называется непустое множество K с двумя бинарными алгебраическими операциями сложения $(+)$ и умножения $(\cdot)$; относительно операции сложения K является абелевой группой, а умножение и сложение связаны законами дистрибутивности

$$(a + b) \cdot c = a \cdot c + b \cdot c; \quad a \cdot (b + c) = a \cdot b + a \cdot c$$

для произвольных $a, b, c \in K$.

Кольца различают по количеству элементов (конечные или бесконечные) и по свойствам умножения (ассоциативные и неассоциативные, коммутативные и некоммутативные, с единицей и без единицы, с делителями нуля и без делителей нуля и т. д.).

Определение 1.5.2. Подкольцо кольца K – это подгруппа аддитивной группы $(K,+)$, в свою очередь являющаяся кольцом, т. е. замкнутая относительно операции умножения в кольце K .

Подкольцо J кольца K называется левым идеалом кольца K, если для любого $k \in K$ и для каждого $j \in J$ произведение $jk \in J$, т. е. $Jk \subseteq J$. Если же $kJ \subseteq J$ для всех элементов $k \in K$, то J называют правым идеалом. Двусторонний идеал – идеал, являющийся одновременно и левым, и правым идеалом.

Пример 1.5.1. $(Z,+,\cdot)$ – кольцо целых чисел. $(Z/nZ,+,\cdot)$ – кольцо классов вычетов по модулю $n > 1$.

Пример 1.5.2. Множество всех квадратных матриц данного порядка n с рациональными, вещественными или же комплексными коэффициентами относительно операций матричного сложения и умножения. Общепринятые обозначения этих колец: $M_n(Q)$, $M_n(R)$, $M_n(C)$ соответственно.

Пример 1.5.3. Множество всех подмножеств $\Omega(M)$ непустого множества M является абелевой группой относительно операции симметрической разности $\overset{\bullet}{\longleftrightarrow}$ (объединение множеств за вычетом их пересечения). Здесь операция пересечения множеств играет роль умножения. В теории множеств известно тождество $(A \overset{\bullet}{\longleftrightarrow} B) \cap C = (A \cap C) \overset{\bullet}{\longleftrightarrow} (B \cap C)$, которое означает, что симметрическая разность и пересечение связаны законом дистрибутивности. Данное кольцо носит название *булеан* – в честь английского математика XIX в. Джорджа Буля, основателя математической логики.

Пример 1.5.4. Множество $F(a,b)$ всех вещественных функций, определенных на данном интервале (a,b) числовой оси с обычными операциями сложения и умножения функций, является кольцом.

Пример 1.5.5. Кольцо полиномов $R[x]$ с вещественными коэффициентами от переменной x с естественными операциями сложения и умножения полиномов.

Определение 1.5.3. Кольцо K называется ассоциативным кольцом, если определенная на нем операция умножения обладает свойством: $(ab)c = a(bc)$ для произвольных $a, b, c \in K$.

Кольцо K называется кольцом с единицей, если оно ассоциативно и имеет нейтральный элемент относительно операции умножения.

Кольцо K называется коммутативным, если $ba = ab$ для произвольных $a, b \in K$.

Пусть K – ассоциативное кольцо с единицей. Множество K^* обратимых относительно умножения элементов кольца K замкнуто относительно этой операции и потому называется мультипликативной группой кольца K.

Пример 1.5.6. Легко видеть, что в кольце целых чисел обратимы относительно умножения только два числа: 1 и –1. Следовательно, $Z^* = \{1, -1\}$. С первого курса вам известно, что $M_n(R)^* = GL_n(R)$. Мультипликативная группа $(Z/nZ)^*$ кольца классов вычетов Z/nZ по модулю n состоит из $\varphi(n)$ классов, порожденных целыми числами, взаимно простыми с модулем, согласно результатам, изложенным в гл. 2 ч. 1 данного пособия.

Определение 1.5.4. Если в кольце K с единицей мультипликативная группа $K^* = K \setminus \{0\}$, то кольцо K называют телом, или алгеброй с делением. Коммутативное тело называют полем.

Пример 1.5.7. Следующие кольца являются полями: а) Q – кольцо рациональных чисел; б) R – кольцо вещественных чисел); в) C – кольцо комплексных чисел; г) Z/pZ – кольцо классов вычетов по простому модулю p.

Пусть P – поле. Пусть $P[x]$ – кольцо полиномов с коэффициентами из P с

обычными операциями сложения и умножения многочленов. По своим свойствам полиномы близки к целым числам. Например, как и для целых чисел имеет место

Теорема 1.5.1 (о делении с остатком для полиномов). *Для любых двух многочленов* $f(x)$ *и* $g(x) \neq 0$ *из кольца* $P[x]$ *существуют единственные многочлены* $q(x)$ *и* $r(x)$, *такие, что* $f(x) = g(x)q(x) + r(x)$, *причем* $r(x) = 0$ *или степень* $r(x)$ *меньше степени* $g(x)$.

Из этой теоремы вытекает известный алгоритм деления многочлена на многочлен «уголком».

Определение 1.5.5. В условиях теоремы о делении с остатком для полиномов многочлен $q(x)$ называют частным, а полином $r(x)$ – остатком от деления $f(x)$ на $g(x)$. Если $r(x) = 0$, то говорят, что $f(x)$ делится на $g(x)$, а $g(x)$ и $q(x)$ называют делителями, или множителями полинома $f(x)$. Если в равенстве $f(x) = g(x) \cdot q(x)$ степени сомножителей не меньше 1, то $q(x)$ и $g(x)$ называют нетривиальными делителями многочлена $f(x)$.

Очевидно, каждый ненулевой элемент поля P является делителем любого многочлена из кольца $P[x]$. Поэтому элементы полей называют тривиальными делителями полиномов. Обратимыми многочленами в кольце полиномов $P[x]$ являются многочлены нулевой степени, отличные от нуля, и только они, т. е. $P[x]^* = P^*$.

Определение 1.5.6. Наибольшим общим делителем многочленов $f_1)x), f_2(x),..., f_s(x)$ называется их общий делитель со старшим коэффициентом 1, который делится на любой другой общий делитель. Его обозначают НОД $(f_1(x), f_2(x),..., f_s(x))$.

Алгоритм Евклида нахождения наибольшего общего делителя, рассмотренный в первом разделе для целых чисел, справедлив и для полиномов.

Теорема 1.5.2. Наибольший общий делитель многочленов $f(x)$ и $g(x)$ из кольца $P[x]$ (с точностью до множителей из поля P) совпадает с последним отличным от нуля остатком $r_n(x)$ следующей цепочки равенств:

$$\begin{cases} f(x) = g(x)\,q_1(x) + r_1(x); \\ g(x) = r(x)\,q_2(x) + r_2(x); \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ r_{n-2}(x) = r_{n-1}(x)\,q_n(x) + r_n(x); \\ r_{n+1}(x) = r_n(x)\,q_{n+1}(x). \end{cases}$$

Пример 1.5.8. Найдем наибольший общий делитель многочленов $f(x) = x^4 + 3x^3 - 4x - 3$ и $g(x) = 3x^3 + 10x^2 + 2x - 3$ в кольце $Q[x]$. Согласно теореме 1.5.2 наибольший общий делитель по алгоритму Евклида получается с точностью до константы. Поэтому и сам алгоритм будем реализовывать с точностью до множителей из Q, с целью проведения вычислений преимуществен-

но с целыми коэффициентами. Последовательным делением «уголком» с учетом сказанного получаем следующую систему равенств алгоритма Евклида:

$$3f(x) = g(x)(x - 1/3) + (-1/3)(5x^2 + 25x + 30) = g(x)q_1(x) + r_1(x);$$

$$g(x) = (x^2 + 5x + 6)(3x - 5) + (9x + 27) = \tilde{r}_1(x)q_2(x) + r_2(x);$$

здесь $\tilde{r}_1(x) = (-3/5)r_1(x)$; $x^2 + 5x + 6 = (x + 3)(x + 2)$, т. е. $\tilde{r}_1(x) = \tilde{r}_2(x)q_3(x)$ для $\tilde{r}_2(x) = (1/9)r\,(x)$. Таким образом, $НОД(f(x), g(x)) = (1/9)r_2(x) = x + 3$.

Определение 1.5.7. Многочлены $f(x)$ и $g(x)$ называют взаимно простыми, если их наибольший общий делитель равен 1.

Обратной «прогонкой» алгоритма Евклида получается следующее утверждение – критерий взаимной простоты двух многочленов.

Теорема 1.5.3. *Многочлены $f(x)$ и $g(x)$ являются взаимно простыми тогда и только тогда, когда найдутся такие полиномы $u(x), v(x)$, для которых выполняется следующее равенство (соотношение Безу для многочленов)*: $f(x)u(x) + g(x)v(x) = 1$.

Определение 1.5.8. Многочлен $f(x) \in P[x]$ степени $n \geq 1$ называется неприводимым в кольце $P[x]$, если в любом его представлении в виде произведения $f(x) = g(x)q(x)$ сомножителей $g(x), q(x) \in P[x]$ один из этих сомножителей является константой, т. е. элементом поля P.

Определение 1.5.9. Корнем многочлена $f(x) \in P[x]$ называется такой элемент поля $\alpha \in P$ (или другого поля, содержащего P), что при подстановке $x = \alpha$ в $f(x)$ получаем равенство $f(\alpha) = 0$.

Теорема 1.5.4 (теорема Безу). *Элемент $\alpha \in P$ (или $\alpha \in F \supset P$) является корнем полинома $f(x) \in P[x]$ степени $n \geq 1$ тогда и только тогда, когда $f(x)$ делится без остатка на $x - \alpha$, т.е. когда выполняется равенство $f(x) = (x - \alpha)\,q(x)$ для некоторого полинома $q(x) \in P[x]$ (для $q(x) \in F[x]$).*

Следствие. Неприводимый полином кольца $P[x]$ степени $n \geq 2$ не имеет корней в поле P.

Теорема Безу позволяет существенно упростить решение алгебраических уравнений: если найден один из корней β полинома $f(x)$, то следует разделить $f(x)$ на $x - \beta$. Тогда остальные корни полинома $f(x)$ являются корнями полинома $q(x)$ – частного от деления $f(x)$ на $x - \beta$.

Определение 1.5.10. Пусть α – корень полинома $f(x) \in P[x]$. Кратностью корня α называется такое натуральное $k \geq 1$, что $f(x)$ делится на $(x - \alpha)^k$, но не делится на $(x - \alpha)^{k+1}$. При $k = 1$ корень α называется простым, а при $k > 1$ – кратным.

Теорема 1.5.5. *Пусть $f(x) \in P[x]$ – многочлен степени $n \geq 1$. Если $\alpha_1, \alpha_2, ..., \alpha_m$ – корни $f(x)$ кратностей $k_1, k_2, ..., k_m$ соответственно, то $f(x)$ делится на произведение $(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2} \cdot ... \cdot (x - \alpha_m)^{k_m}$. Следовательно,*

$k_1 + k_2 + ... + k_m \le n$ *и многочлен* $f(x)$ *имеет не более* n *корней.*

Теорема 1.5.6. *Для неприводимости полинома степени* 2 *или* 3 *в кольце* $P[x]$ *необходимо и достаточно, чтобы он не имел корней в поле* P.

Для неприводимости полинома степени 4 *или* 5 *в кольце* $P[x]$ *необходимо и достаточно, чтобы он не имел корней в поле* P *и не делился ни на какой (неприводимый) полином второй степени. И так далее.*

Структура и многообразие неприводимых полиномов существенно зависят от поля P. Если $P = C$ – поле комплексных чисел, то неприводимыми полиномами в $C[x]$ являются только полиномы 1-й степени, согласно основной теореме алгебры. Отсюда следует, что в кольце $R[x]$ неприводимыми являются лишь полиномы первой степени, а также второй степени с отрицательным дискриминантом. В кольце $Q[x]$ имеются неприводимые полиномы любой степени. В кольце $(Z/pZ)[x]$ также существуют неприводимые полиномы любой степени $n \ge 1$.

Теорема 1.5.6 позволяет реализовать «решето Эратосфена» для нахождения неприводимых полиномов степени $n > 1$ над конечным полем. Данный метод реализуется последовательным делением на неприводимые полиномы степени от 1 до $[n/2]$. В качестве примера приведем список всех неприводимых полиномов в кольце $(Z/2Z)[x]$ степени, меньшей шести.

1) x;
2) $x+1$;
3) $x^2 + x + 1$;
4) $x^3 + x + 1$;
5) $x^3 + x^2 + 1$;
6) $x^4 + x^3 + x^2 + x + 1$;
7) $x^4 + x + 1$;
8) $x^4 + x^3 + 1$;
9) $x^5 + x^2 + 1$;
10) $x^5 + x^3 + 1$;
11) $x^5 + x^3 + x^2 + x + 1$;
12) $x^5 + x^4 + x^2 + x + 1$;
13) $x^5 + x^4 + x^3 + x + 1$;
14) $x^5 + x^4 + x^3 + x^2 + 1$.

Неприводимые полиномы играют роль простых чисел кольца целых чисел. Аналогично основной теореме арифметики доказывается

Теорема 1.5.7. *Всякий многочлен* $f(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$ *с коэффициентами из поля* P *степени* $n \ge 1$ *представим в виде произведения* $f(x) = a_n p_1(x) p_2(x) \cdot ... \cdot p_s(x)$, *где* $p_i(x)$ *– неприводимые полиномы со старшим коэффициентом, равным* 1. *Такое представление единственно с точностью до порядка сомножителей.*

Процедура конкретной факторизации полинома в произведение неприводимых достаточно трудоемка, зависит существенным образом от поля коэффициентов, имеет массу методик и подходов.

Глава 6. Основы теории конечных полей

В кольце полиномов $P[x]$ зафиксируем полином $f(x)$ степени $n > 1$. Множество всех остатков от деления полиномов из $P[x]$ на $f(x)$ состоит из

всевозможных полиномов, степени которых меньше n. Его называют фактор-множеством кольца полиномов $P[x]$ по идеалу $J = < f(x) >$, порожденному полиномом $f(x)$, и обозначают его через $F = P[x]/ < f(x) >$. Фактически это n-мерное пространство над полем P со стандартным базисом $x^{n-1}, x^{n-1}, ..., x, 1$. Поэтому всякий остаток из F можно записывать или в виде полинома $g(x) = a_{n-1}x^{n-1} + ... + a_1 x + a_0$ или в виде вектора $(a_{n-1},...,a_1,a_0)$.

На фактор-множестве $P[x]/ < f(x) >$ определены индуцированные операции сложения $\oplus$ и умножения $\otimes$: произведением $g(x) \otimes h(x)$ остатков $g(x)$ и $h(x)$ называется тот единственный полином $r(x) \in P[x]/ < f(x) >$, который равен остатку от деления произведения $g(x)h(x)$ на $f(x)$.

Поскольку операции $\oplus$ и $\otimes$ полностью определяются сложением и умножением в кольце $P[x]$, то свойства этих операций переносятся на фактор-множество. Поэтому справедлива

Теорема 1.6.1. *Фактор-множество $P[x]/ < f(x) >$ является ассоциативным и коммутативным кольцом с единицей относительно индуцированных с поля P операций и называется фактор-кольцом.*

Пример 1.6.1. Кольцо классов вычетов Z/nZ есть фактор-кольцо кольца целых чисел Z по двустороннему идеалу $J = nZ$.

Пример 1.6.2. Пусть $P = Z/pZ$. В кольце $(Z/pZ)[x]$ имеется, как нетрудно заметить, в точности p^n различных полиномов степени, меньшей n. Поэтому для полинома $f(x)$ степени $n \geq 1$ фактор-кольцо $(Z/pZ)[x]/ < q(x) >$ конечно и состоит из p^n элементов. Следовательно, сложение и умножение в этом кольце можно задать конкретно в виде таблиц.

Пример 1.6.3. Кольцо $F = (Z/2Z)[x]/ < x^2 + x + 1 >$ состоит из смежных классов $\bar{0}$, $\bar{1}$, $\bar{x}$, $\overline{x+1}$. Напишем таблицы сложения и умножения в этом кольце.

$\oplus$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{x}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{x}$	$\bar{1}$	$\bar{0}$

$\otimes$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{x}$	$\overline{x+1}$
$\bar{x}$	$\bar{x}$	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	$\bar{1}$	$\bar{x}$

Из таблицы умножения следует, что в кольце F все ненулевые элементы обратимы относительно умножения, т. е. $F^* = F \setminus \{0\}$. Следовательно, F – поле из четырех элементов.

Теорема 1.6.2. *Если $f(x)$ – неприводимый полином, то фактор-кольцо $P[x]/ < f(x) >$ является полем. Если при этом $P = Z/pZ$ – поле из p элементов для простого числа p, а степень неприводимого полинома $f(x)$ равна $n \geq 1$, то фактор-кольцо $(Z/pZ)[x]/ < f(x) >$ – поле из p^n элементов.*

Как уже отмечалось, поля выделяются из общего многообразия коммутативных колец наличием максимально возможной мультипликативной группы – в нее входят все ненулевые элементы, отсутствием делителей нуля, отсутствием собственных идеалов. Важнейшим из свойств каждого поля является его характеристика.

Определение 1.6.1. Если в поле P существует такое натуральное n, что равна нулю сумма n единиц (n раз складывается с самим собой 1 – нейтральный элемент относительно умножения) $1+1+...+1=0$, то наименьшее n с таким свойством называется характеристикой поля P и обозначается через $charP$. Если в поле P любая конечная сумма единиц отлична от нуля, то говорят, что характеристика поля P равна 0.

Теорема 1.6.3. *Если характеристика поля отлична от нуля, то она является числом простым.*

Например, характеристика поля $P = Z/pZ$, p – простое, равна p. А поля Q, R, C имеют, очевидно, характеристику 0. Поле P называется подполем поля P', если все его элементы принадлежат полю P'. Если подполе поля P имеет характеристику p, то и поле P' имеет ту же характеристику. Все подполя поля P имеют ту же характеристику.

Вам уже знакомы поля характеристики 0. С их точки зрения арифметика полей положительной характеристики весьма экзотична.

Теорема 1.6.4. *Пусть P – произвольное поле положительной характеристики p. Пусть n – произвольное целое число и r – остаток от деления n на p. Тогда для каждого элемента $a \in P$ имеет место равенство: $na = ra$. В частности, при $n = pq$ произведение $na = pqa = 0$. Если $p = 2$, то при $n = 2k$ произведение $na = 2ka = 0$, а при $n = 2k+1$ произведение $na = (2k+1)a = a$.*

Мы хорошо знаем формулу бинома Ньютона $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$. В полях характеристики p при $n = p^k$ формула бинома Ньютона выглядит совершенно по-другому.

Теорема 1.6.5. *Пусть $charP = p > 0$. Тогда для любых $a, b \in P$ $(a+b)^p = a^p + b^p$; $(a-b)^p = a^p - b^p$; а для каждого целого $k \geq 1$ $(a+b)^{p^k} = a^{p^k} + b^{p^k}$; $(a-b)^{p^k} = a^{p^k} - b^{p^k}$.*

Определение и основные свойства векторных пространств над полем R переносятся на произвольные поля. При этом векторное пространство над конечным полем имеет свои особенности.

Теорема 1.6.6. *Пусть V – n-мерное линейное пространство над полем $F(q)$ из q элементов. Тогда V состоит из q^n векторов.*

Определение 1.6.2. Если P является подполем поля F, то F называют расширением поля P.

Очевидно, любое расширение произвольного поля P является векторным пространством над P.

Определение 1.6.3. Расширение F поля P называется конечным (степени n), если размерность векторного пространства F над полем P конечна (и равна n). Степень расширения принято обозначать через $[F:P]$.

Из теоремы 1.6.6 получаем, что расширение F степени n конечного поля $F(q)$ из q элементов состоит из q^n элементов.

Теорема 1.6.7 (теорема о башне расширений полей). *Если поле F есть расширение поля P степени n, а поле H – расширение F степени m, то H есть расширение P степени $[H:P]=mn$.*

Следствие. Если степень расширения $[F:P]=q$ – число простое, то поле F не содержит подполей, промежуточных между F и P.

Определение 1.6.4. Элемент $\alpha \in F$ – расширения поля P – является алгебраическим над полем P, если существует полином $f(x) \in P[x]$, корнем которого является α, то есть $f(\alpha)=0$ В противном случае α называют трансцендентным над P элементом. Поле F называется алгебраическим расширением поля P, если всякий элемент из F является алгебраическим над полем P.

