ФЕДЕРАЛЬНОЕ АГЕНТСТВО ВОЗДУШНОГО ТРАНСПОРТА

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ

"МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ГРАЖДАНСКОЙ АВИАЦИИ "(МГТУ ГА)

Кафедра прикладной математики

Г.И. Калмыков

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению лабораторных работ по дисциплине

ТЕОРИЯ КОДИРОВАНИЯ

для студентов III курса специальности 090106 "Информационная безопасность"дневного обучения

Москва — 2007

Рецензент — д. т. н. профессор Кузнецов В.Л. Калмыков Г.И. Методические указания к выполнению лабораторных работ по дисциплине "Теория кодирования": МГТУ ГА, 2008 25 с.

Данные методические указания издаются в соответствии с учебным планом для студентов III курса специальности 090106 "Информационная безопасность"дневного обучения. Они содержат описание четыре лабораторных работ, каждая из которых рассчитана на 4 академических часа, необходимые для их выполнения теоретические сведения и примеры решения задач, аналогичных задачам, включенным в лабораторные работы. Цель пособия — помочь студентам в выполнении лабораторных работ по дисциплине "Теория кодирования".

Данные методические указания издаются в соответствии с рабочей программой учебной дисциплины ЕН.Р.02 "Теория кодирования"по Учебному плану специальности 090106 "Информационная безопасность", утвержденному 25 января 2007 года, для студентов III курса дневного обучения.

Рассмотрены и одобрены на заседаниях кафедры 17.04.08 и методического совета 24.04.08.

Введение

Данные методические указания предназначены для студентов III–го курса дневной формы обучения специальности 090106 "Информационная безопасность"и содержат описание четырех лабораторных работ, каждая из которых рассчитана на 4 академических часа.

Цель проведения лабораторных работ:

- помочь студентам в закреплении необходимых теоретических сведений по предмету, на основе которых решаются задачи информационной безопасности коммуникационных систем;
- дать студентам некоторые навыки анализа коммуникационных систем в целях защиты безопасности информации и научить основным методам кодирования и декодирования информации;
- дать студентам возможность практики вычислений на компьютере и оформления с его помощью лабораторной работы.

Предполагается, что студенты приходят на занятия, предварительно изучив методические указания.

Отчет по лабораторной работе должен содержать:

- титульный лист, в котором указаны:

  номер и название лабораторной работы,

  группа,

  фамилия и инициалы студента,

  дата выполнения работы;
- номер варианта (если он есть) и текст задания;
- краткий конспект теоретической части;
- результаты вычислений;
- ответы на поставленные в задании вопросы.

Отчеты по всем лабораторным работам помещаются в отдельную тетрадь. Если отчет выполнен на отдельных листах, то они сшиваются вместе.

Отчет необходимо напечать шрифтом 12 или четко написать от руки чернилами.

По каждой работе студент должен получить зачет. Защита лабораторной работы состоит из ответов на контрольные вопросы по теоретической части работы и по ходу ее выполнения.

Работа 1. Код Фано

Цель работы — научить студентов методу построения кодовой таблицы кода Фано и кодированию текстов в этом коде.

1. Общие сведения

Пусть источник сообщений вырабатывает k сообщений $A_1, A_2, \ldots, A_k$. Без ограничения общности можно считать, что их вероятности удовлетворяют неравенствам

$$P\{A_1\} \geq P\{A_1\} \geq \ldots \geq P\{A_k\}.$$

Опишем сначала общую схему *двоичного кода Фано.*

Разобьем множество всех сообщений на две группы так, чтобы суммы вероятностей сообщений по каждой из этих двух групп были как можно более близки друг к другу. При этом вероятность любого из сообщений первой группы должна быть не менее наибольшей из вероятностей сообщений второй группы. Для всех сообщений из одной группы в качестве первого символа кодового слова выбираем символ 0, а для всех сообщений из другой группы — символ 1.

Каждая из полученных групп, если только она состоит не менее чем из двух сообщений, по тем же правилам снова разбивается на две части, и это разбиение определяет значение второго символа кодового слова в каждом сообщении такой группы.