Теорема 1.6.8. *Всякое конечное расширение произвольного поля P является алгебраическим над P.*

Определение 1.6.5. Пусть $\alpha \in F$ – алгебраический над полем P элемент. Минимальным полиномом элемента α над полем P называется неприводимый полином $Irr(\alpha, P, x)$ в кольце $P[x]$, старший коэффициент которого равен 1, а одним из корней является элемент α.

Теорема 1.6.9. *Пусть F – расширение поля P, пусть $\alpha \in F$ – алгебраический над P элемент с минимальным над P полиномом степени $n>1$. Пусть $P(\alpha)$ – минимальное подполе поля F, содержащее P и α. Тогда степень расширения $[P(\alpha):P]=n$, а поле $P(\alpha)$ имеет следующую структуру:*

$$P(\alpha)=\{a_0+a_1\alpha+\ldots+a_{n-1}\alpha^{n-1};\ a_i \in P,\ 0 \le i \le n-1\}.$$

Другими словами, поле $P(\alpha)$ изоморфно фактор-кольцу $P[x]/<Irr(\alpha,P,x)>$.

Конечные поля были впервые введены в математическую практику в начале XIX в. гениальным французским математиком Эваристом Галуа. Поэтому конечные поля часто называют полями Галуа, а также на письме обозначают через $GF(q)$ – поле Галуа из q элементов. Будем использовать и более краткое

обозначение этого же поля $-F(q)$. Перечислим основные свойства конечных полей.

Свойство 1. Любое конечное поле $GF(q)$ элементов имеет конечную характеристику $p>0$, является конечным расширением поля Z/pZ, содержит $q=p^k$ элементов, при этом k – степень расширения $[GF(q):Z/pZ]$.

Свойство 2. Для каждого простого число p и для любого натурального $n\geq 1$ существует конечное поле из $q=p^n$ элементов. Это поле единственно с точностью до изоморфизма, состоит из корней уравнения $x^q-x=0$ и только из них.

Свойство 3. Пусть $F(p^n)$ и $F(p^k)-$ конечные поля, расширения поля $Z/pZ=F(p)$, причем $1<k<n$. Поле $F(p^k)$ является подполем $F(p^n)$ тогда и только тогда, когда k делит n. Для каждого натурального делителя d числа n существует и единственно подполе $F(p^n)$ из p^d элементов.

Свойство 4. Мультипликативная группа конечного поля – циклическая.

Определение 1.6.6. Образующие мультипликативной группы конечного поля называют примитивными элементами этого поля.

Свойство 5. Каждый примитивный элемент поля Галуа $F(p^n)$ является корнем неприводимого полинома степени n из кольца $F(p)[x]$.

Определение 1.6.7. Неприводимый полином $f(x)\in Z/pZ[x]$ степени n называется примитивным полиномом, если его корни – примитивные элементы поля Галуа $F(p^n)$.

В гл. 5 ч. 1 приведен список неприводимых полиномов над полем $Z/2Z$. Среди них – неприводимые полиномы 4-й степени, всего три полинома. Под №6 списка фигурирует полином $f(x)=x^4+x^3+x^2+x+1$. Это не примитивный полином. Действительно, пусть α – корень $f(x)$, принадлежащий полю $F(2^4)$. Порядок $F(2^4)^*=15$. Найдем порядок элемента α в этой группе. $\alpha^4=\alpha^3+\alpha^2+\alpha+1$. Тогда

$$\alpha^5=\alpha\cdot\alpha^4=\alpha^4+\alpha^3+\alpha^2+\alpha=(\alpha^3+\alpha^2+\alpha+1)+\alpha^3+\alpha^2+\alpha=1.$$

Таким образом, элемент α имеет мультипликативный порядок 5 и, следовательно, не является примитивным. Но тогда и полином $f(x)$ непримитивен. По данной схеме можно разделять неприводимые полиномы на примитивные и непримитивные.

Свойство 6. Для каждого натурального n и фиксированного простого числа p существует единственное расширение $F(p^n)$ поля Z/pZ, состоящее из p^n элементов, оно изоморфно полю $(Z/pZ)[x]/<p(x)>$ для любого неприводимого полинома $p(x)$ степени n из кольца $Z/pZ[x]$.

Свойство 7. Всякое конечное поле $F(p^n)$ состоит из всевозможных полиномов степени, меньшей n, с коэффициентами из поля $F(p)=Z/pZ$. Склады-

ваются и вычитаются эти полиномы как обычно, умножаются почленно с учетом равенства $x^n = -a_{n-1}x^{n-1} - ... - a_1 x - a_0$ для фиксированного неприводимого полинома степени n из кольца $Z / pZ[x]$.

Согласно свойству 7 неприводимые полиномы необходимы для формирования конечных полей и вычислений в них: данное поле $F(p^n)$ можно рассматривать как множество сумм вида $\{a_0 + a_1\alpha + ... + a_{n-1}\alpha^{n-1} \mid a_i \in F(p)\}$, где α – корень неприводимого полинома $f(x)$ степени n из кольца $F(p)[x]$. В отдельных ситуациях для формирования конечных полей пользуются принципиально не примитивными полиномами (например, в криптосистеме AES). Однако тогда умножение элементов поля Галуа требует громоздких выкладок. Для непосредственных вычислений в полях Галуа удобнее формировать их с помощью примитивных полиномов. Ведь если α – примитивный элемент поля $F(p^n)$, то все элементы этого поля исчерпываются множеством $\{0, \alpha, \alpha^2, ..., \alpha^{p-1} = 1\}$ и перемножать степени α друг с другом намного проще и удобнее. Чтобы сочетать оба преимущества, следует задавать поле либо в виде системы равенств (отождествляющих оба способа задания поля), либо в виде таблицы степеней и сумм.

Пример 1.6.4. Сформируем поле $F(8) = F(2^3)$. Поскольку $2^3 - 1 = 7$ – число простое, то над полем из двух элементов все неприводимые полиномы третьей степени являются примитивными. Зафиксируем неприводимый полином степени 3, например, $p(x) = x^3 + x + 1$. Обозначим через α его корень, принадлежащий $F(8)$. Тогда $\alpha^3 = \alpha + 1$ (так как характеристика поля $F(8)$ равна 2, то $-1 = 1$). Тогда

$$\alpha^4 = \alpha^2 + \alpha,\ \alpha^5 = \alpha^3 + \alpha^2 = \alpha^2 + \alpha + 1,\ \alpha^6 = \alpha^3 + \alpha^2 + \alpha = \alpha^2 + 1,$$

$$\alpha^7 = \alpha^3 + \alpha = \alpha + \alpha + 1 = 1,\ 0 = \alpha^{-\infty}.$$

Следовательно, поле $F(8)$ можно задать в виде таблицы из двух столбцов: в левом столбце запишем все различные степени α, в правом – соответствующие этим степеням суммы вида $a_2\alpha^2 + a_1\alpha + a_0$.

Таблица элементов поля $F(8)$

$\alpha^{-\infty}$	0
α^1	α
α^2	α^2
α^3	α+1
α^4	α^2+α
α^5	α^2+α+1
α^6	α^2+1
α^7	1.

Пример 1.6.5. Решить над полем $F(8)$ следующую систему уравнений:

$$(\alpha^2+1)\,x+(\alpha^2+\alpha+1)\,y=1,$$

$$\alpha^2 x+(\alpha+1)\,y=\alpha^2+1.$$

Решим систему по правилу Крамера. Для вычислений воспользуемся приведенной выше таблицей задания поля $F(8)$. Определитель матрицы коэффициентов системы таков:

$$\delta=\begin{vmatrix}\alpha^2+1 & \alpha^2+\alpha+1\\ \alpha^2 & \alpha+1\end{vmatrix}=\alpha^3+\alpha^2+\alpha+1+\alpha^4+\alpha^3+\alpha^2=\alpha^2+1.$$

$$\delta_x=\begin{vmatrix}1 & \alpha^2+\alpha+1\\ \alpha^2+1 & \alpha+1\end{vmatrix}=\alpha+1+\alpha^4+\alpha^3+\alpha^2+\alpha^2+\alpha+1=\alpha^4+\alpha^3=\alpha^2+1.$$

$$\delta_y=\begin{vmatrix}\alpha^2+1 & 1\\ \alpha^2 & \alpha^2+1\end{vmatrix}=\alpha^4+1+\alpha^2=\alpha+1.$$

Следовательно,

$$x=\delta_x/\delta=1;\;\; y=\delta_y/\delta=(\alpha+1)/(\alpha^2+1)=1/\alpha^3=\alpha^4=\alpha^2+\alpha.$$

Итак, задание элементов поля Галуа суммами удобно при сложении элементов поля; для умножения удобнее пользоваться степенным заданием элементов поля.

Глава 7. Элементы помехоустойчивого кодирования

Конечные поля имеют многочисленные приложения. Без них немыслимо функционирование практически всех цифровых систем связи.

Все реально действующие цифровые системы связи построены на двоичной арифметике, хотя теоретически их можно строить в полях с любой характеристикой. Реально информация передается блоками фиксированной длины n, т. е. векторами из пространства размерности n над полем $Z/2Z$. Так, в сотовых системах связи $n=31$, планируется переход на длину $n=63$. На советских космических кораблях, исследовавших Венеру, связь для которых была построена усилиями ученых МРТИ (сегодня БГУИР), длина кодовых слов была равна $n=1023$.

Все функционирующие в цифровой системе связи блоки информации называют кодовыми словами. Дело в том, что не всякий блок длиной n является кодовым словом. Кодовые слова образуют подпространство размерности $k<n$. Подлинные информационные передаваемые слова представляют собой всевозможные двоичные блоки длиной k. Их кодируют умножением на специально подобранную двоичную матрицу G порядка $k\times n$, которую называют порождающей матрицей кода. Удлинение информационных слов означает введение в них избыточной информации для устранения искажений, возникающих в про-

цессе передачи этой информации. При правильно подобранной матрице G кодовые слова будут разбросаны друг от друга на некоторые расстояния в смысле метрики Хемминга. Наименьшее из них – d – называется минимальным или кодовым расстоянием.

На приемном устройстве каждой системы связи сформирована другая матрица, называемая проверочной. Если кодовое слово $\bar{c}$ достигло приемного устройства без искажений, то проверочная матрица H выдаст однозначный результат $H \cdot \bar{c}^T = \bar{0}^T$. Если же приемное устройство получило вектор $\bar{x} = \bar{c} + \bar{e}$ с ненулевым вектором ошибок $\bar{e}$, то приемное устройство выдаст вектор $S = H(\bar{x})^T = H(\bar{e})^T \neq \bar{0}^T$, называемый синдромом ошибок. Автоматически проводится анализ синдрома, точно определяется вектор ошибок $\bar{e}$ и на выход подается исправленный вектор $\bar{c}$.

Исторически первыми были коды Хемминга. Их параметры

$$n = 2^m - 1,\ m > 1;\ k = n - m;\ d = 3;$$

проверочная матрица $H = (1, \alpha, \alpha^2, ..., \alpha^{n-1})$, где α – примитивный элемент поля Галуа $GF(2^m)$. Наиболее распространенными кодами являются коды Боуза – Чоудхури – Хоквингема (БЧХ-коды), а также реверсивные коды, исправляющие двойные ошибки. Такие БЧХ-коды задаются матрицами $H = (\alpha^i, \alpha^{3i})^T$, где $0 \le i \le 2^m - 2$, α – примитивный элемент поля Галуа $GF(2^m)$. Реверсивные коды задаются матрицами $H = (\alpha^i, \alpha^{-i})^T$, $0 \le i \le 2^m - 2$, α – примитивный элемент поля Галуа $F(2^m)$. При этом в каждой матрице каждый элемент $\alpha^i = a_{n-1}\alpha^{n-1} + ...a_1\alpha + a_0$ заменен двоичным столбцом $(a_{n-1}, ..., a_1, a_0)^T$.

Пример 1.7.1. В системе связи, построенной на основе БЧХ-кода C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le 14$, α – примитивный элемент поля Галуа $F(16)$, корень полинома $x^4 + x + 1$, выяснить, не содержит ли ошибок принятое сообщение $\bar{x} = (111011110110101)$.

Решение. Все кодовые слова $\bar{c} \in C$ (и только они) составляют ядро проверочной матрицы: $H \cdot (\bar{c}^T) = \bar{0}$. Если $\bar{s} = H(\bar{x}^T) \neq \bar{0}$, то сообщение $\bar{x}$ явно содержит ошибки, а вектор $\bar{s}$ называют синдромом этих ошибок. В данном случае $\bar{s} = (s_1, s_2)^T$, где

$$s_1 = 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{10} + \alpha^{12} + \alpha^{14},$$

$$s_2 = 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21} + \alpha^{27} + \alpha^{30} + \alpha^{36} + \alpha^{42}.$$

Читателю предлагается сформировать по аналогии с примером 1.6.4 конечное поле $F(16)$, построить двоичную матрицу H, провести необходимые вычисления и убедиться, что $s_1 = \alpha^{11} = \alpha^3 + \alpha^2 + \alpha$, $s_2 = \alpha$. Таким образом, полученное сообщение $\bar{x}$ содержит ошибки.

Пример 1.7.2. Построим матрицу БЧХ-кода длиной $n = 2^3 - 1 = 7$ над полем $F(8)$ с примитивным элементом α – корнем полинома $x^3 + x + 1$. Это поле сформировано в примере 1.6.4. С учетом сказанного выше

$$H = \begin{pmatrix} \alpha^i \\ \alpha^{3i} \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^5 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Предположим, что устройство связи с данным кодом приняло сообщение $\bar{x} = (110\,110\,1)$. Проверим наличие ошибок в нем. Для этого вычислим произведение:

$$H \cdot (\bar{x})^T = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ \alpha^5 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Следовательно, принятое сообщение содержит ошибки.

Задания для аудиторной работы

Задание 1.1. Найти канонические разложения натуральных чисел $a = 110$ и $b = 68$. Вычислить $\text{НОД}(a, b)$ и $\text{НОК}(a, b)$.

Решение. $110 = 11 \cdot 5 \cdot 2$; $68 = 17 \cdot 2^2$. Из канонических разложений видим, что $\text{НОД}(110, 68) = 2$ и $\text{НОК}(110, 68) = 11 \cdot 5 \cdot 17 \cdot 2^3 = 7480$.

Задание 1.2. Вычислить $\text{НОД}(110, 48)$ с помощью алгоритма Евклида.

Решение. $110 = 48 \cdot 2 + 14$; $48 = 14 \cdot 3 + 6$; $14 = 6 \cdot 2 + 2$; $6 = 2 \cdot 3$. Следовательно, $\text{НОД}(110, 48) = 2$.

Задание 1.3. С помощью расширенного алгоритма Евклида найти целые числа u, υ, удовлетворяющие соотношению Безу: $au + b\upsilon = \text{НОД}(a, b)$ для целых чисел $a = 110$ и $b = 48$.

Решение. Воспользуемся вычислениями $\text{НОД}(110, 48)$ из задания 1.2. Обратной прогонкой алгоритма Евклида построим соотношение Безу для данных $a = 110$ и $b = 48$.

$110 = 48 \cdot 2 + 14$; поэтому $14 = 110 + 48 \cdot (-2)$;

$48 = 14 \cdot 3 + 6$; поэтому $6 = 48 + 14 \cdot (-3)$;

$14 = 6 \cdot 2 + 2$; поэтому $2 = 14 + 6 \cdot (-2)$. В это равенство подставим полученное выше выражение для 6 и приведем подобные относительно чисел 48 и 14. Итак, $2 = 14 + 6 \cdot (-2) = 14 + (48 + 14 \cdot (-3))(-2) = 14 \cdot 7 + 48 \cdot (-2)$.

В полученное выражение для $\text{НОД}(110, 48) = 2$ подставим вышеприведенное выражение числа 14. Получим окончательно:

$$2 = 14 \cdot 7 + 48 \cdot (-2) =$$

$= (110 + 48 \cdot (-2))\, 7 + 48 \cdot (-2) = 110 \cdot 7 + 48 \cdot (-16)$. $u = 7$; $v = -14$.

Задание 1.4. Выполнить предыдущие задания 1.1 – 1.3 для пар чисел:

а) 8281 и 3234; б) 6075 и 1296.

Задание 1.5. Вычислить $\varphi(n)$ для чисел n: а) в диапазоне от 2 до 12; б) 68, 69, 70; в) 2000 и 2001.

Решение. Найдем $\varphi(2001)$. Для этого найдем каноническое разложение числа 2001. $2001 = 3 \cdot 667 = 3 \cdot 23 \cdot 29$. Поэтому

$$\varphi(2001) = \varphi(3) \cdot \varphi(23) \cdot \varphi(29) = 2 \cdot 22 \cdot 28 = 1232.$$

$$2000 = 2^4 \cdot 5^3.$$

Поэтому $\varphi(2000) = \varphi(2^4) \cdot \varphi(5^3) = (2^4 - 2^3) \cdot (5^3 - 5^2) = 800$.

Задание 1.6. Построить таблицы сложения и умножения в кольцах $Z/6Z$, $Z/7Z$ и $Z/9Z$.

Задание 1.7. Указать пары взаимообратных элементов относительно умножения в кольцах из задания 1.6. Обосновать их отсутствие для отдельных классов.

Решение. В любом кольце Z/nZ класс $\overline{0}$ никогда не обратим, обратимы

лишь те классы $\overline{k}$, для которых $\text{НОД}(k, n) = 1$. Поэтому их общее количество совпадает с числом $\varphi(n)$. $\text{НОД}(3, 9) = 3$; $\text{НОД}(6, 9) = 3$. Следовательно, в кольце $Z/9Z$ классы $\overline{3}$ и $\overline{6}$ не обратимы и имеется $\varphi(9) = 6$ обратимых классов: $\overline{1},\ \overline{1}^{-1} = \overline{1}$; $\overline{2},\ \overline{2}^{-1} = \overline{5}$; $\overline{4},\ \overline{4}^{-1} = \overline{7}$; $\overline{5},\ \overline{5}^{-1} = \overline{2}$; $\overline{7},\ \overline{7}^{-1} = \overline{4}$; $\overline{8},\ \overline{8}^{-1} = \overline{8}$.

Задание 1.8. Являются ли циклическими мультипликативные группы $Z/6Z^*$, $Z/7Z^*$ и $Z/9Z^*$?

Решение. Группа $Z/9Z^*$ состоит из $\varphi(9) = 6$ элементов: $\overline{1};\ \overline{2};\ \overline{4};\ \overline{5};\ \overline{7};\ \overline{8}$. Все они принадлежат циклической группе $< \overline{2} > = \{\overline{2}; \overline{4}; \overline{8}; \overline{7}; \overline{5}; \overline{1}\}$. Таким образом, группа $Z/9Z^*$ является циклической.

Задание 1.9. Расшифровать криптограмму Цезаря:

а) ЕФИ РЗ ХГН ОЗЁНС, НГН НГЙЗХФВ. (КГНСР ПЗУЧЛ);

б) ЦРЩЛВ УЗТЦХГЩЛЛ ФХСЛХ ЧЦРХГ УГДСХЮ.

Задание 1.10. Перевести с тарабарского:

а) ЖОГЕВЬ ЩЫКЬ ЛГАЛКСИШЫР – ЩУЦЬ ИР. Т. НМУКТОШ;

б) ПА ОФАМЕППЫЙ НОКОСОТ СОХИСИЛЬ КЕПИ

Задание 1.11. Следующий текст зашифрован с помощью девиза «Роза»:

а) щшхоъьюпэюмпюяицягфпяпшпэососынтс;

б) жгмпшэсльпщуъэьггнцпилщйгюкбэ.

Расшифруйте данный текст.

Задание 1.12. Прочитайте текст, зашифрованный методом постолбцовой транспозиции $(n = 5, m = 6)$.

а) унёрв ыесит ррнпс нхапо мтлае гпаок;

б) чисра сютше руаоц внядё массе левху.

Задание 1.13. Расшифруйте криптосообщение RSA.

а) {ш,e,n}={196,11,209}; б) {ш,e,n}={253,7,527}.

Задание 1.14. Расшифруйте криптосообщение Эль Гамаля.

а) {m,O,P,g,h,x}={17,14,37,5,18,7}; б) {m,O,P,g,h,x}={29,19,41,11,16,8}.

Задание 1.15. Исследовать на неприводимость следующие полиномы из кольца $Z/2Z[x]$: а) $x^4 + x^2 + 1$; б) $x^6 + x^5 + x^3 + x + 1$; в) $x^4 + x^3 + 1$.

Решение. В случае а) полином приводим: $x^4 + x^2 + 1 = (x^2 + x + 1)^2$. В случае в) полином неприводим, т. к. удовлетворяет условиям теоремы 5.6: элементы 0 и 1 поля $Z/2Z$ не являются его корнями и полином этот не делится на единственный неприводимый полином второй степени $x^2 + x + 1$.

Задание 1.16. Исследовать неприводимый полином $x^4 + x^3 + 1$ на примитивность.

Решение. Всякий неприводимый полином

$$p(x) = x^m + a_{m-1}x^{m-1} \ldots + 1 \in Z/2Z[x]$$

порождает конечное поле $GF(2^m)$ из 2^m элементов. Согласно теории конечных полей, поле $GF(2^m) = Z/2Z[x]/ < p(x) > -$ является фактор-кольцом кольца полиномов $Z/2Z[x]$ по идеалу $J = < p(x) >$, порожденному полиномом $p(x)$. Другими словами, $GF(2^m)$ состоит из полиномов – всевозможных остатков от деления на полином $p(x)$. Это множество всех полиномов, степени которых меньше m. Остатки эти в поле $GF(2^m)$ складываются обычным образом, а умножаются по модулю $p(x)$. Например, $\bar{x}^i \cdot \bar{x}^{m-i} = a_{m-1}\bar{x}^{m-1} + ... + 1$. Из-за этого специфического умножения элементы фактор-кольца обозначаются не как обычные полиномы $f(x)$, а выражением $\overline{f(x)}$ аналогично элементам Z/nZ. В фактор-кольце $GF(2^m) = Z/2Z[x]/ < p(x) >$ всегда имеется корень полинома $p(x)$. Им является элемент $\alpha = \bar{x}$. Неприводимый полином $p(x)$ называется примитивным, если циклическая группа $< \alpha >= GF(2^m)^*$. Данное равенство эквивалентно тому, что минимальная степень k, такая, что $\alpha^k = 1$, равна $2^m - 1$.

Итак, для проверки примитивности полинома $p(x)$ следует вычислить цепочку степеней α с учетом фундаментального соотношения $\alpha^m = a_{m-1}\alpha^{m-1} + a_{m-2}\alpha^{m-2} + ... + 1$ до получения 1. Если $\alpha^k = 1$ для целого k, $1 < k < 2^m - 1$, то $p(x)$ – неприводимый, но не примитивный полином. Если же $\alpha^k = 1$ для минимального $k = 2^m - 1$, то $p(x)$ – примитивный полином.

Пусть α – корень полинома $x^4 + x^3 + 1 \in Z/2Z[x]$. Здесь $2^m - 1 = 15$. Имеем:

$\alpha^4 = \alpha^3 + 1$; $\alpha^5 = \alpha^4 + \alpha = \alpha^3 + \alpha + 1$; $\alpha^6 = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1$; $\alpha^7 = \alpha^2 + \alpha + 1$; $\alpha^8 = \alpha^3 + \alpha^2 + \alpha$; $\alpha^9 = \alpha^2 + 1$; $\alpha^{10} = \alpha^3 + \alpha$; $\alpha^{11} = \alpha^3 + \alpha^2 + 1$; $\alpha^{12} = \alpha + 1$; $\alpha^{13} = \alpha^2 + \alpha$; $\alpha^{14} = \alpha^3 + \alpha^2$; $\alpha^{15} = 1$.

Следовательно, данный полином $x^4 + x^3 + 1$ является примитивным.

Задание 1.17. С помощью примитивного полинома $p(x) = x^4 + x^3 + 1$ сформировать поле Галуа $GF(2^4)$.

Решение. Для работы с конечным полем $GF(2^m)$ необходимо иметь под рукой три основных задания этого поля и знать взаимосвязь между этими заданиями. Основные задания поля: 1) мультипликативное, или степенное – в виде степеней примитивного элемента α; 2) аддитивное, или полиномиальное – в виде полиномов из $Z/2Z[x\}$, степени которых меньше m; 3) векторное – в виде векторов из m-мерного векторного пространства над полем $Z/2Z$. Взаимосвязь между вторым и третьим заданиями простая: полиному

$g(x) = b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + ... + b_0$ соответствует m-мерный вектор $(b_{m-1}, b_{m-2}, ..., b_0)$. Взаимосвязь же между первым и вторым заданиями задается таблицей степеней α. Для полноты картины можно взять $0 = \alpha^{-\infty}$.

С учетом сказанного поле $GF(2^4)$ задается табл. 1.1.

Таблица 1.1

Элементы поля $GF(2^4)$, сформированные на основе полинома

$$p(x) = x^4 + x^3 + 1$$

Степенное задание	Полиномиальное задание	Векторное задание
α	α	(0, 0, 1, 0)
α^2	α^2	(0, 1, 0, 0)
α^3	α^3	(1, 0, 0, 0)
α^4	$\alpha^3 + 1$	(1, 0, 0, 1)
α^5	$\alpha^3 + \alpha + 1$	(1, 0, 1, 1)
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$	(1, 1, 1, 1)
α^7	$\alpha^2 + \alpha + 1$	(0, 1, 1, 1)
α^8	$\alpha^3 + \alpha^2 + \alpha$	(1, 1, 1, 0)
α^9	$\alpha^2 + 1$	(0, 1, 0, 1)
α^{10}	$\alpha^3 + \alpha$	(1, 0, 1, 0)
α^{11}	$\alpha^3 + \alpha^2 + 1$	(1, 1, 0, 1)
α^{12}	$\alpha + 1$	(0, 0, 1, 1)
α^{13}	$\alpha^2 + \alpha$	(0, 1, 1, 0)
α^{14}	$\alpha^3 + \alpha^2$	(1, 1, 0, 0)
α^{15}	1	(0, 0, 0, 1)
$\alpha^{-\infty}$	0	(0, 0, 0, 0)

Задание 1.18. Выписать проверочную матрицу $H = (\alpha^i)^T$ (15, 11) – кода Хемминга C_X, где $0 \le i \le 2^m - 2$, α – корень полинома $p(x) = x^4 + x^3 + 1$.

Решение. Для формирования матрицы H воспользуемся третьим столбцом табл. 1.1. Элементы его запишем последовательно в столбцы проверочной матрицы кода Хемминга:

$$H = \left(1\ \alpha\ \alpha^2 ... \alpha^{14}\right) = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \end{pmatrix}.$$

Задание 1.19. Выписать проверочную матрицу $H = (\alpha^i, \alpha^{3i})^T$ (15, 7) – БЧХ-кода C_5, где $0 \le i \le 2^m - 2,\ \alpha -$ корень полинома $p(x) = x^4 + x^3 + 1.$

Решение. Воспользуемся табл. 1.1 для формирования матрицы H. При этом будем учитывать, что $\alpha^{31 \cdot q + r} = \alpha^r$. С учетом сказанного

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Задание 1.20. Выписать проверочную матрицу $H = (\alpha^i, \alpha^{-i})^T$ реверсивного (15, 7)-кода C_R, где $0 \le i \le 2^m - 2,\ \alpha -$корень полинома $p(x) = x^4 + x^3 + 1.$

Решение. Воспользуемся табл. 1.1 для формирования матрицы H_R. При этом будем учитывать, что $\alpha^{31 \cdot q + r} = \alpha^r$. С учетом сказанного

$$H_R = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}..$$

Задание 1.21. Устройство связи с помехоустойчивым реверсивным кодом из задания 1.20 приняло сообщение

$$\bar{x} = (1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 1\ \ 0\ \ 0).$$

Содержит ли принятое сообщение ошибки?

Решение. Наличие ошибок в принятом сообщении $\bar{x}$ определяет проверочная матрица $H = H_R$: если $H \cdot \bar{x}^T = \bar{0},$ то сообщение принято без ошибок, если же $H \cdot \bar{x}^T = S \ne \bar{0},$ то принятое сообщение содержит ошибки. Непосредственные вычисления показывают, что в данном случае

$H \cdot \bar{x}^T = (1\ \ 0\ \ 0\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0)^T \neq \bar{0}$. Следовательно, принятое сообщение содержит ошибки.

Задание 1.22. Устройство связи с помехоустойчивым БЧХ-кодом из задания 1.19 приняло сообщение $\bar{x} = (1\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1\ \ 0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 1\ \ 1)$. Найти его синдром ошибок. Содержит ли принятое сообщение ошибки?

Решение. Синдром ошибок в принятом сообщении $\bar{x}$ вычисляется по формуле: $S = H \cdot \bar{x}^T$, где H – матрица из решения задания 1.19. Вычисления показывают, что в данном случае $S = H \cdot \bar{x}^T = (0\ \ 0\ \ 0\ \ 1\ \ 0\ \ 0\ \ 0\ \ 0)^T \neq \bar{0}^T$. Следовательно, сообщение $\bar{x}$ содержит ошибки.

Контрольная работа «Прикладная математика»

Задание 1. Даны натуральные числа a и b. Найти их каноническое разложение. Вычислить их наибольший общий делитель и наименьшее общее кратное. Вычислить НОД(a, b) с помощью алгоритма Евклида. Выписать соотношение Безу для чисел a и b с помощью расширенного алгоритма Евклида.

Задание 2. Вычислить $\varphi(a)$, $\varphi(b)$ для a и b из задания 1, $\varphi(n)$, где $n = 2010 + k$, k – номер вашего варианта в данной контрольной работе.

Задание 3. Построить таблицы сложения и умножения в кольце классов вычетов Z/mZ, где $m = 10 + k$, k – номер вашего варианта в данной контрольной работе. К каждому классу из Z/mZ указать обратный класс или обосновать его отсутствие. Сравнить количество всех обратимых классов с $\varphi(m)$. Циклична ли группа Z/mZ^*?

Задание 4. Установить истинное сообщение, зашифрованное классическим методом.

Задание 5. Расшифровать криптосообщение RSA.

Задание 6. Расшифровать криптосообщение Эль Гамаля.

Задание 7. Убедиться в неприводимости и примитивности данного полинома $p(x)$ пятой степени с коэффициентами из $Z/2Z$. Сформировать с помощью этого полинома поле Галуа из 32-х элементов. Выписать проверочную матрицу H примитивного двоичного БЧХ-кода (варианты 1 – 6) или реверсивного (варианты 7 – 10) длиной 31, исправляющего двойные ошибки.

Задание 8. Аппарат сотовой связи с кодом из задания 7 принял сообщение $\bar{x}$. За 40 наносекунд он определяет и исправляет ошибки в сообщении. Не ограничивая себя 40 наносекундами, убедиться, что сообщение $\bar{x}$ содержит ошибки.

Варианты данных к заданиям контрольной работы

Задание 1.

В.1: $a = 1825;\ \ b = 1971.$	В. 2: $a = 1917;\ \ b = 2272.$
В. 3: $a = 2412;\ \ b = 1675.$	В. 4: $a = 1885;\ \ b = 1690.$
В. 5: $a = 1647;\ \ b = 1952.$	В. 6: $a = 1888;\ \ b = 2065.$
В. 7: $a = 1696;\ \ b = 1537.$	В. 8: $a = 2303;\ \ b = 1692.$
В. 9: $a = 1568;\ \ b = 1715.$	В. 10: $a = 1296;\ \ b = 1476.$

Задание 4а: расшифровать криптограмму Цезаря.

В.1. ХУЦЖРС ЛКДЗЙГХЯ ДЦЖЦЬЗЁС. С. ЦГМОЯЖ.
В.2. ЕСХ ЦЙ СФЗРЯ ЦОЗХЗОГ, Л ТУЛПЪГОГФВ КЛПГ.
В.3. ЦЪЛХЗФЯ ЕОГФХЕСЕГХЯ ФСДСМ.Г.Ф.ТЦЫНЛР.
В.4. РЗОЯКВ СДЭВХЯ РЗСДЭВХРСЗ (Н. ТУЦХНСЕ).
В.5. СДОГНСП ЕСОРЛФХЮП ТЮОЯ ЕФХГИХ ЕЖГОЛ.
В.6. ХЛШС ЕЗХШГВ НГОЛХНГ КГ ТОЗХРЗП ФНУЛТЛХ.
В.7. ФСОСЕЯЛ ЖГЕРС КГТЗОЛ, ФЦПУГН ЕСКЕЗФХВ.
В.8. РГ ЖЕСМРСП ФХЗНОЗ ЦКСУЮ РГЪЗУХЛО ПСУСК.
В.9. НСРЗЩ ГООЗЛ СТВХЯ Ф ЦХУГ ЛФЪЗК Е ТЮОЛ.
В.10. ЪЦХЯ ЕЗЪЗУРЗБ УСФСБ СФЮТГЗХФВ ХУГЕГ.

Задание 4б: перевести с тарабарского.

В.1. ГУКЬ ШЕГЕМПЕЮ МОЛОЮ ОЛЫНАЕКЛЯ КМАША.
В.2. ТОПЕД АССЕИ ОНЯКЬ Л УКМА ИЛГЕФ Ш НЫСИ.
В.3. ПА ЦШОЙПОР ЛКЕТСЕ УФОМЫ ПАГЕМКИС РОМОФ.
В.4. ЛОСОЩЬИ ЦАШПО ФАНЕСИ, ЛУРМАТ ШОФШЕЛКЯ.
В.5. КИЖО ШЕЖЖАЯ ТАСИКТА ФА НСЕКПЕР ЛТМИНИК.
В.6. ОЩСАТОР ШОСПИЛКЫР НЫСЬ ШЛКАЁК ШЦАСИ.
В.7. ПЕСЬФЯ ОЩЪЯКЬ ПЕОЩЪЯКПОЕ (Т. НМУКТОШ).
В.8. УГИКЕЛЬ ШСАЛКШОШАКЬ ЛОЩОЙ. А.Л. НУВТИП.
В.9. ШОК УХ ОЛЕПЬ УСЕКЕСА, И НМИРГАСАЛЯ ФИРА.
В.10. КМУЦПО ИФЩЕХАКЬ ЩУЦУБЕЧО. О. УАЙСЬЦ.

Задание 4в: расшифруйте текст, зашифрованный с помощью девиза «Роза».

В.1. ьюцёзпфмцшчррветевщбъбаёщсшьэш
В.2. япмгащцпюбыёьынфщющьяпаёввсмюющпщ
В.3. гэнвсяиесысрезсоьшцбщпхжвчбйцячмр
В.4. дшюпуфыцсоубэшылсчирэфыоцьълвшшйд
В.5. игыэуфаёвэнявюъппюъьбпнугоыссси
В.6. япшпэососыьдсучгцбцьэфлмъбцёфп
В.7. бюьувгкшцаиеацмэубыёьыипьюцтдгабэ

В.8. япчтцэцяптщащлцбипфрсуиунбцёшюу
В.9. тффьыбцёфяьщъбыьыскпщуьццъщфшшытр
В.10. арфбьюхгаыцйгвднбкфэубыбчвкесыс

Задание 4г: прочитайте текст, зашифрованный методом постолбцовой транспозиции ($n = 5$, $m = 6$).

В.1. втись оирез рдалз иазио семтм ечеыл
В.2. ветду бйрве юеыор анвит онмчв еарес
В.3. кпяез вчтоо ниьсп ыисее цлуал иртла
В.4. жйвпо пыеои ллтлу гекен асеса йевев
В.5. нгали сгдуа плоен елвао лнеыг ансия
В.6. пвсос тптьо удену чокжт ролка лоаду
В.7. чюртс теоеу тнсар апорь веюыв асоче
В.8. навпо пыена хятлу гексо хлеса йевил
В.9. оисёт ватнб ллытд асмоа квпвл илымо
В.10. нзььс нтняа ораае ждчгс еюаао кплюн

Задание 5.

В.1. $\{ш,е,п\}=\{828,13,1147\}$
В.2. $\{ш,е,п\}=\{1330,9,1681\}$
В.3. $\{ш,е,п\}=\{1205,11,1517\}$
В.4. $\{ш,е,п\}=\{163,13,961\}$
В.5. $\{ш,е,п\}=\{1423,13,1681\}$
В.6. $\{ш,е,п\}=\{1557,11,1681\}$
В.7. $\{ш,е,п\}=\{131,13,1517\}$
В.8. $\{ш,е,п\}=\{389,11,1147\}$
В.9. $\{ш,е,п\}=\{1074,17,1517\}$
В.10. $\{ш,е,п\}=\{1378,11,1763\}$

Задание 6.

В.1. $\{m,O,P,g,h,x\}=\{35,35,47,13,3,6\}$
В.2. $\{m,O,P,g,h,x\}=\{10,8,43,12,37,7\}$
В.3. $\{m,O,P,g,h,x\}=\{15,14,37,13,6,9\}$
В.4. $\{m,O,P,g,h,x\}=\{14,24,41,13,7,9\}$
В.5. $\{m,O,P,g,h,x\}=\{17,24,47,11,42,10\}$
В.6. $\{m,O,P,g,h,x\}=\{7,35,53,8,51,9\}$
В.7. $\{m,O,P,g,h,x\}=\{11,33,61,6,44,11\}$
В.8. $\{m,O,P,g,h,x\}=\{6,22,61,7,34,12\}$
В.9. $\{m,O,P,g,h,x\}=\{23,13,53,12,9,10\}$
В.10. $\{m,O,P,g,h,x\}=\{44,57,61,10,14,10\}$

Задание 7.

В.1: $p(x)=x^5+x^2+1.$
В.2: $p(x)=x^5+x^3+1.$
В.3: $p(x)=x^5+x^3+x^2+x+1.$
В.4: $p(x)=x^5+x^4+x^2+x+1.$
В.5: $p(x)=x^5+x^4+x^3+x+1.$
В.6: $p(x)=x^5+x^4+x^3+x^2+1.$

В.7: $p(x) = x^5 + x^2 + 1.$ В.8: $p(x) = x^5 + x^3 + 1.$

В.9: $p(x) = x^5 + x^3 + x^2 + x + 1.$ В.10: $p(x) = x^5 + x^4 + x^2 + x + 1.$

Задание 8.

В.1: $\overline{x}$ = (001 011 011 100 000 100 000 000 100 000 1).

В.2: $\overline{x}$ = (110 110 100 100 100 000 000 000 000 100 1).

В.3: $\overline{x}$ = (101 101 101 100 000 000 100 000 100 100 0).

В.4: $\overline{x}$ = (111 011 011 100 000 001 000 100 000 000 1).

В.5: $\overline{x}$ = (110 110 111 100 000 000 001 100 000 000 1).

В.6: $\overline{x}$ = (110 110 110 100 010 000 000 001 000 100 0).

В.7: $\overline{x}$ = (011 010 110 100 000100 001 000 000 00 1).

В.8: $\overline{x}$ = (011 010 110 100 000 000 010 000 000 010 1).

В.9: $\overline{x}$ = (101 111 101 100 010 001 000 000 000 000 1).

В.10: $\overline{x}$ = (001 110 001 000 000 010 000 000 100 001 0).

Часть II. Теория норм синдромов

Глава 1. Линейные помехоустойчивые коды

Главным теоретическим импульсом в создании помехоустойчивых кодов явилась следующая

Теорема 2.1.1. (К. Шеннон, 1948 г.). *Введением избыточности в передаваемую в зашумленном канале связи информацию можно добиться исправления возникающих в процессе передачи этой информации сколь угодно сложных ошибок.*

Для систем цифровой связи естественным является допущение, что информация записывается в виде блоков – конечных последовательностей фиксированной длины k символов из данного поля P. Другими словами, всякое информационное слово представляет собой k-разрядный вектор – произвольный вектор из линейного пространства $P_k = \{(x_1, x_2, ..., x_k) | x_i \in P\}$. Кодирование и есть внедрение избыточности в блоки передаваемой информации. Реализуется оно введением специальных покоординатных проверок. С математической точки зрения – это линейное отображение линейного пространства P_k в пространство большей размерности P_n, $n > k$. Результатом кодирования является код – многообразие закодированных слов.

Определение 2.1.1. Линейным (n, k)-кодом C над полем P называется произвольное k-мерное подпространство линейного пространства P_n. Параметр n называется длиной кода, а k-размерностью кода. Линейный (n, k)-код называется высокоскоростным, если отношение k/n близко к 1, и низкоскоростным, если отношение $k/n << 1$ – близко к нулю.

Все линейные операторы имеют матричную реализацию. Поэтому кодирование есть, по сути, умножение информационных слов-векторов на некоторую матрицу G порядка $k \times n$ с коэффициентами из поля P.