Процедура продолжается до тех пор, пока все множество не будет разбито на отдельные сообщения. В результате каждому сообщению будет сопоставлено кодовое слово, состоящее из нулей и единиц.

Чем более вероятно сообщение, тем быстрее оно образует самостоятельную группу и тем более коротким словом оно будет закодировано. Это обстоятельство и обеспечивает высокую экономичность кода Фано.

Опишем теперь общую схему кода Фано, когда кодовые слова являются словами в конечном алфавите, состоящем из q букв. В этом случае на каждом шагу разбиение производится на q групп, если только разбиваемое множество сообщений содержит не менее чем q сообщений. Принципы, по которым производится это разбиение, те же, что и в случае двоичного кода Фано. Сформулируем их. Группы, на которые разбивается данное множество, обозначим $G_1, C_2, \ldots, G_q$. Сумму вероятностей сообщений по каждой из этих групп будем называть суммарной вероятностью по этой группе. Введем следующие обозначения: S_i — сумма вероятностей сообщений по группе G_i, $i = 1, 2, \ldots, q$; S_{max} — наибольшая из сумм $S_1, S_2, \ldots, S_q$; S_{min} — наименьшая из сумм $S_1, S_2, \ldots, S_q$; M_i — наибольшая из вероятностей сообщений в группе G_i, $i = 1, 2, \ldots, q$; m_i — наименьшая из вероятностей сообщений в группе G_i, $i = 1, 2, \ldots, q$.

Разбиение на группы должно удовлетворять следующим правилам.

Во-первых, разность $S_{max} - S_{min}$ должна быть как можно меньше. В том случае, когда это требование выполняется, мы будем говорить, что суммарные вероятности по группам максимально близки друг к другу.

Во-вторых, разбиение на группы должно удовлетворять неравенствам $m_i \geq M_{i+1}$, $i = 1, 2, \ldots, q-1$.

Если же разбиваемое множество сообщений содержит менее чем q сообщений, то оно разбивается на отдельные сообщения. То есть в этом случае множество разбивается на столько групп, сколько сообщений оно содержит.

Из определения кода Фано следует, что этот код является префиксным.

2. Лабораторное задание

1. Дано множество событий. Исходя из данных вероятностей появления этих событий, создать для этого множества код Фано, в котором кодовые слова являются словами в конечном алфавите, состоящем из q букв.

2. Закодировать полученным кодом Фано заданную последовательность событий.

Множество событий, их вероятности и число q задаются преподавателем.

Отчет должен быть напечатан шрифтом 12 или четко написан от руки чернилами. Если отчет написан от руки, то в таблицах и кодируемом тексте высота символов 0, 1 и всех букв должна быть равна 0,5 см, а все буквы написаны в печатном виде. При этом каждый символ должен быть вписан в отдельную клетку высотой и шириной 0,5 см. Фамилия в заголовке должна быть написана печатными буквами.

Работа 2. Код Хемминга

Цель работы — ознакомить студентов с методами кодирования и декодирования в коде Хемминга.

1. Общие сведения

Двоичным кодом Хемминга называется двоичный линейный код, позволяющий исправить одиночную ошибку и удовлетворяющий условиям:

1. Длина кодовых векторов равна $2^m - 1$, где $m \geq 3$.

2. Каждый кодовый вектор содержит $2^m - m - 1$ информационных символов и m проверочных символов, а для определения положения одиночной ошибки требуется m проверок. Число m является минимальным числом проверок, необходимых для исправления одиночной ошибки в кодовом векторе длины $2^m - 1$.

Проверочная матрица $\mathbf{H}$ кода Хемминга имеет порядок $m \times (2^m - 1)$. Так как код Хемминга — двоичный линейный код, то элементы проверочной матрицы являются элементами поля $GF(2)$. Все столбцы этой матрицы должны быть ненулевыми и различными. Каждый столбец этой матрицы есть двоичный вектор-столбец длины m. Всего существует 2^m таких вектор-столбцов, один из которых — нулевой. Поэтому для построения проверочной матрицы нужно выписать, в качестве столбцов матрицы, все ненулевые двоичные вектор-столбцы длины m. Порядок столбцов безразличен. Чаще всего их упорядочивают так, чтобы содержимое каждого столбца являлось записью в двоичной системе счисления номера этого столбца.