Определение 2.1.2. Пусть C – линейный (n, k)-код над полем P. Пусть $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_k$ – базис кода C. Порождающей матрицей кода C называется (k, n) – матрица G, строки которой состоят из координат векторов $\bar{g}_1, \bar{g}_2, \ldots, \bar{g}_k$ в некотором заданном базисе пространства P_n.

Название порождающей матрицы объясняется тем, что любое кодовое слово кода C является линейной комбинацией строк матрицы G, порождаясь ее строками. Из определения непосредственно следует, что ранг матрицы G равен k.

Пример 2.1.1. С середины XX в. долгое время в американских системах цифровой связи передача данных осуществлялась в так называемом ASCII-формате. Этот формат требовал передавать данные блоками по 8 двоичных бит, 7 из них были информационными, а 8-й был проверочным, в нем записывался 0 или 1 так, чтобы во всем байте, т. е. во всем блоке сохранялось

четное число единиц. Таким образом, восьмой бит осуществлял проверку на четность во всем байте – все восемь координат x_i, $1 \le i \le 8$, байта в совокупности удовлетворяли линейному однородному уравнению

$$x_1 + x_2 + ... + x_8 = 0.$$

Множество решений данного однородного уравнения представляют весь спектр векторов-слов ASCII-формата. Эти решения – двоичные векторы 8-мерного пространства P_8 над полем Галуа $P = GF(2)$ из двух элементов – образуют в P_8 7-мерное подпространство $L - (8, 7) -$ линейный код над полем из двух элементов. Легко видеть, что фундаментальную систему решений – базис пространства L решений данного уравнения – образуют следующие 7 векторов

$$\bar{e}_1 = (1000\ 0001), \quad \bar{e}_2 = (0100\ 0001), ..., \quad \bar{e}_7 = (0000\ 0011).$$

Пусть $G - (7 \times 8) -$ матрица, строки которой состоят из координат векторов $\bar{e}_1, \bar{e}_2, ..., \bar{e}_7$. Умножением произвольных 7-мерных информационных двоичных векторов на матрицу G мы преобразуем их в ASCII-формат.

Пример 2.1.2. Очевидно, пример 2.1.1 имеет прозрачное обобщение для двоичных кодов любой длины. Каждое кодовое слово получается добавлением к информационным блокам длиной k единственного $k+1$-го проверочного разряда, в нем записывается 0 или 1 так, чтобы во всем блоке сохранялось четное число единиц. Здесь, $n = k + 1$. Такие коды $C_{\div}$ называют кодами с проверкой на четность.

Теорема 2.1.2. *Из каждого кодового слова $\bar{c} \in C$ закодированная в нем информация $\bar{i} \in P_k$ однозначно восстанавливается с помощью порождающей код матрицы G.*

Доказательство. Пусть $\bar{x} = (x_1, x_2, ..., x_k) -$ такой вектор пространства P_k, что $\bar{x} \cdot G = \bar{c}$ для данного $\bar{c} \in C$. Равенство $\bar{x} \cdot G = \bar{c}$ есть система n линейных уравнений с k неизвестными $x_1, x_2, ..., x_k$. По определению $rankG = k$. Это означает существование в $(k \times n)$-матрице G невырожденной квадратной подматрицы M порядка k. В таком случае система уравнений $\bar{x} \cdot G = \bar{c}$ эквивалентна своей подсистеме $\bar{x} \cdot M = \bar{c}'$, имеющей, по правилу Крамера, единственное решение. Теорема доказана.

Определение 2.1.3. Матрица H порядка $m \times n, m = n - k$ называется проверочной матрицей кода C, если $KerH = C$.

Из этого определения следует, что код C состоит из решений однородной системы линейных уравнений $H \cdot \bar{x}^T = \bar{0}^T$, т. е. H – матрица коэффициентов системы из m проверочных линейных соотношений, определяющих код C.

Пример 2.1.3. Код $C_{\div}$ с проверкой на четность из примера 2.1.2 состоит из векторов-решений единственного уравнения $x_1 + x_2 + ... + x_n = 0$ над полем $P = GF(2)$. Следовательно, проверочная матрица кода $C_{\div}$ есть $(1 \times n)$-матрица и имеет вид $H = (1\,1\,...\,1)$.

Пример 2.1.4. Пусть $P = GF(2)$ – поле Галуа из двух элементов; $k = 4$, т. е. передаваемая информация состоит из 4-мерных векторов $\bar{x} = (x_1, x_2, x_3, x_4)$ с координатами x_i, $1 \le i \le 4$, со значениями $0,1 \in GF(2)$. Каждый вектор $\bar{x}$ кодируем, присоединив к нему координаты x_5, x_6, x_7, вычисленные по правилам: $x_5 = x_1 + x_2 + x_4$, $x_6 = x_1 + x_3 + x_4$, $x_7 = x_2 + x_3 + x_4$. Тем самым получим линейный код L, состоящий из векторов $\bar{z} = (x_1, x_2, \ldots, x_7) \in P_7$, удовлетворяющих проверочным соотношениям

$$\begin{cases} x_1 + x_2 \quad + x_4 + x_5 \quad = 0, \\ x_1 \quad + x_3 + x_4 \quad + x_6 \quad = 0, \\ \quad x_2 + x_3 + x_4 \quad + x_7 = 0. \end{cases} \qquad (2.1)$$

Это известный совершенный систематический линейный $(7,4)$- код, принадлежащий семейству кодов Хэмминга.

Согласно определению 2.1.3 матрица коэффициентов приведенной выше системы линейных уравнений (2.1)

$$H = \begin{pmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

есть проверочная матрица данного кода. Так как базисный минор матрицы H расположен в последних трех столбцах, то x_1, x_2, x_3, x_4 – свободные переменные системы линейных уравнений (2.1). Отсюда легко получаем порождающую матрицу кода Хэмминга:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

Координаты базиса ядра матрицы G составляют проверочную $(n-k) \times n$-матрицу H кода L: только для векторов $\bar{c} \in L$ $H \cdot \bar{c}^T = \bar{0}$ и только для них. Каждая из матриц G или H однозначно определяет код L.

Определение 2.1.4. Коды, отличающиеся перестановкой отсчетов, т. е. координат, называются эквивалентными.

Пример 2.1.5. Для кода Хэмминга используют различные задания. Одним из наиболее известных является лексикографическое – когда i-й столбец проверочной матрицы есть двоичная запись числа i. Значит, лексикографически заданный $(7,4)$-код Хэмминга имеет проверочную матрицу

$$H_{\text{лекс}} = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}.$$

Общепринятым является интерпретация столбцов проверочной матрицы как элементов поля $GF\left(2^m\right)$, являющихся векторами из P_n в базисе $1, \alpha, \alpha^2, ..., \alpha^n$ для примитивного элемента α поля $GF\left(2^m\right)$. Если в качестве α взять корень неприводимого полинома $x^3 + x + 1$, то матрица

$$\widetilde{H} = \left[1, \alpha, \alpha^2, ..., \alpha^{2^m - 2}\right] = \begin{bmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

есть матрица линейного $(7,4)$-кода.

Определение 2.1.5. Метрикой, или расстоянием на множестве X называется определенная на декартовом квадрате $X \times X$ функция ρ с неотрицательными действительными значениями, удовлетворяющая при любых $x, y \in X$ условиям:

1) $\rho(x, y) = 0$ тогда и только тогда, когда $x = y$ (аксиома тождества);

2) $\rho(x, y) + \rho(y, z) \geq \rho(x, z)$; (аксиома треугольника);

3) $\rho(x, y) = \rho(y, x)$ (аксиома симметрии).

В дальнейшем будем предполагать, что $P = GF(q)$ – конечное поле из q элементов, P_n – векторное n-мерное пространство над полем P, содержащее линейный (n, k)-код C.

Определение 2.1.6. Расстоянием Хэмминга между векторами $\bar{x}, \bar{y} \in P_n$ называется количество $dist(\bar{x}, \bar{y})$ несовпадающих координат этих векторов. Весом $wt(\bar{x})$ вектора $\bar{x} \in P_n$ называется количество ненулевых координат этого вектора.

Несложно видеть, что расстояние Хэмминга между векторами $\bar{x}, \bar{y} \in P_n$ равно весу вектора $\bar{x} - \bar{y}$. Очевидно, $wt(\bar{x} + \bar{y}) \leq wt(\bar{x}) + wt(\bar{y})$.

Лемма 2.1.1. Расстояние Хэмминга обладает всеми свойствами расстояния из определения 2.1.5:

1) $dist(\bar{y}, \bar{x}) = dist(\bar{x}, \bar{y})$ – свойство симметричности;

2) $dist(\bar{x}, \bar{y}) = 0$ тогда и только тогда, когда $\bar{x} = \bar{y}$;

3) $dist(\bar{x}, \bar{z}) + dist(\bar{z}, \bar{y}) \geq dist(\bar{x}, \bar{y})$ – неравенство треугольника.

Определение 2.1.7. t-окрестностью вектора $\bar{x} \in P_n$ назовем совокупность всех векторов $\bar{y} \in P_n$, для которых $dist(\bar{x}, \bar{y}) \leq t$.

t – окрестности обладают обычным свойством отделимости.

Лемма 2.1.2. Если $dist(\bar{x}, \bar{z}) > 2t$, то t-окрестности векторов $\bar{x}, \bar{z} \in P_n$ не пересекаются.

Определение 2.1.8. Минимальным, или кодовым расстоянием кода C называется наименьшее из расстояний между попарно различными векторами кода C.

Из равенства $dist(\bar{x}, \bar{y}) = wt(\bar{x} - \bar{y})$ следует, что минимальное расстояние линейного кода равно наименьшему из весов ненулевых векторов этого кода.

Значение кодового расстояния определяет следующая, фундаментальная в помехоустойчивом кодировании

Теорема 2.1.3. *Если минимальное расстояние кода* C *равно* $d = 2t+1$ *или* $d = 2t+2$, *то код* C *может обнаружить до* $d-1$ *ошибок и исправить до* t *ошибок в каждом принятом векторе-слове длиной* n.

По определению 2.1.1 далеко не каждое k-мерное подпространство линейного пространства P_n относят к реальным линейным кодам. На практике применяются коды с попарно удаленными друг от друга кодовыми словами согласно метрике Хемминга – с достаточно большим кодовым расстоянием d. Следующая теорема служит критерием для определения минимального расстояния кода.

Теорема 2.1.4. *Пусть* H *– проверочная матрица двоичного кода* C. *Минимальное расстояние этого кода равно* d *тогда и только тогда, когда любые* $d-1$ *столбцов матрицы* H *линейно независимы, но найдутся* d *линейно зависимых столбцов.*

Определение 2.1.9. Кодом Хемминга называется линейный код C_χ с проверочной матрицей $H_\chi = \left(1, \alpha, ..., \alpha^{2m-2}\right)$. Здесь α^i – двоичный вектор-столбец над полем $GF(2)$ в базисе $1, \alpha, ..., \alpha^{m-1}$ для примитивного элемента α поля $GF\left(2^m\right)$.

Из определения следует, что столбцами матрицы H_χ являются все возможные ненулевые векторы двоичного пространства P_n. Поэтому произвольный код Хэмминга имеет параметры $n = 2^m - 1$, $k = n - m$: $(7, 4); (15, 11); (31, 26); (63, 57); (127, 120); (255, 247); (511, 502); (1023, 1013)$ и т. д.

Теорема 2.1.5. *Минимальное расстояние у кода Хэмминга* $d = 3$. *Код Хэмминга исправляет одиночные ошибки.*

Одним из важнейших понятий теории помехоустойчивых кодов является синдром ошибок. В процессе передачи информации на кодовое слово $\overline{c}$ может наложиться «шум» – вектор ошибок $\overline{e}$. В результате приемное устройство получает искаженное сообщение $\overline{y} = \overline{c} + \overline{e}$.

Определение 2.1.10. Синдромом ошибок принятого слова $\overline{y}$ в коде C с проверочной матрицей H называется вектор $S = H \cdot \overline{y}^T$.

Если $S = \overline{0}$, то $\overline{y}$ – кодовое слово. Следовательно, условие $S \neq \overline{0}$ служит признаком наличия ошибочных символов в принятом слове $\overline{y}$. В силу ассоциативности операций сложения и умножения матриц синдром

$$S = H \cdot \overline{y}^T = H \cdot \left(\overline{c}^T + \overline{e}^T\right) = H \cdot \overline{c}^T + H \cdot \overline{e}^T = H \cdot \overline{e}^T .$$

Это означает, что S зависит только от вектора ошибок $\overline{e}$ и не зависит от кодовых слов.

Предложение 2.1.1. Пусть C – линейный код, исправляющий ошибки ве-

сом ϖ, $1 \le \varpi \le t$ для некоторого $t \ge 1$. Обозначим через $K_{od...t}$ множество всех ошибок весом 1, 2, …, *t*, исправляемых кодом C. Если $\bar{x} \ne \bar{e}$ для $\bar{e} \in K_{od...t}$, но $S(\bar{e}) = S(\bar{x})$, то $w(\bar{x}) \ge d$. Следовательно, для произвольных $\bar{e}_1, \bar{e}_2 \in K_{od...t}$, $\bar{e}_1 \ne \bar{e}_2$, их синдромы попарно различны $S(\bar{e}_1) \ne S(\bar{e}_2)$.

Доказательство. Пусть $\bar{e} \in K_{od...t}$, а $\bar{x}$ – произвольный вектор ошибок, но $S(\bar{e}) = S(\bar{x})$. Тогда $S(\bar{x} - \bar{e}) = \bar{0}$. Это означает, что вектор $\bar{y} = \bar{x} - \bar{e} \in C$. Согласно пятому свойству расстояния Хэмминга

$$w(\bar{x}) = w(\bar{y} + \bar{e}) \ge w(\bar{y}) - w(\bar{e}) \ge w(\bar{y}) \ge d .$$

Предложение 2.1.1 вместе с очевидной уверенностью, что наиболее вероятны ошибки малого веса, создают теоретическую базу для синдромных методов коррекции ошибок, по значениям синдромов ошибок определяющих соответствующие векторы ошибок из множества $K_{od...t}$.

Существуют различные методы коррекции ошибок. Основные преимущества синдромных методов в следующем:

1) согласно предложению 2.1.1 синдромы однозначно соответствуют ошибкам декодируемого многообразия;

2) синдромы имеют существенно меньшие размеры по сравнению с кодовыми словами и векторами ошибок (что особенно наглядно для высокоскоростных кодов, например, для кодов Хемминга);

3) для нахождения синдромов не требуется специальных вычислений, кроме обусловленных необходимостью индикации наличия или отсутствия ошибок в принятом блоке-сообщении;

4) синдром совершенно не связан с передаваемой информацией, а только исключительно с произошедшей ошибкой.

Синдромное декодирование кодов Хэмминга. Пусть $H = \left(1, \alpha, ..., \alpha^{2m-2}\right)$ – проверочная матрица кода Хэмминга. Как установлено выше, код Хэмминга имеет минимальное расстояние 3 и может декодировать только одиночные ошибки. Пусть $\bar{e}_i$ – двоичный вектор-ошибка весом 1 с единственной ненулевой i-й координатой. Ясно, что $S(\bar{e}_i) = H \cdot \bar{e}_i^T = \alpha^{i-1}$ – i-й столбец матрицы H, однозначно указывающий на ошибочную координату – единственную ненулевую координату вектора $\bar{e}_i$.

Определение 2.1.11. Код называется совершенным, если множество его ненулевых синдромов совпадает по мощности с множеством декодируемых ошибок.

Название объясняется тем, что у совершенных кодов синдромная информация об ошибках на 100 % используется для их коррекции. Большинство кодов, конечно же, совершенными не являются. Но примеры таких кодов есть. Очевидно, код Хэмминга относится к разряду совершенных кодов.

Глава 2. Основы теории БЧХ-кодов

§2.1. Определение и основные свойства БЧХ-кодов

Для всякого натурального n, делящего q^m-1, в поле Галуа $GF(q^m)$ найдется элемент β порядка n (например, $\beta=\alpha^c$ для примитивного элемента $\alpha\in GF(q^m)$ и $c=(q^m-1)/n$). Зафиксируем целые числа $b>0$, не делящееся на n; $\delta>1$; натуральное n, делящее или равное q^m-1, но не делящее q^s-1 для всех целых s, $0<s<m$. При этом значение δ должно быть таким, что выполняется неравенство $m(\delta-1)<n$.

Определение 2.2.1. Линейный код C длиной n с проверочной матрицей

$$H=\left[\begin{array}{cccc} 1 & \beta^{b} & \beta^{2b} & \beta^{(n-1)b} \\ 1 & \beta^{b+1} & \beta^{2(b+1)} & \beta^{(n-1)(b+1)} \\ \hline 1 & \beta^{b+\delta-2} & \beta^{2(b+\delta-2)} & \beta^{(n-1)(b+\delta-2)} \end{array}\right]=[\beta^{bi},\beta^{(b+1)i},\ldots,\beta^{(b+\delta-2)i}]^T \qquad (2.2)$$

над полем $GF(q)$ называется кодом Боуза – Чоудхури – Хоквингема (БЧХ-кодом) с конструктивным расстоянием δ. При $n=q^m-1$ БЧХ-код называют примитивным, и не примитивным, если $n<q^m-1$.

В определении не говорится, но подразумевается (как это было и в определении кода Хемминга), что в матрице H каждый элемент $\beta^i=\alpha^{ci}$ заменен на соответствующий вектор-столбец $(b_{m-1},b_{m-2},\ldots,b_0)^T$ поэтому код действительно определен над полем $GF(q)$, а матрица H имеет конструктивные размеры $m(\delta-1)\times n$. Неравенство $m(\delta-1)<n$ гарантирует, что ядро этой матрицы не тривиально и, следовательно, код C существует, являясь линейным пространством размерности, не меньшей, чем $n-m(\delta-1)$.

Теорема 2.2.1. Для всякого целого числа n, не делящегося на q, над полем $GF(q)$ существует БЧХ-код длиной n. Для всякого нечетного $n\geq 3$ существует двоичный БЧХ-код длиной n.

Здесь изучим некоторые свойства элементов $\beta\in GF(q^m)$, играющих неотъемлемую роль в определении БЧХ-кодов – в формировании проверочных матриц этих кодов. Они возникают несколько затененно, как степени примитивных элементов. В принципе, это естественно, т. к. мультипликативная группа $GF(q^m)^*$ циклична. Но такой подход не позволяет сказать что-либо об аддитивных свойствах β.

Теорема 2.2.2. Для всякого натурального n, являющегося делителем q^m-1, но не делящего q^s-1 для всех целых s, $0<s<m$, элемент $\beta\in GF(q^m)^*$ порядка n существует. Он является корнем неприводимого и не

примитивного полинома показателя n и степени m над полем $GF(q)$.

Размерность линейного кода L длиной n как векторного пространства над полем P при задании этого кода с помощью проверочной матрицы H определяется формулой $k = \dim L = \dim KerH = n - rankH$.

Ранг проверочной матрицы H БЧХ-кода C чаще всего совпадает с числом ее строк $m(\delta - 1)$. Но иногда возникают ситуации, когда этот ранг меньше $m(\delta - 1)$. Наиболее типичную из таких ситуаций описывает

Теорема 2.2.3. *Пусть для некоторого целого t, не делящегося на $q^m - 1$, проверочная матрица H БЧХ-кода C содержит, с точностью до перестановки строк, подматрицу $[\beta^{it}, \beta^{itq}]$. Тогда $rank[\beta^{it}, \beta^{itq}] = rank[\beta^{it}]$.*

Замечание. Теорема остается справедливой, если в подматрице $[\beta^{it}, \beta^{itq}]$ степень itq заменить на $f(s) = itq^s$ для целых s, $1 \le s \le m - 1$.

Выяснением равенства $H \cdot \bar{x}^T = \bar{0}$ устанавливается принадлежность $\bar{x}$ данному коду. Все декодеры телекоммуникационных цифровых систем реализуют проверку этого соотношения. Вычисления происходят быстро, синхронно с поступлением информации. Поэтому эти вычисления должны требовать минимум временных затрат. В силу сказанного матрица H должна быть минимально сложной, в частности, не содержать линейно зависимых строк – такие из матрицы H следует удалять. Из указанного обстоятельства и возникло условие: ранг проверочной матрицы кода равен числу ее строк.

Указанная теоремой 2.2.3 ситуация чаще всего возникает при $b = 1$ (тогда код называют БЧХ-кодом в узком смысле). Наиболее типична она для двоичных кодов, когда $q = 2$. Поэтому после удаления линейно зависимых строк проверочная матрица БЧХ-кода в узком смысле в данном случае и для $\delta = 2t$ и для $\delta = 2t + 1$ имеет один и тот же вид:

$$H = (\beta^i, \beta^{3i}, ..., \beta^{(2t-1)i})^{\mathrm{T}},\ 0 \le i \le n - 1. \qquad (2.3)$$

Истинная размерность данного БЧХ-кода C_{2t+1} есть величина $k \le n - tm$, что существенно больше конструктивной размерности $n - m(\delta - 1)$. Именно такие коды получили наибольшее применение, особенно, когда $n = q^m - 1$, т. е. при $\beta = \alpha$.

§2.2. Синдромное декодирование примитивных БЧХ-кодов с минимальным расстоянием 5

Здесь рассматривается классический примитивный БЧХ-код C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le n - 1$, α – примитивный элемент поля Галуа $GF(2^m)$, $n = 2^m - 1$. Его кодовое расстояние равно 5, $k - n - 2m$. Следовательно, этот код корректирует одиночные и двойные ошибки.

Пусть при передаче вектора-сообщения $\bar{c}$ в цифровой системе связи с

данным кодом C на сообщение наложился вектор-ошибка $\bar{e} = (i, j)$ весом 2 с ненулевыми координатами на неизвестных позициях i и j. Это означает, что приемное устройство связи приняло сообщение $\bar{x} = \bar{c} + \bar{e}$. В соответствии со свойствами и структурой матрицы H синдром $S(\bar{x}) = S(\bar{e}) = (s_1, s_2)$, где $s_1 = \alpha^{i-1} + \alpha^{j-1}$; $s_2 = \alpha^{3(i-1)} + \alpha^{3(j-1)}$. Величины α^{i-1} и α^{j-1} пока неизвестные элементы поля Галуа $GF(2^m)$. Обозначим их через x и y соответственно. Эти величины – решения системы уравнений

$$\begin{cases} x + y = s_1, \\ x^3 + y^3 = s_2. \end{cases} \qquad (*)$$

Преобразуем второе уравнение этой системы.

$$x^3 + y^3 = (x + y)(x^2 + xy + y^2) = s_1(s_1^2 + xy) = s_2.$$

Следовательно, $xy = s_2 s_1^{-1} + s_1^2$. Правую часть полученного равенства обозначим через a. Таким образом, система преобразована к виду $\begin{cases} x + y = s_1, \\ xy = a. \end{cases}$ Согласно теореме Виета корни x, y системы являются корнями квадратного уравнения $t^2 + s_1 t + a = 0$. Решив уравнение, найдем $x = \alpha^{i-1}$, $y = \alpha^{j-1}$, а с ними и вектор-ошибку $\bar{e} = (i, j)$.

Пример 2.2.1. В системе связи, построенной на основе БЧХ-кода C с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le 14$, α – примитивный элемент поля Галуа $F(16)$, корень полинома $x^4 + x + 1$, принято сообщение $\bar{x} = (111011110110101)$. Выяснить наличие ошибок в этом сообщении и попытаться их исправить.

Решение. Для проведения вычислений необходимо иметь под рукой сформированное поле Галуа из 16 элементов, а именно: таблицу степеней α – корня полинома $x^4 + x + 1$ и их полиномиальных эквивалентов. Все кодовые слова $\bar{c} \in C$ (и только они) составляют ядро проверочной матрицы: $H \cdot (\bar{c}^T) = \bar{0}$. Если $\bar{S} = H(\bar{x}^T) \neq \bar{0}$, то сообщение $\bar{x}$ явно содержит ошибки. В данном случае $\bar{S} = (s_1, s_2)^T$, где

$$s_1 = 1 + \alpha + \alpha^2 + \alpha^4 + \alpha^5 + \alpha^6 + \alpha^7 + \alpha^9 + \alpha^{10} + \alpha^{12} + \alpha^{14} = \alpha^{11};$$

$$s_2 = 1 + \alpha^3 + \alpha^6 + \alpha^{12} + \alpha^{15} + \alpha^{18} + \alpha^{21} + \alpha^{27} + \alpha^{30} + \alpha^{36} + \alpha^{42} = \alpha.$$

Таким образом, полученное сообщение $\bar{x}$ содержит ошибки. Данный код исправляет двойные ошибки. Для нахождения такой ошибки имеем следующую конкретную систему $(*)$: $\begin{cases} x + y = \alpha^{11}, \\ x^3 + y^3 = \alpha. \end{cases}$

Данная система сводится к квадратному уравнению. Действительно,

$$x^3 + y^3 = (x + y)(x^2 + xy + y^2) = \alpha^{11}(\alpha^{22} + xy) = \alpha.$$

Отсюда получаем $xy = \alpha^{22} + \alpha / \alpha^{11} = \alpha^7 + \alpha^5 = \alpha^{13}$. Замена $y = x + \alpha^{11}$ приводит это уравнение к следующему квадратному уравнению: $x^2 + \alpha^{11}x + \alpha^{13} = 0$. Непосредственным подбором (методом Чэня) можно убедиться, что его корнями являются $x_1 = 1; x_2 = \alpha^{12}$. Таким образом, ошибочными в принятом сообщении являются 1-я и 13-я позиции и правильным является сообщение $\overline{c}_0 = (011011110110001)$.

§2.3. Реверсивные коды

Реверсивные коды относятся к разряду модифицированных БЧХ-кодов.

Определение 2.2.2. Реверсивным называется код C_R^m, который задается проверочной матрицей $H = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$, где α – примитивный элемент поля $GF(2^m)$, $m \geq 3$; $0 \leq i \leq n-1$ для $n = 2^m - 1$.

Как и в определении БЧХ-кода, каждый элемент матрицы H есть двоичный m-разрядный вектор. Таким образом, H – это двоичная $(2m \times n)$-матрица, ранг которой, очевидно, равен $2m$.

В проверочной матрице $H = (H_1, H_2)^T = (\alpha^i, \alpha^{-i})^T$ реверсивного кода C_R^m подматрица H_1 совпадает с такой же подматрицей проверочной матрицы БЧХ-кода из §2.2, а вторая подматрица H_2 представляет собой запись элементов первой строки, но в обратном порядке. Поэтому такой код и называют реверсивным.

Теорема 2.2.4. *При четных значениях* $m = 2\mu$ *реверсивный код* C_R^m *имеет минимальное расстояние* 3*, а при нечетных* – 5.

Из теоремы следует, что перспективным для приложений является реверсивный код C_R^{2r+1}, который может исправлять двойные ошибки, в общей сложности $C_n^1 + C_n^2 = \dfrac{n(n+1)}{2}$ различных ошибок. Его и будем далее рассматривать.

В соответствии со структурой матрицы H двоичные координаты вектора-синдрома $\overline{S}$ произвольной ошибки в реверсивном коде сгруппируем последовательно в две группы по m координат в каждой. Тогда вектор $\overline{S}$ можно записать в виде $\overline{S} = (s_1, s_2)^T$, где s_1 и s_2 – элементы поля $GF(2^m)$. Следовательно, $s_1 = \alpha^i, s_2 = \alpha^j$ для подходящих i, j из множества $T = \{-\infty, 0, 1, 2, ..., n-1\}$. Код $C_R^{2\mu+1}$ имеет конструктивное расстояние 5 и, следовательно, исправляет двойные ошибки. Для определения координат двойной ошибки здесь аналог системы $(*)$ имеет следующий вид:

$$\begin{cases} x + y = s_1, \\ 1/x + 1/y = s_2. \end{cases} \qquad (**)$$

Левую часть второго уравнения приведем к общему знаменателю, т. е. к виду $(x+y)/xy = s_2$. Легко видеть, что здесь синдром любой двойной ошибки имеет ненулевые компоненты s_1, s_2. Поэтому с учетом первого уравнения имеем $xy = s_1/s_2 = b.$ Становится ясным, что компоненты решения системы (**) по теореме Виета совпадают с корнями квадратного уравнения

$$x^2 + s_1 x + b = 0. \qquad (***)$$

Пример 2.2.2. Пусть в реверсивном коде C_R^5, проверочная матрица которого построена с помощью примитивного элемента α – корня неприводимого полинома $x^5 + x^3 + x^2 + x + 1,$ получено сообщение

$$\bar{x} = (101\,101\,101\,100\,000\,000\,100\,000\,100\,1000).$$

Показать наличие в этом сообщении ошибок и устранить их.

Решение. Вычислим $\bar{S} = H \cdot \bar{x}^T$. Получим $\bar{S} = (\alpha^3, \alpha^6)^T \neq \bar{0}.$ Следовательно, сообщение $\bar{x}$ содержит ошибки. Для их определения имеем следующее уравнение (***) $x^2 + \alpha^3 x + \alpha^{28} = 0.$ Подбором, т. е. методом Чэня, находим корни этого уравнения $x_1 = \alpha^9;\ x_2 = \alpha^{19}$. Таким образом, принятое сообщение $\bar{x}$ содержит двойную ошибку на 10-й и 20-й позициях, а правильным является сообщение $\bar{c} = (101\,101\,101\,000\,000\,000\,110\,000\,100\,1000).$

§2.4. Синдромное декодирование произвольных примитивных БЧХ-кодов

Примитивный двоичный БЧХ-код C_{2t+1}, исправляющий $t \geq 1$ случайных ошибок, задается над полем Галуа $GF(2^m)$ проверочной матрицей

$$H = (\alpha^i, \alpha^{3i}, ..., \alpha^{(2t-1)i})^T, \qquad (2.4)$$

где α – фиксированный примитивный элемент поля $GF(2^m)$, параметр i принимает целые значения в пределах от 0 до $n-2$ для $n = 2^m - 1.$

Предполагается, что каждый элемент матрицы H есть двоичный столбец из m элементов 0 или 1 – координат соответствующей степени α^j как вектора пространства $GF(2^m)$ над полем $GF(2)$ в базисе $1, \alpha, ..., \alpha^{m-1}$. Поскольку ядром матрицы H является весь код C – ненулевое k-мерное подпространство в двоичном n-мерном пространстве, то ранг матрицы H, по построению равный tm, должен быть существенно меньше n. Таким образом, при задании кода автоматически должно выполняться строгое неравенство $tm < n.$ Конструктивное кодовое расстояние такого БЧХ-кода $\delta = 2t + 1,$ отсюда следует мотива-

ция обозначения данного кода через C_{2t+1}. Как уже отмечалось, реальное кодовое расстояние $d \geq \delta$.

Пусть $x_1, x_2, ..., x_t$ – локаторы ошибочных позиций принятого сообщения $\bar{x}$. Это элементы первой строки матрицы H как матрицы с элементами из поля $GF(2^m)$, соответствующие ошибочным позициям. Покоординатная запись векторного равенства $S = H \cdot \bar{x}^T$ приводит к следующей системе уравнений:

$$\begin{aligned} x_1 + x_2 + ... + x_t &= s_1, \\ x_1^3 + x_2^3 + ... + x_t^3 &= s_2, \\ ..... \\ x_1^{2t-1} + x_2^{2t-1} + ... + x_t^{2t-1} &= s_t. \end{aligned} \qquad (2.5)$$

Если систему (2.5) удастся решить относительно неизвестных $x_1, x_2, ..., x_t$, то координаты вектора ошибок $\bar{e}$ будут однозначно определены и будет найдено истинное сообщение $\bar{c} = \bar{x} + \bar{e}$. При $t = 2$ система (2.5) легко сводится к квадратному уравнению и решается. При $t \geq 3$ следует воспользоваться теорией симметрических полиномов. Дело в том, что левые части уравнений системы (2.5) можно рассматривать как симметрические многочлены от t неизвестных. Симметрические многочлены – это полиномы, не меняющиеся при любой перестановке местами переменных, т. е. инвариантные относительно группы подстановок – симметрической группы. В высшей алгебре построена специальная теория симметрических полиномов. Фундаментальный результат этой теории гласит, что любой симметрический полином можно выразить единственным образом в виде полинома от элементарных симметрических полиномов.

Определение 2.2.3. Следующие n симметрических многочленов от n неизвестных называются элементарными симметрическими многочленами:

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + ... + x_n, \\ \sigma_2 &= x_1x_2 + x_1x_3 + ... + x_{n-1}x_n, \\ &..... \\ \sigma_{n-1} &= x_1x_2 \cdot ... \cdot x_{n-1} + x_1x_2 \cdot ... \cdot x_{n-2}x_n + ... + x_2x_3 \cdot ... \cdot x_n, \\ \sigma_n &= x_1x_2 \cdot ... \cdot x_n. \end{aligned}$$

Для степенных сумм $f_k = x_1^k + x_2^k + ... + x_n^k$, $k = 1, 2, ...,$ еще Ньютоном установлены следующие рекуррентные формулы:

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^{k-1} f_1\sigma_{k-1} + (-1)^k k\sigma_k = 0, \quad k \leq n, \qquad (2.6)$$

$$f_k - f_{k-1}\sigma_1 + f_{k-2}\sigma_2 - ... + (-1)^n f_{k-n}\sigma_n = 0, \quad k > n. \qquad (2.7)$$

Эти формулы позволяют последовательно выражать степенные суммы через элементарные симметрические полиномы. Очевидно, $f_1 = \sigma_1$. Формула (2.6) при $k = 2 \leq n$ имеет вид $f_2 - f_1\sigma_1 + 2\sigma_2 = 0$. Следовательно, $f_2 = \sigma_1^2 - 2\sigma_2$. Формула (2.6) при $k = 3 \leq n$ имеет более сложный вид:

$f_3 - f_2\sigma_1 + f_1\sigma_2 - 3\sigma_3 = 0$. Подстановкой в это уравнение найденных значений для f_1 и f_2 получаем $f_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$. Продолжая аналогичным образом, можно получить выражение через элементарные симметрические полиномы любой конкретной степенной суммы f_k.

Для обработки БЧХ-кодов все эти вычисления необходимо проводить в поле $GF(2^m)$ – поле характеристики 2. Здесь $1+1=0$. Поэтому формулы несколько меняются. Здесь $f_2 = \sigma_1^2$; $f_3 = \sigma_1^3 + \sigma_1\sigma_2 + \sigma_3$; $f_4 = \sigma_1^4$. Выражение для f_5 зависит от $t = n$: если $n > 5$, то для выражения f_5 через элементарные симметрические многочлены применяем формулу (2.6), в противном случае – формулу (2.7).

Предположим, что мы применяем БЧХ-код C_7, исправляющий тройные ошибки, т. е. код с параметром $t = 3$. Тогда для исправления тройных ошибок необходимо решить следующий более простой аналог системы (2.5):

$$\begin{cases} x_1 + x_2 + x_3 = s_1, \\ x_1^3 + x_2^3 + x_3^3 = s_2, \\ x_1^5 + x_2^5 + x_3^5 = s_3. \end{cases} \qquad (2.8)$$

В данном случае для выражения f_5 через элементарные симметрические многочлены следует воспользоваться формулой (2.7). В таком случае $f_5 = f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = \sigma_1^5 + (\sigma_1^3 + \sigma_1\sigma_2 + \sigma_2)\sigma_2 + \sigma_1^2\sigma_3$, и т. д.

Посмотрим, однако, на соотношения (2.6) – (2.7) с противоположной точки зрения – как на соотношения для определения элементарных симметрических полиномов. Фактически уравнения (2.5) и (2.8) определяют значения степенных сумм f_k. Тогда уравнения (2.7) – (2.8) определяют систему линейных уравнений для нахождения σ_k. Так, для БЧХ-кода C_7 эта система линейных уравнений имеет вид

$$\begin{cases} \sigma_1 = f_1 = s_1, \\ f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = f_3 = s_2, \\ f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = f_5 = s_3 \end{cases} \quad \text{или} \quad \begin{cases} \sigma_1 = s_1, \\ s_1^2\sigma_1 + s_1\sigma_2 + \sigma_3 = s_2, \\ s_1^4\sigma_1 + s_2\sigma_2 + s_1^2\sigma_3 = s_3. \end{cases} \qquad (2.9)$$

Предположим, мы решили такую систему уравнений и нашли значения элементарных симметрических многочленов $\sigma_1 = \sigma_1^0, \sigma_2 = \sigma_2^0, \ldots, \sigma_t = \sigma_t^0$. Этой информацией мы можем воспользоваться для нахождения координат ошибочных позиций принятого с помощью БЧХ-кода C_{2t+1} сообщения $\bar{x}$. Идея эта базируется на следующей классической теореме о связи корней алгебраических уравнений с коэффициентами этих уравнений.

Теорема Виета. *Пусть коэффициенты уравнения*

$$x^t + \sigma_1^0 x^{t-1} + \ldots + \sigma_t^0 = 0 \qquad (2.10)$$

принадлежат полю F. *Элементы* $x_1, x_2, ..., x_t$ *поля* F *являются корнями данного уравнения тогда и только тогда, когда*

$$\begin{aligned}
&x_1 + x_2 + ... + x_t = -\sigma_1^0,\\
&x_1x_2 + x_1x_3 + ... + x_{t-1}x_t = \sigma_2^0,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&x_1x_2 \cdot ... \cdot x_{t-1} + x_1x_2 \cdot ... \cdot x_{n-2}x_t + ... + x_2x_3 \cdot ... \cdot x_t = (-1)^{t-1}\sigma_{t-1}^0,\\
&x_1x_2 \cdot ... \cdot x_t = (-1)^t \sigma_t^0.
\end{aligned} \qquad (2.11)$$

Теорему Виета будем применять следующим образом. По найденным $\sigma_1 = \sigma_1^0, \sigma_2 = \sigma_2^0, ..., \sigma_t = \sigma_t^0$ в силу соотношений (2.11) составляем уравнение (2.10), называемое уравнением локаторов ошибок. Алгебраические уравнения над полями Галуа $GF(2^m)$ проще всего решать методом Чэня, т. е. последовательной подстановкой в уравнение элементов данного поля. Найдя корни $x_1 = x_1^0, x_2 = x_2^0, ..., x_t = x_t^0$, мы однозначно определяем вектор $\bar{e}$ и, следовательно, исправляем принятое сообщение.

Пример 2.2.3. В системе связи, построенной на основе примитивного БЧХ-кода C_7 длиной 63 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, $0 \le i \le 62$, α – примитивный элемент поля Галуа $F(16)$, корень неприводимого полинома $x^6 + x^5 + x^4 + x + 1$, принято сообщение $\bar{x}$ с синдромом

$$\bar{S} = \bar{S}(\bar{x}) = (\alpha^{21}, \alpha^{44}, \alpha^{27})^T.$$

Выяснить наличие ошибок в этом сообщении и попытаться их исправить.

Решение. Система линейных уравнений (2.9) здесь имеет вид

$$\begin{cases} \sigma_1 = s_1 = \alpha^{21}, \\ \alpha^{42} \cdot \alpha^{21} + \alpha^{21} \cdot \sigma_2 + \sigma_3 = \alpha^{44}, \\ \alpha^{84} \cdot \alpha^{21} + \alpha^{44}\sigma_2 + \alpha^{42}\sigma_3 = \alpha^{27} \end{cases} \quad \text{или} \quad \begin{cases} \sigma_1 = \alpha^{21}, \\ \alpha^{21}\sigma_2 + \sigma_3 = \alpha^{12}, \\ \alpha^{44}\sigma_2 + \alpha^{42}\sigma_3 = \alpha^{29}. \end{cases}$$

Несложные вычисления показывают, что здесь $\sigma_2 = \alpha^{41}$; $\sigma_3 = \alpha^{60}$. Теперь можно составить уравнение (2.10) $x^3 + \alpha^{21}x^2 + \alpha^{41}x + \alpha^{60} = 0$. Кропотливые вычисления методом Чэня позволяют найти следующие корни этого уравнения: $x_1 = \alpha^{10}$; $x_2 = \alpha^{20}$; $x_3 = \alpha^{30}$. Следовательно, в принятом сообщении имеется тройная ошибка на 11, 21 и 31-й позициях.

В заключение заметим, что представленный синдромный метод декодирования не лишен недостатков. В его реализации имеются такие громоздкие этапы, как нахождение коэффициентов уравнения (2.10) и его решение переборным методом Чэня. Обойти все эти сложности синдромного метода позволяет теория норм синдромов.