Пример 2.1. Матрица

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

есть проверочная матрица $(7, 4)$-кода Хемминга, в которой содержимое каждого столбца является записью в двоичной системе счисления номера этого столбца.

Код Хемминга допускает *расширение*, позволяющее обнаруживать четное число ошибок. Проверочная матрица $\mathbf{H}_\text{р}$ расширенного кода Хемминга получается из матрицы $\mathbf{H}$ кода Хемминга следующим образом: к каждой строке этой матрицы приписывается нулевой символ, а к получившимся строкам сверху добавляется строка из единиц.

К кодовому вектору $\alpha_1, \alpha_2, \ldots, \alpha_n$ добавляется слева символ α_0, определяемый из равенства $\alpha_0 + \alpha_1 + \alpha_2 + \ldots + \alpha_n = 0$.

Определение 2.1. *Пусть* $\mathbf{u} = (u_1, u_2, \ldots, u_n)$ *— вектор из* n*-мерного векторного пространства* B^n *над полем* $GF(2)$. *Синдромом вектора* $\mathbf{u}$ *называется вектор* $\mathbf{s}(\mathbf{u}) = \mathbf{u} \cdot \mathbf{H}^T$, *где* $\mathbf{H}^T$ *— транспонированная матрица* $\mathbf{H}$.

Так как элементами проверочной матрицы $\mathbf{H}$ также, как и компонентами вектора $\mathbf{u}$, являются элементы поля $GF(2)$, то из определения синдрома вектора $\mathbf{u}$ следует, что его вычисление сводится к операциям сложения и умножения элементов поля $GF(2)$.

Из определения синдрома вектора $\mathbf{u}$ следует:

1. Синдром есть вектор длины m, где m — число строк проверочной матрицы.

2. Вектор u является кодовым тогда и только тогда, когда $\mathbf{s}(\mathbf{u}) = 0$.

Если синдром принятого вектора является нулевым вектором, то принятый вектор является кодовым, а ошибка, если она и произошла, не обнаружена. Естественно полагать, что в данном случае принятое слово не содержит ошибок и совпадает с посланным кодовым словом.

В случае, когда синдром принятого вектора не является нулевым вектором, принятое слово содержит ошибку. Если при этом код Хемминга является расширенным, то возможны два случая:

1) синдром принятого вектора совпадает с одним из столбцов расширенной проверочной матрицы кода Хемминга;

2) синдром принятого вектора не совпадает ни с одним из столбцов расширенной проверочной матрицы кода Хемминга.

В первом случае число ошибок является нечетным. Если предположить, что произошла одиночная ошибка, то ее позиция совпадает с позицией, которую в расширенной прове-

рочной матрице кода Хемминга занимает столбец, совпадающий с транспонированным синдромом принятого вектора.

Так как код Хемминга является линейным, то множество всех его кодовых векторов является линейным подпространством n-мерного векторного пространства B^n двоичных n-мерных векторов.

Код Хемминга может быть задан не только проверочной матрицей. Он может быть задан также матрицей, которая называется *порождающей.*

В самом деле, так как код Хемминга является линейным, то множество всех его кодовых векторов является линейным подпространством n-мерного векторного пространства B^n двоичных n-мерных векторов. Как и во всяком подпространстве, в этом подпространстве существует базис, то есть максимальная система линейно независимых векторов в этом подпространстве. Через эти базисные векторы линейно выражаются все кодовые векторы.

Пусть система векторов

$$\mathbf{g}_1 = (g_{11}, g_{12}, \ldots, g_{1n}), \mathbf{g}_2 = (g_{21}, g_{22}, \ldots, g_{2n}), \ldots$$
$$\ldots, \mathbf{g}_k = (g_{k1}, \quad g_{k2}, \ldots, g_{kn}) \quad (2.1)$$

есть базис в подпространстве, состоящем из всех кодовых векторов кода Хемминга.

Система (2.1) полностью определяет код Хемминга.