Глава 3. Нормы синдромов и их свойства

Теория норм синдромов – синдромный метод, который опирается на свойства автоморфизмов кодов. Нормы синдромов – это синдромные инварианты автоморфизмов кодов.

§3.1. Автоморфизмы кодов. Орбиты векторов ошибок

Определение 2.3.1. Автоморфизмом кода C называется произвольная перестановка координат кодовых слов, которая преобразует кодовые слова в новые кодовые слова.

Очевидно, множество $AutC$ всех автоморфизмов данного кода образует группу относительно операции их последовательного их применения, подгруппу симметрической группы S_n. Полное описание группы $AutC$ конкретного кода – сложная задача теории помехоустойчивых кодов. Но определенные подгруппы группы автоморфизмов для многих конкретных кодов указать можно.

Теорема 2.3.1. *Пусть* $\sigma -$*оператор циклического сдвига координат векторов, действие которого на произвольный вектор* $\bar{e} = (e_1, e_2, ..., e_n)$ *пространства* $E_n = P_n$ *осуществляется по следующему простому правилу*: $\sigma(e_1, e_2, ..., e_n) = (e_n, e_1, e_2, ..., e_{n-1})$. *Оператор* σ *является автоморфизмом кодов Хемминга*, *БЧХ-кодов с проверочной матрицей* (2.2), *реверсивных кодов.*

Следствие. У каждого кода C длиной n из теоремы 2.3.1 группа автоморфизмов $AutC$ содержит циклическую подгруппу

$$\Gamma = <\sigma> = \{\sigma, \sigma^2, ..., \sigma^n = e\}$$ порядка n.

Определение 2.3.2. Совокупность всех попарно различных векторов-ошибок $\sigma^k(\bar{e}), 0 \le k < n$, называется Γ-орбитой вектора-ошибки $\bar{e}$ в пространстве ошибок E_n и обозначается через $<\bar{e}>$. Γ-орбита называется полной, если она содержит n векторов, в противном случае Γ-орбиту называют неполной.

Γ-орбиты имеют четкую структуру, которую описывает

Теорема 2.3.2. *Для произвольного фиксированного вектора* $\bar{e}$ *из пространства ошибок* $E_n = P_n$ *его* Γ*-орбита* $<\bar{e}>$ *состоит из* λ *элементов, где* $\lambda = n$ *или* λ *делит* n. *При этом* $\lambda -$*наименьшее натуральное число с условием* $\sigma^\lambda(\bar{e}) = \bar{e}$ *и* Γ*-орбита* $<\bar{e}>$ *имеет следующую структуру* $<\bar{e}> = \{\bar{e}, \sigma(\bar{e}), \ldots, \sigma^{\lambda-1}(\bar{e})\}$. *Для любых двух векторов-ошибок* $\bar{e}$ *и* $\bar{e}'$ *из* E_n *их* Γ*-орбиты* $<\bar{e}>$ *и* $<\bar{e}'>$ *либо совпадают, либо не имеют одинаковых элементов.*

Из теоремы 2.3.2 следует, что векторы каждой Γ-орбиты имеют тесную взаимосвязь – каждый из них можно получить циклическими сдвигами любого фиксированного вектора этой Γ-орбиты. Подавляющее большинство Γ-орбит принадлежит многообразию полных Γ-орбит. Такая же тесная связь существует и между синдромами векторов-ошибок каждой Γ-орбиты. Об этом свидетельствует

Теорема 2.3.3. *Пусть* $\bar{e}$ *– вектор ошибок в БЧХ-коде C с проверочной матрицей* (2.2). *Пусть* $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ *– синдром ошибок вектора* $\bar{e}$. *Тогда*

$$S(\sigma(\bar{e})) = (\beta^b \cdot s_1, \beta^{b+1} \cdot s_2, ..., \beta^{b+i-1} \cdot s_i, ..., \beta^{b+\delta-2} \cdot s_{\delta-1}); \qquad (2.12)$$

а для произвольного целого λ *синдром*

$$S(\sigma^{\lambda}(\bar{e})) = (\beta^{\lambda b} \cdot s_1, \beta^{\lambda(b+1)} \cdot s_2, ..., \beta^{\lambda(b+i-1)} \cdot s_i, ..., \beta^{\lambda(b+\delta-2)} \cdot s_{\delta-1}). \qquad (2.13)$$

Если же БЧХ-код задан проверочной матрицей (2.3), то

$$S(\sigma(\bar{e})) = (\beta s_1, \beta^3 s_2, \beta^5 s_3, ..., \beta^{2i-1} s_i, ..., \beta^{2t-1} s_t). \qquad (2.14)$$

Пусть C_R^{2r+1} *– реверсивный код с проверочной матрицей* $H = (\alpha^i, \alpha^{-i})^T$. *Тогда* $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^{-1} \cdot s_2)$.

Определение 2.3.3. Спектром синдромов *S*(*J*) в БЧХ-коде *C* *Г*-орбиты *J* называется множество синдромов всех векторов-ошибок из *J* в этом коде. Спектр *S*(*J*) называется полным, если его мощность совпадает с мощностью *Г*-орбиты *J*: |*S*(*J*)| = |*J*|, в противном случае спектр *S*(*J*) будем называть неполным.

Формулы (2.12) – (2.14) определяют структуру спектра синдромов *Г*-орбит векторов-ошибок, дают синдромные признаки полноты *Г*-орбит.

Теорема 2.3.3 утверждает, что как и векторы каждой *Г*-орбиты J, спектр синдромов $S(J)$ можно «сконструировать» по формулам (2.12) – (2.14) из синдрома $S(\bar{e})$ любого вектора $\bar{e} \in J$. Здесь, при условии полноты $S(J)$, существует полное взаимно однозначное соответствие между циклическими сдвигами векторов и соответствующими преобразованиями их синдромов.

Норма синдрома – это векторная характеристика векторов-ошибок, вычисляемая через координаты синдрома.

Определение 2.3.4. Нормой синдрома $S(\bar{e}) = (s_1, s_2, ..., s_{\delta-1})$ вектора ошибок $\bar{e}$ в БЧХ-коде *C* с проверочной матрицей (2.2) называется вектор

$$\bar{N}(S(\bar{e})) = (N_{12}, N_{13}, ..., N_{1(\delta-1)}, N_{23}, ..., N_{(\delta-2)(\delta-1)})$$

с $C_{\delta-1}^2$ координатами $N_{ij}, 1 \le i < j \le \delta - 1$, которые вычисляются по формулам:

а) $N_{ij} = \infty$, если $s_j \neq 0$, $s_i = 0$; $N_{ij} = -$ (не существует), если $s_i = s_j = 0$;

б) $N_{ij} = s_j^{(b+i-1)/h_{ij}} / s_i^{(b+j-1)/h_{ij}}$, если $s_i \neq 0$. (2.15)

В двоичном БЧХ-коде с проверочной матрицей (2.3) синдром имеет меньше координат – t, следовательно, норма синдрома есть вектор

$$\bar{N} = \bar{N}(S) = (N_{12}, N_{13}, ..., N_{1t}, N_{23}, ..., N_{(t-1)t})$$

с C_t^2 координатами, которые для $h_{ij} = \text{НОД}(2i-1, 2j-1)$ вычисляются в случае $s_i \neq 0$ по формуле

$$N_{ij} = s_j^{(2i-1)/h_{ij}} \Big/ s_i^{(2j-1)/h_{ij}}. \qquad (2.16)$$

Пусть $t=2,$ т. е. БЧХ-код C задается проверочной матрицей $H=(\beta^i,\beta^{3i}),\ 0\le i\le n-1.$ Тогда норма синдрома состоит из одной компоненты $N=s_2/s_1^3.$ Пусть $t=3,$ т. е. БЧХ-код C задается проверочной матрицей $H=(\beta^i,\beta^{3i},\beta^{5i}),\ 0\le i\le n-1.$ Тогда норма синдрома, согласно формуле (2.16), состоит из трех компонент $N_1=s_2/s_1^3;\ N_2=s_3/s_1^5;\ N_3=s_3^3/s_2^5.$ Они соответствуют компонентам $N_{13},\ N_{15},\ N_{35}$ определения 2.3.4 при $b=1.$

Определение 2.3.5. Нормой синдрома $S(\bar{e})=(s_1,s_2)$ вектора ошибки $\bar{e}$ в реверсивном коде C_R^{2r+1} с проверочной матрицей $H=(\alpha^i,\alpha^{-i})^T$ называется величина $N=N(S(\bar{e}))=s_1\cdot s_2.$

Предложение 2.3.1. Пусть в БЧХ-коде C_{2t+1} синдром $S=(s_1,s_2,...,s_t)$ имеет координату $s_1\ne 0.$ Тогда для всех целых $i,\ j,\ 2\le i<j\le t,$ справедлива формула $N_{ij}=\left(N_{1j}\right)^{\frac{2i-1}{h_{ij}}}\Big/\left(N_{1i}\right)^{\frac{2j-1}{h_{ij}}}$, т. е. все координаты вектора $\bar{N}(S)$ определяются его первыми $t-1$ координатами.

Основное свойство норм синдромов отражает

Теорема 2.3.4. *Для всякого вектора ошибок $\bar{e}$ и его синдрома $S(\bar{e})$ в БЧХ-коде C справедливо равенство $\bar{N}(S(\sigma(\bar{e})))=\bar{N}(S(\bar{e}))$. Это же равенство справедливо и для реверсивных кодов C_R^{2r+1}.*

Из теоремы 2.3.4 следует, что все векторы каждой Γ-орбиты имеют одинаковую норму синдрома, т. е. норма синдрома инвариантна относительно группы Γ циклических сдвигов. Это позволяет ввести

Определение 2.3.6. Нормой $N(J)$ Γ-орбиты J векторов-ошибок в любом БЧХ-коде, а также и в реверсивном коде, называется норма синдрома любого вектора-ошибки из этой Γ-орбиты.

Норма Γ-орбиты является ее однозначной характеристикой, т. е. идентификатором этой орбиты.

Предложение 2.3.2. Пусть J_1,J_2 – две Γ-орбиты векторов-ошибок в БЧХ-коде C (в реверсивном коде C_R^{2r+1}), имеющие различные нормы: $N(J_1)\ne N(J_2)$. Тогда для любых векторов $\bar{g}\in J_1$ и $\bar{f}\in J_2$ их синдромы $S(\bar{f})$ и $S(\bar{g})$ различны. Другими словами, спектры синдромов таких Γ-орбит не пересекаются.

Предложение 2.3.3. Пусть I и J – две Γ-орбиты векторов-ошибок с одинаковыми нормами в примитивном двоичном БЧХ-коде C_{2t+1} (в реверсивном коде C_R^{2r+1}). Пусть I – полная Γ-орбита с полным спектром синдромов. Тогда для всякого вектора $\bar{f}\in J$ найдется вектор $\bar{e}\in I$, такой, что $S(\bar{e})=S\left(\bar{f}\right).$

Следствие. Множество Γ-орбит всех векторов-ошибок весом 1–3 имеет в примитивном двоичном БЧХ-коде C_7 попарно различные нормы. Множество Γ-орбит всех векторов-ошибок весом 1–2 имеет в примитивном двоичном БЧХ-коде C_5 попарно различные нормы.

Пример 2.3.1. Составим табл. 2.1 образующих всех Γ-орбит 15-мерных векторов-ошибок весом 1–3, их синдромов и норм синдромов в БЧХ-коде C_7 над полем $GF(2^4)$ с примитивным элементом α – корнем полинома $x^4 + x + 1$.

Из табл. 2.1 непосредственно видно, что все выписанные в ней нормы попарно различны в полном соответствии со следствием из предложения 2.3.3.

Построенная теория позволяет предложить норменный метод коррекции ошибок в БЧХ-кодах. Суть метода такова. Составляем таблицу всех Γ-орбит $<\bar{e}_i>$ корректируемых ошибок, таблицу синдромов $S(\bar{e}_i)$, а также таблицу $\overline{N}(S(\bar{e}_i))$. По принятому вектору-сообщению вычисляем $S(\bar{x}) = S(\bar{e})$ и $\overline{N}(S(\bar{e}))$. В таблице норм находим $\overline{N}(S(\bar{e}_i)) = \overline{N}(S(\bar{e}))$. Тогда вектор $\bar{e} \in <\bar{e}_i>$. Сравнивая первые компоненты синдромов $S(\bar{e}_i)$ и $S(\bar{x}) = S(\bar{e})$, определяем величину λ циклического сдвига для получения вектора $\bar{e}$ из вектора $\bar{e}_i$. Тогда $\bar{e} = \sigma^{\lambda}(\bar{e}_i)$ – искомый вектор ошибок.

Таблица 2.1

Образующие Г-орбит ошибок весом 1, 2, 3 в пространстве E_{15}, их синдромы и нормы синдромов

№	Образующая $\bar{e}$ Γ-орбиты	*Синдром* $S(\bar{e})$	*Норма* $\overline{N}$ *Г-орбиты*
1	**2**	**3**	**4**
1	(1)	(1, 1, 1)	(1, 1, 1)
2	(1, 2)	(α^4, α^{14}, α^{10})	(α^2, α^5, α^5)
3	(1, 3)	(α^8, α^{13}, α^5)	(α^4, α^{10}, α^{10})
4	(1, 4)	(α^{14}, α^7, 0)	(α^{10}, 0, 0)
5	(1, 5)	(α, α^{11}, α^{10})	(α^8, α^5, α^5)
6	(1, 6)	(α^{10}, 0, α^5)	(0, 1, ∞)
7	(1, 7)	(α^{13}, α^{14}, 0)	(α^5, 0, 0)
8	(1, 8)	(α^9, α^{13}, α^9)	(α, α^{10}, α^{10})
9	(1, 2, 3)	(α^{10}, α^8, 0)	(α^8, 0, 0)
10	(1, 2, 4)	(α^7, α^4, α^5)	(α^{13}, 1, α^{10})
11	(1, 3, 4)	(α^{13}, α^{10}, α^{10})	(α, α^5, α^{10})
12	(1, 2, 5)	(0, α^5, 1)	(∞, ∞, α^5)
13	(1, 3, 5)	(α^5, α, 0)	(α, 0, 0)
14	(1, 4, 5)	(α^9, α^2, α^5)	(α^5, α^5, α^5)
15	(1, 2, 6)	(α^8, α^3, 0)	(α^9, 0, 0)
16	(1, 3, 6)	(α^4, α^6, 1)	(α^9, α^{10}, 1)
17	(1, 4, 6)	(α^{12}, α^9, α^{10})	(α^3, α^{10}, 1)
18	(1, 5, 6)	(α^2, α^{12}, 0)	(α^6, 0, 0)

Окончание табл. 2.1

1	**2**	**3**	**4**
19	(1, 2, 7)	(α^{12}, 1, α^{5})	(α^{9}, α^{5}, 1)
20	(1, 3, 7)	(α^{14}, α^{8}, α^{10})	(α^{11}, 1, α^{5})
21	(1, 4, 7)	(α^{8}, α^{4}, 1)	(α^{10}, α^{5}, α^{10})
22	(1, 5, 7)	(α^{11}, α^{5}, α^{5})	(α^{2}, α^{10}, α^{5})
23	(1, 6, 7)	(α^{7}, α^{3}, α^{10})	(α^{12}, α^{5}, 1)
24	(1, 2, 8)	(α^{3}, α^{8}, 1)	(α^{14}, 1, α^{5})
25	(1, 3, 8)	(α^{11}, 1, 0)	(α^{12}, 0, 0)
26	(1, 4, 8)	(α, α^{10}, α^{5})	(α^{7}, 1, α^{10})
27	(1, 5, 8)	(α^{14}, α, 1)	(α^{4}, α^{5}, α^{10})
28	(1, 6, 8)	(α^{6}, α^{6}, 0)	(α^{3}, 0, 0)
29	(1, 7, 8)	(α^{5}, α^{8}, α^{5})	(α^{8}, α^{10}, α^{5})
30	(1, 2, 9)	(α^{5}, α^{4}, 0)	(α^{4}, 0, 0)
31	(1, 3, 9)	(0, α^{10}, 1)	(∞, ∞, α^{10})
32	(1, 4, 9)	(α^{6}, 1, α^{10})	(α^{12}, α^{10}, 1)
33	(1, 5, 9)	(α^{10}, α^{2}, α^{0})	(α^{2}, 0, 0)
34	(1, 6, 9)	(α, α^{9}, 1)	(α^{6}, α^{10}, 1)
35	(1, 7, 9)	(α^{3}, α^{4}, α^{10})	(α^{10}, α^{10}, α^{10})
36	(1, 4, 10)	(α^{4}, α^{2}, 1)	(α^{5}, α^{10}, α^{5})
37	(1, 5, 10)	(α^{3}, 1, α^{5})	(α^{6}, α^{5}, 1)
38	(1, 6, 10)	(α^{13}, α^{12}, α^{10})	(α^{3}, α^{5}, 1)
39	(1, 6, 11)	(0, 1, 0)	(∞, –, 0)

Задания для аудиторной работы

Задание 2.1. В задании 1.19 (ч. 1 данного пособия) явно построена двоичная проверочная (8×15)-матрица $H=(\alpha^i, \alpha^{3i})^T$, $0\le i\le 14$, α – корень полинома $p(x)=x^4+x^3+1$, (15, 7)-БЧХ-кода C_5:

$$H=\begin{pmatrix} 0&0&0&1&1&1&1&0&1&0&1&1&0&0&1\\ 0&0&1&0&0&0&1&1&1&1&0&1&0&1&1\\ 0&1&0&0&0&1&1&1&1&0&1&0&1&1&0\\ 1&0&0&0&1&1&1&1&0&1&0&1&1&0&0\\ 0&1&1&0&0&0&1&1&0&0&0&1&1&0&0\\ 0&0&1&1&0&0&0&1&1&0&0&0&1&1&0\\ 0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\ 1&0&1&1&1&1&0&1&1&1&1&0&1&1&1 \end{pmatrix}.$$

Найти порождающую матрицу этого кода.

Решение. Строки порождающей код матрицы G состоят из координат базисных векторов ядра проверочной матрицы H этого кода. Иными словами, матрица G составлена из фундаментальной системы решений однородной системы уравнений $H\cdot\bar{x}^T=\bar{0}^T$. Классический метод решения такой системы – метод Гаусса – Жордана. Суть метода – в элементарных преобразованиях системы, т. е. строк матрицы H, которые приводят систему, т. е. матрицу H к квазитреугольному виду, а затем к виду $H'=(E_{n-k}|K)$ или подобному виду. Здесь E_{n-k} – единичная матрица порядка $n-k$. После этого до получения матрицы G, как говорят, рукой подать.

Попытаемся привести матрицу H к виду H'. Для этого прибавим 4-ю и 6-ю строки к 8-й; в результате 8-я строка преобразуется к виду $(0\ 0\ 0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1)$. 2-ю строку прибавим к 7-й. Получим строку $(0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0)$. 1-ю и 2-ю строки прибавим к 6-й. Получим строку $(0\ 0\ 0\ 0\ 1\ 1\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0)$. 2-ю и 3-ю строки прибавим к 5-й. Получим строку $(0\ 0\ 0\ 0\ 0\ 1\ 1\ 1\ 0\ 1\ 1\ 0\ 0\ 0\ 1)$. 4-ю строку поменяем местами с 1-й, 2-ю – с 3-й. В итоге получим промежуточную матрицу

$$H''=\begin{pmatrix} 1&0&0&0&1&1&1&1&0&1&0&1&1&0&0\\ 0&1&0&0&0&1&1&1&1&0&1&0&1&1&0\\ 0&0&1&0&0&0&1&1&1&1&0&1&0&1&1\\ 0&0&0&1&1&1&1&0&1&0&1&1&0&0&1\\ 0&0&0&0&0&1&1&1&0&1&1&0&0&0&1\\ 0&0&0&0&1&1&0&0&1&1&1&0&1&0&0\\ 0&0&0&0&1&0&1&0&1&0&0&1&1&1&0\\ 0&0&0&0&0&0&1&1&0&0&1&1&1&0&1 \end{pmatrix}.$$

В матрице H'' 6-ю строку прибавим к 1-й и 4-й, 5-ю – ко второй, 7-ю прибавим к 6-й, 7-ю и 5-ю поменяем местами. В итоге получаем матрицу

$$H^* = \begin{pmatrix} 1&0&0&0&0&0&1&1&1&0&1&1&0&0&0 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1&1&1 \\ 0&0&1&0&0&0&1&1&1&1&0&1&0&1&1 \\ 0&0&0&1&0&0&1&0&0&1&0&1&1&0&1 \\ 0&0&0&0&1&0&1&0&1&0&0&1&1&1&0 \\ 0&0&0&0&0&1&1&0&0&1&1&1&0&1&0 \\ 0&0&0&0&0&1&1&1&0&1&1&0&0&0&1 \\ 0&0&0&0&0&0&1&1&0&0&1&1&1&0&1 \end{pmatrix}.$$

В матрице H^* 6-ю строку прибавим к 7-й, 8-ю – к 1, 3, 4, 5 и 6-й, затем исправленную 7-ю поменяем местами с 8-й. В итоге получаем матрицу

$$H^{**} = \begin{pmatrix} 1&0&0&0&0&0&0&0&1&0&0&0&1&0&1 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1&1&1 \\ 0&0&1&0&0&0&0&0&1&1&1&0&1&1&0 \\ 0&0&0&1&0&0&0&1&0&1&1&0&0&0&0 \\ 0&0&0&0&1&0&0&1&1&0&1&0&0&1&1 \\ 0&0&0&0&0&1&0&1&0&1&0&0&1&1&1 \\ 0&0&0&0&0&0&1&1&0&0&1&1&1&0&1 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \end{pmatrix}.$$

В матрице H^{**} 8-ю строку прибавим к 4, 5, 6 и 7-й. В итоге получаем искомую матрицу

$$H' = \begin{pmatrix} 1&0&0&0&0&0&0&0&1&0&0&0&1&0&1 \\ 0&1&0&0&0&0&0&0&1&1&0&0&1&1&1 \\ 0&0&1&0&0&0&0&0&1&1&1&0&1&1&0 \\ 0&0&0&1&0&0&0&0&0&1&1&1&0&1&1 \\ 0&0&0&0&1&0&0&0&1&0&1&1&0&0&0 \\ 0&0&0&0&0&1&0&0&0&1&0&1&1&0&0 \\ 0&0&0&0&0&0&1&0&0&0&1&0&1&1&0 \\ 0&0&0&0&0&0&0&1&0&0&0&1&0&1&1 \end{pmatrix} = (E_8 | K).$$

Мы установили, что система линейных уравнений $H \cdot \bar{x}^T = \bar{0}^T$ эквивалентна системе $(E_8|K) \cdot \bar{x}^T = \bar{0}^T$, которая легко разрешима. В ней 15 неизвестных. Базисный минор составляют первые 8 столбцов матрицы $H' = (E_8|K)$ и базисными переменными являются переменные $x_1, x_2, ..., x_8$. Поэтому свободными переменными являются $x_9, x_{10}, ..., x_{15}$. Положим $x_9 = 1, x_{10} = 0, ..., x_{15} = 0$. Тогда базисные переменные принимают однозначно определенные значения, причем столбец этих значений $(x_1, x_2, ..., x_8)^T$ совпадает с первым столбцом подматрицы K матрицы H'. А в целом получим первый базисный вектор про-

странства решений системы $H \cdot \bar{x}^T = \bar{0}^T$: $\bar{c}_1 = (1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0)$ и одновременно первую строку матрицы G. Пусть $x_9 = 0, x_{10} = 1, x_{11} = 0, ..., x_{15} = 0$. Тогда легко заметить, что столбец значений $(x_1, x_2, ..., x_8)^T$ совпадает со вторым столбцом подматрицы K. А в целом получаем второе решение системы $H \cdot \bar{x}^T = \bar{0}^T$: $\bar{c}_2 = (0\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0)$ и одновременно вторую строку матрицы G и т. д. Придав, наконец, свободным переменным значения $x_9 = 0, ..., x_{14} = 0, x_{15} = 1$, получим столбец значений $(x_1, x_2, ..., x_8)^T$, совпадающий с последним столбцом подматрицы K, а в целом получаем 8-е решение системы и 8-ю строку матрицы:

$$G: \bar{c}_8 = (1\ 1\ 0\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 0\ 0\ 0\ 0\ 1).$$

Таким образом, получена следующая порождающая код матрица

$$G = \begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} = (K^T | E_7).$$

Задание 2.2. С помощью найденной порождающей матрицы закодировать информацию $\bar{i} = (1\ 0\ 0\ 1\ 1\ 0\ 1)$.

Решение. Кодовое слово по данному информационному слову вычисляется по формуле $\bar{c} = \bar{i} \cdot G = (1\ 1\ 0\ 0\ 0\ 0\ 1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 1)$.

Задание 2.3. По найденному в задании 2.2 кодовому слову $\bar{c} = \bar{i} \cdot H$ попытаться восстановить сообщение $\bar{i}$.

Решение. В силу структуры матрицы G информационный вектор $\bar{i}$ идентично отображается на последние 7 координат вектора $\bar{c}$ и, следовательно, однозначно восстанавливается по вектору $\bar{c}$.

Задание 2.4. В первой части задания 1.19 (ч. 1 данного пособия) рассматривается модель ТКС, функционирующей на основе (15, 7)-БЧХ-кода C_5 с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, $0 \le i \le 14$, α – корень полинома $p(x) = x^4 + x^3 + 1$. На приемное устройство ТКС поступило очередное сообщение

$$\bar{x} = (1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1)$$

с синдромом ошибок $S = (0\ 0\ 0\ 1\ 0\ 0\ 0\ 0)^T \neq \bar{0}^T$. По данному синдрому найти вектор ошибок сведением задачи к квадратному уравнению и решением последнего по формулам Чэня. Привести истинное, исправленное сообщение.

Решение. В соответствии со структурой матрицы H данный синдром S разбивается на компоненты $s_1 = (0\ 0\ 0\ 1)$ и $s_2 = (0\ 0\ 0\ 0)$. Их можно ин-

терпретировать как элементы 1 и 0 поля Галуа $GF(2^4)$. (15, 7)-БЧХ-код C_5 исправляет одиночные и двойные ошибки в принимаемых сообщениях. Если бы сообщение $\bar{x}$ содержало одиночную ошибку, то его синдром совпадал бы с одним из столбцов проверочной матрицы

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha & \dots & \alpha^{14} \\ 1 & \alpha^3 & \dots & \alpha^{42} \end{pmatrix}.$$

Очевидно, такого совпадения мы не наблюдаем. Предположим, что сообщение $\bar{x}$ содержит двойную ошибку на неизвестных пока двух позициях. Этим позициям соответствуют столбцы $\begin{pmatrix} \alpha^i & \alpha^{3i} \end{pmatrix}^T$ и $\begin{pmatrix} \alpha^j & \alpha^{3j} \end{pmatrix}^T$ матрицы H с неизвестными целыми значениями i, j. Пусть $\alpha^i = x, \quad \alpha^{ji} = y$. Тогда $\begin{cases} x + y = s_1 = 1, \\ x^3 + y^3 = s_2 = 0. \end{cases}$

Займемся решением этой системы уравнений. Здесь $x^3 + y^3 = (x + y)(x^2 + y^2 + xy) = 1 + xy = 0$. Следовательно, $xy = 1, \quad y + x = 1$. По теореме Виета x и y являются корнями квадратного уравнения $t^2 + t + 1 = 0$. Это уравнение над полем $Z/2Z$ корней не имеет. Но в поле $GF(2^4)$, как показывает непосредственная проверка, у него имеются два различных корня: α^5 и α^{10}. Следовательно, двойная ошибка произошла на 6-й и 11-й позициях и истинным является сообщение

$$\bar{c} = \bar{x} + \bar{e} = (1 \;\; 0 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 1 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 0 \;\; 1 \;\; 1).$$

Задание 2.5. Решить в том же коде ту же задачу из задания 2.4 для сообщения

$$\bar{x} = (0 \;\; 0 \;\; 1 \;\; 1 \;\; 1 \;\; 0 \;\; 1 \;\; 0 \;\; 1 \;\; 1 \;\; 0 \;\; 0 \;\; 1 \;\; 1 \;\; 0).$$

Задание 2.6. Сколько всевозможных ошибок весом 1, 2 и 3 имеется в линейном двоичном коде длиной $n = 9$? А в двоичном коде длиной $n = 15$?

Решение. Координаты двоичных векторов принимают лишь два значения: 0 и 1. Вес двоичного вектора равен количеству его ненулевых координат, т. е. количеству единиц в этом векторе. Таким образом, все двоичные векторы с n координатами и весом 1 имеют лишь одну 1 и остальные координаты равны 0. Очевидно, таких векторов наберется в точности $n -$ по количеству различных координат, на которых эта единица может встретиться. Для количества всевозможных расположений двух 1 на n местах имеется хорошо известная формула

$C_n^2 = \frac{n \cdot (n-1)}{2}$. Это и есть количество всех возможных двойных векторов-ошибок в пространстве V_n над полем $Z/2Z$. Соответственно имеется $C_n^3 = \frac{n \cdot (n-1) \cdot (n-2)}{6}$ ошибок весом 3 в том же пространстве V_n над полем $Z/2Z$. Следовательно, в двоичном пространстве V_9 имеется 9 одиночных ошибок, $\frac{9 \cdot 8}{2} = 36$ двойных ошибок и $\frac{9 \cdot 8 \cdot 7}{2 \cdot 3} = 84$ тройных ошибок.

В двоичном пространстве V_{15} имеется 15 одиночных ошибок, $\frac{15 \cdot 14}{2} = 105$ двойных ошибок и $\frac{15 \cdot 14 \cdot 13}{2 \cdot 3} = 455$ тройных ошибок.

Задание 2.7. На сколько Г-орбит делятся ошибки весом 1, 2 и 3 соответственно в двоичном пространстве V_9? А в пространстве V_{15}?

Решение. Через σ обозначается линейный оператор циклического сдвига координат векторов пространства $P_n = \{(a_1,\ a_2,\ \ldots\ a_n) | a_i \in P\}$ над любым полем P, который на произвольный вектор $\bar{x} = (x_1, x_2, \ldots, x_n) \in P_n$ действует по правилу $\sigma(\bar{x}) = (x_n, x_1, x_2, \ldots, x_{n-1})$. Г – это циклическая подгруппа порядка n в группе $AutP_n$ невырожденных линейных операторов пространства P_n в себя, порожденная оператором σ. $\Gamma = \{\sigma, \sigma^2, \ldots, \sigma^n = e\}$, где e – тождественный оператор.

Для произвольного вектора $\bar{x} \in P_n$ Г-орбитой $< \bar{x} >$ называется совокупность всех тех векторов пространства P_n, которые получаются из $\bar{x}$ под действием операторов их группы Г.

Чаще всего *Г*-орбиты содержат по n векторов и называются полными. Иногда получаются Г-орбиты с количеством векторов, меньшим n. Тогда они называются неполными.

Все векторы-ошибки весом 1 в двоичном пространстве образуют одну Г-орбиту $< \bar{e}_1 >$ для вектора $\bar{e}_1 = (1, 0, \ldots, 0)$. Векторы $\bar{e}_{12} = (110\ldots0)$, $\bar{e}_{13} = (101\ldots0)$ и т. д. порождают полные Г-орбиты векторов-ошибок весом 2. В двоичном пространстве V_9 полные Г-орбиты $< \bar{e}_{12} >, < \bar{e}_{13} >, < \bar{e}_{14} >, < \bar{e}_{15} >$ вместе содержат 36 векторов-ошибок и, следовательно, исчерпывают весь список двойных ошибок. Как установлено в предыдущем задании, в двоичном пространстве V_9 имеется 84 различных тройных векторов-ошибок. Они разбиваются на 9 полных Г-орбит и одну неполную. Неполную Г-орбиту легко определить – это Г-орбита $< \bar{e}_{147} >= \{(100100100), (010010010), (001001001)\}$. К полным Г-орбитам тройных ошибок относятся *Г*-орбиты:

$< \bar{e}_{123} > = < (111000000) >;\ \ < \bar{e}_{124} > = < (110100000) >;$

$< \bar{e}_{125} > = < (110010000) >;\ \ < \bar{e}_{126} > = < (110001000) >;$

$< \bar{e}_{135} > = < (101010000) >;\ < \bar{e}_{136} > = < (101001000) >;$
$< \bar{e}_{127} > = < (110000100) >;\ < \bar{e}_{137} > = < (101000100) >;$
$< \bar{e}_{134} > = < (101100000) >.$

В двоичном пространстве V_{15} имеется одна полная Γ-орбита векторов-ошибок весом 1, 105 векторов-ошибок весом 2 делятся на 7 полных Γ-орбит. Образующие этих орбит представляет следующая табл. 2.2.

Таблица 2.2

Г-орбиты двойных ошибок в двоичном пространстве V_{15}

№	$\bar{e}_{1i}$	Координаты порождающего вектора $\bar{e}_{1i}$														
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1	$\bar{e}_{12}$	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0
2	$\bar{e}_{13}$	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0
3	$\bar{e}_{14}$	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
4	$\bar{e}_{15}$	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0
5	$\bar{e}_{16}$	1	0	0	0	0	1	0	0	0	0	0	0	0	0	0
6	$\bar{e}_{17}$	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
7	$\bar{e}_{18}$	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0

455 тройных векторов-ошибок пространства V_{15} делятся на 30 полных Г-орбит и одну неполную.

Задание 2.8. Выписать формулу, связывающую синдромы векторов-ошибок $\bar{e}$ и $\sigma(\bar{e})$: а) в БЧХ-коде C_5; б) в реверсивном коде C_R; в) в (n, k) – БЧХ-коде C_7, задаваемом проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где $0 \le i \le n-1,\ n = 2^m - 1,\ k = n - 3m,\ \alpha$ – корень примитивного и неприводимого над $Z/2Z$ полинома m-й степени.

Решение. В обоих кодах, определенных над полем $GF(2^m)$, синдром произвольного вектора-ошибки $\bar{e}$ имеет синдром $S(\bar{e}) = (s_1, s_2)$ с компонентами $s_1, s_2 \in GF(2^m)$. Из определения оператора ϖ следует, что в БЧХ-коде C_5 синдром $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2)$, а в реверсивном коде C_R синдром $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^{-1} \cdot s_2)$. В БЧХ-коде C_7 всякий вектор ошибок $\bar{e}$ имеет синдром $S(\bar{e}) = (s_1, s_2, s_3)$ с компонентами $s_1, s_2, s_3 \in GF(2^m)$. Здесь $S(\sigma(\bar{e})) = (\alpha \cdot s_1, \alpha^3 \cdot s_2, \alpha^5 \cdot s_3)$,

Задание 2.9. Сформулировать определение нормы синдрома

$S(\bar{e}) = (s_1, s_2)$ вектора-ошибки $\bar{e}$: а) в БЧХ-коде C_5; б) в реверсивном коде C_R; в) в (n, k) – БЧХ-коде C_7.

Решение. В реверсивном коде C_R нормой синдрома называется величина $N = N(S(\bar{e})) = s_1 \cdot s_2$. Это элемент поля $GF(2^m)$. В БЧХ-коде C_5 нормой синдрома называется величина $N = N(S(\bar{e})) = s_2 / s_1^3 \in GF(2^m)$, если $s_1 \neq 0$. Если $s_1 = 0, s_2 \neq 0,$ то считается $N = \infty$.

В БЧХ-коде C_7 нормой синдрома называется вектор $\bar{N} = \bar{N}(S(\bar{e})) = (N_1, N_2, N_3)$, где $N_1 = s_2 / s_1^3 \in GF(2^m)$, если $s_1 \neq 0$; если $s_1 = 0$, $s_2 \neq 0$, то $N_1 = \infty$; если же $s_1 = 0$, $s_2 = 0$, то $N_1 = -$ (не существует); $N_2 = s_3 / s_1^5 \in GF(2^m)$, если $s_1 \neq 0$; если $s_1 = 0$, $s_3 \neq 0$, то $N_2 = \infty$; если же $s_1 = 0$, $s_3 = 0$, то $N_2 = -$ (не существует); $N_3 = s_3^3 / s_2^5 \in GF(2^m)$, если $s_2 \neq 0$; если $s_2 = 0$, $s_3 \neq 0$, то $N_3 = \infty$; если же $s_2 = 0$, $s_3 = 0$, то $N_3 = -$ (не существует).

Основные свойства нормы синдрома:

– у всех векторов-ошибок отдельно взятой Г-орбиты норма синдрома одна и та же; норма синдрома является характерным признаком, меткой каждой *Г*-орбиты;

– если у двух полных Г-орбит совпадают нормы, то и множества синдромов векторов-ошибок этих орбит также совпадают;

– синдромы всех корректируемых векторов-ошибок попарно различны; следовательно, нормы синдромов Г-орбит ошибок любой корректируемой совокупности имеют попарно различные нормы.

Задание 2.10. В задании 2.7 составлена таблица образующих $\bar{e}_{1i}$, $2 \le i \le 8$, Г-орбит двойных ошибок для (15, 7)-БЧХ-кода C_5. Составить таблицу синдромов образующих $\bar{e}_{1i}$ и их норм синдромов.

Решение. Воспользуемся табл. 1.1 (см. разд. «Задания для аудиторной работы», ч. 1), задающей поле Галуа $GF(2^4)$ с помощью полинома $p(x) = x^4 + x^3 + 1$. Для вектора-ошибки $\bar{e}_{12}$ синдром $S(\bar{e}_{12}) = (s_1, s_2)$, где $s_1 = 1 + \alpha = \alpha^{12}$; $s_2 = 1 + \alpha^3 = \alpha^4$. Тогда

$$N(S(\bar{e}_{12})) = s_2 / s_1^3 = \alpha^4 / \alpha^{36} = \alpha^4 / \alpha^6 = \alpha^4 \cdot \alpha^9 / \alpha^6 \cdot \alpha^9 = \alpha^{13} / \alpha^{15} = \alpha^{13}.$$

Для вектора-ошибки $\bar{e}_{13}$ синдром $S(\bar{e}_{13}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^2 = \alpha^9$; $s_2 = 1 + \alpha^6 = \alpha^8$. Тогда

$$N(S(\bar{e}_{13})) = s_2 / s_1^3 = \alpha^8 / \alpha^{27} = \alpha^8 / \alpha^{12} = \alpha^8 \cdot \alpha^3 / \alpha^{12} \cdot \alpha^3 = \alpha^{11} / \alpha^{15} = \alpha^{11}.$$

Для вектора-ошибки $\bar{e}_{14}$ синдром $S(\bar{e}_{14}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^3 = \alpha^4$; $s_2 = 1 + \alpha^9 = \alpha^2$. Тогда

$$N(S(\bar{e}_{14})) = s_2 / s_1^3 = \alpha^2 / \alpha^{12} = \alpha^2 \cdot \alpha^3 / \alpha^{12} \cdot \alpha^3 = \alpha^5 / \alpha^{15} = \alpha^5.$$

Для вектора-ошибки $\bar{e}_{15}$ синдром $S(\bar{e}_{15}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^4 = \alpha^3$; $s_2 = 1 + \alpha^{12} = \alpha$. Тогда

$$N(S(\bar{e}_{15})) = s_2 / s_1^3 = \alpha / \alpha^9 = \alpha \cdot \alpha^6 / \alpha^9 \cdot \alpha^6 = \alpha^7 / \alpha^{15} = \alpha^7.$$

Для вектора-ошибки $\bar{e}_{16}$ синдром $S(\bar{e}_{16}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^5 = \alpha^{10}$; $s_2 = 1 + \alpha^{15} = 0$. Тогда $N(S(\bar{e}_{16})) = s_2 / s_1^3 = 0 / \alpha^{30} = 0$.

Для вектора-ошибки $\bar{e}_{17}$ синдром $S(\bar{e}_{17}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^6 = \alpha^8$; $s_2 = 1 + \alpha^{18} = 1 + \alpha^3 = \alpha^4$. Тогда

$$N(S(\bar{e}_{17})) = s_2 / s_1^3 = \alpha^4 / \alpha^{24} = \alpha^4 \cdot \alpha^6 / \alpha^{24} \cdot \alpha^6 = \alpha^{10} / \alpha^{30} = \alpha^{10}.$$

Для вектора-ошибки $\bar{e}_{18}$ синдром $S(\bar{e}_{18}) = (s_1, s_2)$, где $s_1 = 1 + \alpha^7 = \alpha^{13}$; $s_2 = 1 + \alpha^{21} = \alpha^8$. Тогда

$$N(S(\bar{e}_{18})) = s_2 / s_1^3 = \alpha^8 / \alpha^{39} = \alpha^8 \cdot \alpha^6 / \alpha^9 \cdot \alpha^6 = \alpha^{14} / \alpha^{15} = \alpha^{14}.$$

Результаты вычислений сведем в единую табл. 2.3.