Матрица

$$\mathbf{G} = \begin{pmatrix} g_{11} & g_{12} & g_{1n} \\ g_{21} & g_{22} & g_{2n} \\ \ldots\ldots\ldots\ldots \\ g_{k1} & g_{k2} & g_{kn} \end{pmatrix},$$

составленная из компонентов базисных векторов кода Хемминга, называется *порождающей матрицей* этого кода. Так как код Хемминга — двоичный линейный код, то элементами порождающей матрицы являются элементы поля $GF(2)$.

Так как базис можно выбрать не единственным способом, то и порождающая матрица определена неоднозначно. Это замечание относится и к проверочной матрице.

Пусть $\mathrm{A} = \alpha_1\alpha_2\ldots\alpha_k$ — подлежащее кодированию слово в алфавите, состоящем из двух символов: 0 и 1. Тогда самое удобное — сопоставить слову A кодовый вектор $\mathbf{u}$, являющийся линейной комбинацией базовых векторов кода и получаемый по формуле

$$\mathbf{u} = \mathbf{A} \cdot \mathbf{G}, \quad (2.2)$$

где $\mathbf{A} = \begin{pmatrix} \alpha_1 & \alpha_2 & \ldots & \alpha_k \end{pmatrix}$ — однострочная вектор-матрица, элементами которой являются элементы поля $GF(2)$.

Так как элементами порождающей матрицы $\mathbf{H}$ также, как и компонентами вектора $\mathbf{A}$, являются элементы поля $GF(2)$, то из формулы (2.2) следует, что вычисление кодового вектора $\mathbf{u}$ сводится к операциям сложения и умножения элементов поля $GF(2)$.

Далее мы будем полагать, что в коде Хемминга каждому кодируемому слову сопоставляется кодовый вектор, определяемый по формуле (2.2).

Пример 2.2. Рассмотрим код Хемминга, порождающей матрицей которого является матрица

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

Этот код содержит $2^4 = 16$ кодовых слов, которыми можно закодировать все двоичные слова длины 4. Пусть $\mathrm{A} = 0101$ — кодируемое слово. Найдем кодовый вектор этого слова.

Применяя формулу (2.2), получаем:

$$\mathbf{u} = \mathbf{A} \cdot \mathbf{G} = \begin{pmatrix} 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} =$$

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

Пусть $\mathbf{G}$ есть порождающая матрица данного кода Хемминга. Допустим, что нам удалось исправить ошибки и восстановить переданное по каналу связи слово $U = u_1 u_2 \dots u_n$ этого кода. В этом случае мы можем, исходя из уравнения (2.2), найти то слово, которое в данном коде Хемминга было закодировано переданным кодовым словом. В самом деле, произведение матриц $\mathbf{A} \cdot \mathbf{G}$ есть однострочная матрица

$$\begin{pmatrix} \sum_{i=1}^{k} \alpha_i g_{i1} & \sum_{i=1}^{k} \alpha_i g_{i2} & \dots & \sum_{i=1}^{k} \alpha_i g_{in} \end{pmatrix},$$

равная однострочной вектор-матрице $\mathbf{u} = (u_1 \ u_2 \ \dots \ u_n)$. Приравнивая соотвествующие элементы этих двух однострочных матриц, получаем систему уравнений

$$\begin{cases} \sum_{i=1}^{k} \alpha_i g_{i1} = u_1; \\ \sum_{i=1}^{k} \alpha_i g_{i2} = u_2; \\ \dots\dots\dots\dots\dots \\ \sum_{i=1}^{k} \alpha_i g_{in} = u_n. \end{cases} \tag{2.3}$$

Так как слово $U = u_1 u_2 \dots u_n$ является кодовым, то существует такое слово $\mathrm{A} = \alpha_1 \alpha_2 \dots \alpha_k$, состоящее из k двоичных символов, которое в данном коде Хемминга кодируется словом U. Значит, соответствующая слову $\mathrm{A} = \alpha_1 \alpha_2 \dots \alpha_k$ вектор-матрица $\mathbf{A} = \begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_k \end{pmatrix}$ является решением матричного уравнения (2.2), а вектор $(\alpha_1, \alpha_2, \dots, \alpha_k)$ — решением эквивалентной уравнению (2.2) системы уравнений (2.3). Следовательно, система уравнений (2.3) является совместной. Так как система векторов (2.1) является системой линейно независимых векторов, то ранг матрицы $\mathbf{G}$ равен k. Отсюда и из теоремы Кронекера-Капелли следует, что решение системы уравнений (2.3) — единственное.