Таблица 2.3

Образующие Г-орбит двойных ошибок, их синдромы и нормы синдромов в (15, 7)-БЧХ-коде C_5

№	Образующая Г-орбиты $\bar{e}_{1i}$	Синдром $S(\bar{e}_{1i}) = (s_1, s_2)$		Норма $N(S(\bar{e}_{1i}))$
		s_1	s_2	
1	$\bar{e}_{12}$	α^{12}	α^4	α^{13}
2	$\bar{e}_{13}$	α^9	α^8	α^{11}
3	$\bar{e}_{14}$	α^4	α^2	α^5
4	$\bar{e}_{15}$	α^3	α	α^7
5	$\bar{e}_{16}$	α^{10}	0	0
6	$\bar{e}_{17}$	α^8	α^4	α^{10}
7	$\bar{e}_{18}$	α^{13}	α^8	α^{14}

Задание 2.11. Решить задачу 2.4 норменным методом.

Решение. Согласно условию задания 2.4 ТКС на основе (15, 7)-БЧХ-кода C_5 с проверочной матрицей $H = (\alpha^i, \alpha^{3i})^T$, где $0 \le i \le 14$, α – корень полинома $p(x) = x^4 + x^3 + 1$, приняло сообщение $\bar{x} = (1\ 0\ 1\ 0\ 0\ 1\ 1\ 0\ 0\ 0\ 1\ 0\ 0\ 1\ 1)$ с синдромом ошибок $S(\bar{x}) = (1, 0)$. Вычислим норму этого синдрома $N^* = N(S(\bar{x})) = 0/1 = 0$. Сравниваем вычисленную норму с данными табл. 2.3. Как видим, $N^* = N(S(\bar{e}_{16}))$. Следовательно, двойная вектор-ошибка $\bar{e}$, которая

присутствует в сообщении $\bar{x}$, принадлежит Г-орбите $J = <\bar{e}_{16}>$ и получается циклическим сдвигом вектора $\bar{e}_{16}$. Величина циклического сдвига определяется отношением первой компоненты $s_1^{\text{эксп}} = 1$ синдрома $S(\bar{x})$ к первой компоненте $s_1 = \alpha^{10}$ синдрома $S(\bar{e}_{16})$. В данном случае $s_1^{\text{эксп}} / \alpha^{10} = 1/\alpha^{10} = \alpha^5$. Следовательно, искомая ошибка $\bar{e} = \sigma^5(\bar{e}_{16}) = \bar{e}_{6,11}$ – вектор-ошибка весом 2 с единицей на 6-й и 11-й позициях, что полностью совпадает с полученным ранее решением задания 2.4.

Задание 2.12. В (15, 3)-БЧХ-коде C_7 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где $0 \le i \le 14$, α – корень полинома $p(x) = x^4 + x^3 + 1$, принято сообщение $\bar{x} = (11011\ 00101\ 01101)$ с синдромом ошибок $S(\bar{x}) = (\alpha, \alpha^7, \alpha^5)$. Найти вектор ошибок в этом сообщении, если известно, что произошла ошибка весом 3.

Решение. Тройная ошибка в сообщении $\bar{x}$ произошла на неизвестных позициях i, j, k, $1 \le i < j < k \le 15$. В подматрице $\widetilde{H} = (\alpha^i)$ матрицы $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ позициям i, j, k соответствуют столбцы $\alpha^{i-1} = x, \alpha^{j-1} = y, \alpha^{k-1} = z$. Эти столбцы образно называют локаторами ошибочных позиций. Их рассматривают как элементы поля Галуа $GF(2^4)$, задаваемые с помощью полинома $p(x) = x^4 + x^3 + 1$. Синдром $S(\bar{x}) = (\alpha, \alpha^7, \alpha^5)$ получается двоичным сложением столбцов матрицы $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$ с номерами i, j, k. Каждый $\bar{i}$-й столбец матрицы H состоит из трех частей, интерпретируемых как элементы x, x^3, x^5 поля $GF(2^4)$. Поэтому для определения истинных значений позиций i, j, k искомой тройной ошибки с помощью синдрома $S(\bar{x}) = (\alpha, \alpha^7, \alpha^5)$ получаем следующую систему уравнений:

$$\begin{cases} x + y + z = s_1 = \alpha, \\ x^3 + y^3 + z^3 = s_2 = \alpha^7, \\ x^5 + y^5 + z^5 = s_3 = \alpha^5. \end{cases} \qquad (*)$$

Левые части уравнений системы $(*)$ есть симметрические степенные полиномы f_1, f_3, f_5 от трех переменных x, y, z. Здесь $f_k = x^k + y^k + z^k$. В нашем случае, в условиях двоичной арифметики, $f_2 = f_1^2$; $f_4 = f_1^4$. В теории симметрических полиномов существуют формулы, принадлежащие перу великого Ньютона, которые связывают степенные симметрические полиномы с элементарными симметрическими полиномами σ_i. Элементарные симметрические полиномы от трех переменных x, y, z выглядят следующим образом: $\sigma_1 = x + y + z = f_1$; $\sigma_2 = xy + xz + yz$; $\sigma_3 = xyz$.

В полях характеристики 2 формулы Ньютона, связывающие $f_1, f_2, ..., f_5$ с $\sigma_1, \sigma_2, \sigma_3$, имеют специальный вид:

$$\begin{cases} \sigma_1 = f_1, \\ f_2\sigma_1 + f_1\sigma_2 + \sigma_3 = f_3, \\ f_4\sigma_1 + f_3\sigma_2 + f_2\sigma_3 = f_5. \end{cases} \quad (**)$$

Подставим в систему (**) значения f_i из системы (*): $f_1 = s_1$; $f_2 = s_1^2$; $f_3 = s_2$; $f_4 = s_1^4$; $f_5 = s_3$. Получим следующую систему линейных уравнений относительно неизвестных $\sigma_1, \sigma_2, \sigma_3$:

$$\begin{cases} \sigma_1 = s_1, \\ s_1^2\sigma_1 + s_1\sigma_2 + \sigma_3 = s_2, \\ s_1^4\sigma_1 + s_2\sigma_2 + s_1^2\sigma_3 = s_3. \end{cases} \quad (***)$$

Подставим в (***) значения $s_1 = s_2 = \alpha$, $s_3 = \alpha^5$. Получим систему

$$\begin{cases} \sigma_1 = \alpha, \\ \alpha^2\sigma_1 + \alpha\sigma_2 + \sigma_3 = \alpha^7, \\ \alpha^4\sigma_1 + \alpha^7\sigma_2 + \alpha^2\sigma_3 = \alpha^5. \end{cases}$$

Отсюда следует

$$\begin{cases} \alpha\sigma_2 + \sigma_3 = \alpha^7 + \alpha^3 = \alpha^6, \\ \alpha^5\sigma_2 + \sigma_3 = 0. \end{cases}$$

Следовательно, $\sigma_3 = \alpha^5\sigma_2$; $\sigma_2(\alpha^5 + \alpha) = \alpha^6$ или $\sigma_2\alpha^4 = \alpha^6$. Таким образом, $\sigma_2 = \alpha^2$; $\sigma_3 = \alpha^7$. Полученные значения $\sigma_1, \sigma_2, \sigma_3$ служат, согласно теореме Виета, коэффициентами кубического уравнения $t^3 + \sigma_1 t^2 + \sigma_2 t + \sigma_3 = 0$, корнями которого и являются искомые в системе (*) неизвестные x, y, z. Итак, решение системы (*) сводится к поиску корней кубического уравнения $t^3 + \alpha \cdot t^2 + \alpha^2 \cdot t + \alpha^7 = 0$ в поле $GF(2^4)$.

Метод Чэня, т. е. последовательная подстановка в уравнение элементов поля $GF(2^4)$ вместо t, позволяет найти следующие его корни: $x = 1$; $y = \alpha^9$; $z = \alpha^{13}$. Корни однозначно указывают тройную ошибку на 1, 10 и 14-й позициях в сообщении $\bar{x}$. Следовательно, отправлено было истинное сообщение $\bar{c} = (01011\ \ 00100\ \ 01111\ )$.

Задание 2.13. Указать количество тройных векторов-ошибок $\bar{e}$ в БЧХ-коде C_7, синдромы $S(\bar{e}) = (s_1, s_2, s_3)$ которых имеют первую компоненту $s_1 = 0$. Оценить количество Г-орбит таких ошибок.

Решение. Количество T тройных векторов-ошибок $\bar{e}$ в БЧХ-коде C_7, синдромы $S(\bar{e}) = (s_1, s_2, s_3)$ которых имеют первую компоненту $s_1 = 0$, опре-

деляется формулой $T = C_n^2 / 3 = n(n-1)/6$, где $n = 2^m - 1$ – длина кода. Отсюда следует, что количество Г-орбит таких тройных ошибок оценивается числом $T/n = (n-1)/6 = (2^m - 2)/6 = (2^{m-1} - 1)/3$. Это число равно 3 при $n = 15$, 5 – при $n = 31$ и т. д.

Задание 2.14. Решить задачу 2.12 норменным методом.

Решение. В двоичном коде длиной 15 имеется 455 тройных ошибок, которые делятся на 31 орбиту (см. решение задания 2.7). Прямой норменный метод требует построения таблицы образующих всех орбит тройных ошибок, синдромов этих образующих, а также норм синдромов образующих.

Модифицируем норменный метод: преобразуем искомую вектор-ошибку $\bar{e}$ в другую тройную ошибку $\bar{e}^*$, синдром которой имеет первую компоненту $s_1^* = 0$. В решении задания 2.12 x, y, z – локаторы ошибочных позиций вектора $\bar{x}$, ненулевых координат вектора $\bar{e}$. В качестве $\bar{e}^*$ берем вектор-ошибку весом 3 с локаторами ненулевых позиций $x^* = x + s_1$; $y^* = y + s_1$; $z^* = z + s_1$. Тогда компоненты синдрома $S(\bar{e}^*) = (s_1^*, s_2^*, s_3^*)$ выражаются следующим образом через компоненты синдрома $S(\bar{e})$:

$$s_1^* = x^* + y^* + z^* = (x + s_1) + (y + s_1) + (z + s_1) = (x + y + z) + s_1 = s_1 + s_1 = 0;$$

$$s_2^* = (x^*)^3 + (y^*)^3 + (z^*)^3 = (x + s_1)^3 + (y + s_1)^3 + (z + s_1)^3 =$$

$$= x^3 + y^3 + z^3 + s_1(x^2 + y^2 + z^2) + s_1^2(x + y + z) + s_1^3 + s_1^3 + s_1^3 = s_2 + s_1^3;$$

$$s_3^* = (x^*)^5 + (y^*)^5 + (z^*)^5 = (x + s_1)^5 + (y + s_1)^5 + (z + s_1)^5 =$$

$$= (x + s_1)^4 (x + s_1) + (y + s_1)^4 (y + s_1) + (z + s_1)^4 (z + s_1) =$$

$$= x^5 + y^5 + z^5 + s_1(x^4 + y^4 + z^4) + s_1^4(x + y + z) + s_1^5 + s_1^5 + s_1^5 = s_2 + s_1^5 = s_3 + s_1^5.$$

В нашем случае $S(\bar{e}) = (\alpha, \alpha^7, \alpha^5)$. Следовательно, $s_2^* = \alpha^7 + \alpha^3 = \alpha^6$; $s_3^* = \alpha^5 + \alpha^5 = 0$. Таким образом, $S(\bar{e}^*) = (0, \alpha^6, 0)$. Тогда $\bar{N}(S(\bar{e}^*) = (\infty, -, 0)$.

Поищем в нашем (15, 7)-БЧХ-коде C_7 Г-орбиту с такой «экзотической» нормой. Единственная неполная Г-орбита J тройных ошибок в этом коде задается вектором $\bar{e}_J = (1, 6, 11)$ с ненулевыми координатами на 1, 6 и 11-й позициях. Его синдром $S(\bar{e})$ имеет компоненты $s_1 = 1 + \alpha^5 + \alpha^{10} = 0$; $s_2 = 1 + \alpha^{15} + \alpha^{30} = 1$; $s_3 = 1 + \alpha^{25} + \alpha^{50} = 1 + \alpha^{10} + \alpha^5 = 0$. $\bar{N}(S(\bar{e})) = (\infty, -, 0) = \bar{N}(S(\bar{e}))^*$. Следовательно, $\bar{e}^* \in J$ и получается циклическим сдвигом вектора $\bar{e}_J = (1, 6, 11)$. $S(\sigma(\bar{e}_J)) = (0, \alpha^3, 0)$. $S(\sigma^2(\bar{e}_J)) = (0, \alpha^6, 0) = S(\bar{e}^*)$. Значит, $\bar{e}^* = \sigma^2(\bar{e}_J) = (3, 8, 13)$ – тройная вектор-ошибка с ненулевыми координатами на 3, 8, 13-й позициях, локаторы которых $x^* = \alpha^2$, $y^* = \alpha^7$, $z^* = \alpha^{12}$. Отсюда легко находятся локаторы x, y, z ненулевых координат искомого вектора ошибок $\bar{e}$:

$x = x^* + s_1 = \alpha^2 + \alpha = \alpha^{13}$; $y = y^* + s_1 = \alpha^7 + \alpha = \alpha^9$; $z = z^* + s_1 = \alpha^{12} + \alpha = 1$.

Следовательно, $\bar{e} = (1, 10, 14)$ – тройная ошибка на 1, 10 и 14-й позициях, что полностью совпадает с решением задания 2.12.

Контрольная работа «Теория норм синдромов»

Задание 1. Найти порождающую (21×31)-матрицу G по построенной в задании 7 из контрольной работы «Прикладная математика» для двоичной проверочной (10×31)-матрицы H БЧХ-кода (или реверсивного, в зависимости от вашего варианта).

Задание 2. С помощью найденной порождающей матрицы закодировать информацию: $\bar{i} = (111\,011\,001\,000\,100\,110\,001)$.

Задание 3. По найденному в задании 2 кодовому слову $\bar{c} = \bar{i} \cdot H$ попытаться восстановить сообщение $\bar{i}$.

Задание 4. По найденному в задании 7 синдрому из контрольной работы «Прикладная математика» найти вектор ошибок сведением задачи к квадратному уравнению и решением последнего по формулам Чэня.

Задание 5. Для рассматриваемого в задании 4 кода данной контрольной работы составить таблицу образующих $\bar{e}_i$ Г-орбит двойных ошибок, синдромов $S(\bar{e}_i)$ и норм $N_i = N(S(\bar{e}_i))$. По синдрому из задания 7 в контрольной работе «Прикладная математика» найти вектор-ошибку норменным методом.

Задание 6. В $(31, 16)$-БЧХ-коде C_7 с проверочной матрицей $H = (\alpha^i, \alpha^{3i}, \alpha^{5i})^T$, где α – корень примитивного полинома $p(x)$, принято сообщение $\bar{x}$ с синдромом $S = S(\bar{x}) = (s_1, s_2, s_3)$. Найти вектор ошибок в принятом сообщении сведением задачи к кубическому уравнению и решением этого уравнения методом Чэня. Данные представлены в следующих вариантах:

В.1: $p(x) = x^5 + x^2 + 1$, $S = (\alpha^{24}, \alpha^2, \alpha^{16})$;

В.2: $p(x) = x^5 + x^3 + 1$, $S = (\alpha^{20}, \alpha^{23}, \alpha^{13})$;

В.3: $p(x) = x^5 + x^3 + x^2 + x + 1$, $S = (\alpha^{18}, \alpha^{14}, \alpha^{27})$;

В.4: $p(x) = x^5 + x^4 + x^2 + x + 1$, $S = (\alpha^{28}, \alpha^{29}, \alpha^{28})$;

В.5: $p(x) = x^5 + x^4 + x^3 + x + 1$, $S = (\alpha^{16}, \alpha^{29}, \alpha^9)$;

В.6: $p(x) = x^5 + x^4 + x^3 + x^2 + 1$, $S = (\alpha^{11}, \alpha^{12}, \alpha^7)$;

В.7: $p(x) = x^5 + x^2 + 1$, $S = (\alpha^{20}, 1, 0)$;

В.8: $p(x) = x^5 + x^3 + 1$, $S = (\alpha^2, \alpha^4, \alpha^{30})$;

В.9: $p(x) = x^5 + x^3 + x^2 + x + 1$, $S = (\alpha^{22}, \alpha^{17}, \alpha^{11})$;

В.10: $p(x) = x^5 + x^4 + x^2 + x + 1$, $S = (\alpha^6, \alpha^6, \alpha^{21})$.

Задание 7. Задачу из задания 6 решить норменным методом.

Литература

1. Шеннон, К. Работы по теории информации и кибернетике / К. Шеннон. – М. : ИЛ, 1963. – 732 с.

2. Мак-Вильямс, Ф. Дж. Теория кодов, исправляющих ошибки / Ф. Дж. Мак-Вильямс, Н. Дж. А. Слоэн. – М. : Связь, 1979. – 744 с.

3. Самсонов, Б. Б. Теория информации и кодирование / Б. Б. Самсонов [и др.]. – Ростов н/Д: Феникс, 2002. – 288 с. – (Серия «Учебники и учебные пособия»).

4. Прикладная теория кодирования : учеб. пособие для вузов / В. К. Конопелько [и др.]. – Т. 1–2. – Минск : БГУИР, 2004. – 688 с.

5. Липницкий, В. А. Современная прикладная алгебра. Математические основы защиты информации от помех и несанкционированного доступа : учеб.-метод. пособие / В. А. Липницкий. – Минск : БГУИР, 2005, 2-е изд.: Минск : БГУИР, 2006. – 88 с.

6. Конопелько, В. К. Теория норм синдромов и перестановочное декодирование помехоустойчивых кодов / В. К. Конопелько, В. А. Липницкий. – 2-е изд. – М. : УРСС, 2004. – 176 с.

7. Липницкий, В. А. Норменное декодирование помехоустойчивых кодов и алгебраические уравнения / В. А. Липницкий, В. К. Конопелько. – Минск : Изд. центр БГУ, 2007. – 240 с.

8. Липницкий, В. А. Норменное декодирование ошибок посредством их модификации / В. А. Липницкий, Е. К. Аль-Хайдар // Доклады БГУИР, №5(43) – 2009. – С. 12 – 16.

9. Вернер, М. Основы кодирования : учеб. для вузов / М. Вернер. – М. : Техносфера, 2006. – 288 с.

10. Морелос-Сарагоса, Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение : учеб. пособие для вузов / Р. Морелос-Сарагоса. – М.: Техносфера, 2006. – 320 с.

11. Лидл, Р. Конечные поля. В 2 т. / Р. Лидл, Г. Нидеррайтер. – М. : Мир, 1988. – 820 с.

12. Виноградов, И. М. Основы теории чисел / И. М. Виноградов. – М. : Наука, 1972. – 168 с.

13. Каргаполов, М. И. Основы теории групп / М. И. Каргаполов, Ю. И. Мерзляков. – М. : Наука, 1972. – 240 с.

14. Кострикин, А. И. Введение в алгебру / А. И. Кострикин. – М. : Наука, 1977. – 496 с.

15. Введение в криптографию / под ред. В. В. Ященко. – 2-е изд. – М. : МЦНМО, 1999. – 272 с.

16. Смарт, Н. Криптография / Н. Смарт. – М. : Техносфера, 2005. – 526 с.

Св план 2010, поз. 63

Учебное издание

Липницкий Валерий Антонович

Спичекова Наталья Викторовна

ПРИКЛАДНАЯ МАТЕМАТИКА И ТЕОРИЯ НОРМ СИНДРОМОВ

Методическое пособие
для студентов специальностей
1-45 01 03 «Сети телекоммуникаций»,
1-45 01 05 «Системы распределения мультимедийной информации»,
1-98 01 02 «Защита информации в телекоммуникациях»
заочной и дистанционной форм обучения

Редактор Г. С. Корбут
Корректор Е. Н. Батурчик

Подписано в печать	Формат 60x84 1/16.	Бумага офсетная.
Гарнитура «Таймс».	Отпечатано на ризографе.	Усл. печ. л.
Уч.-изд. л. 4,0.	Тираж 150 экз.	Заказ 187.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники»
ЛИ №02330/0494371 от 16.03.2009. ЛП №02330/0494175 от 03.04.2009.
220013, Минск, П. Бровки, 6