2. Лабораторное задание

Дана порождающая матрица $\mathbf{G}$ расширенного (16,11)-кода Хемминга.

1. Определить, содержит ли указанная в задании принятая последовательность ошибку?

2. Если принятая последовательность содержит ошибку, то определить, четным или нечетным является число ошибок.

3. Если число ошибок нечетное, то предположить, что принятая последовательность содержит одиночную ошибку. При этом предположении исправить одиночную ошибку в этой последовательности и найти закодированное ей слово.

Отчет должен быть напечатан шрифтом 12 или четко написан от руки чернилами. В рукописном варианте отчета высота символов 0, 1 и латинских букв должна быть равна 0,5 см. Каждый символ должен быть вписан в отдельную клетку высотой и шириной 0,5 см. Фамилия в заголовке должна быть написана печатными буквами.

Работа 3. Кольцо и поле многочленов. Примитивный элемент мультипликативной группы поля многочленов

Цель работы — закрепить у студентов основные понятия теории многочленов.

1. Общие сведения

Определение 3.1. Многочлен

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$$

с коэффициентами a_k, a_{k-1}, $\ldots$, a_1, a_0 из поля F называется *многочленом от переменной x над полем F*. Множество всех многочленов от переменной x над полем F обозначается $F(x)$. Число $\max\{i \mid a_i \neq 0\}$ называется *степенью* многочлена $f(x) = = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0$.

Степень многочлена $f(x)$ обозначается $\deg f(x)$.

Множество всех многочленов степени менее k обозначается $F^k(x)$.

Определение 3.2. Два многочлена

$$f(x) = a_k x^k + a_{k-1}x^{k-1} + \ldots + a_1 x + a_0 \tag{3.1}$$

и

$$g(x) = b_l x^l + b_{l-1}x^{l-1} + \ldots + b_1 x + b_0 \tag{3.2}$$

называются *равными*, если $k = l$ и $a_i = b_i$ при всех $i = 1, 2, \ldots, k$.

Естественно, что $x^0 = 1$. Число 0 называется *нулевым многочленом*. Степень нулевого многочлена не определена. Этот многочлен принадлежит как множеству $F(x)$, так и множеству $F^k(x)$ при любом $k > 0$.

Операции сложения и умножения многочленов

Во множестве многочленов $F(x)$ операция сложения двух многочленов $f(x)$ и $g(x)$, определенных формулами (3.1) и (3.2) соответственно, определяется формулой

$$f(x) + g(x) = \sum_{i=0}^{\max\{k,l\}} (a_i + b_i)x^i,$$

где $a_i + b_i$ есть результат определенной в поле F операции сложения элементов a_i и b_i этого поля. При этом мы полагаем, что при всех i, удовлетворяющих неравенствам $k < i \leq \max\{k, l\}$, $a_i = 0$. Точно также мы полагаем, что при всех i, удовлетворяющих неравенствам $l < i \leq \max\{k, l\}$, $b_i = 0$.

В частности, если $F = GF(p)$, то $a_i + b_i$ есть результат операции сложения элементов a_i и b_i поля $GF(p)$, то есть результат сложения по модулю p.

Операция умножения во множестве многочленов $F(x)$ двух многочленов $f(x)$ и (x), определенных формулами (3.1) и (3.2) соответственно, определяется формулой

$$f(x) \cdot g(x) = \sum_{m=0}^{k \cdot l} c_m x^m,$$

где коэффициент c_m при x^m определяется формулой

$$c_m = \sum_{i+j=m} a_i \cdot b_j,$$

а $a_i \cdot b_i$ есть результат определенной в поле F операции умножения элементов a_i и b_i этого поля.

В частности, если $F = GF(p)$, то $a_i \cdot b_i$ есть результат операции умножения элементов a_i и b_i поля $GF(p)$, то есть результат умножения по модулю p.

Из определения операции умножения двух многочленов над полем F вытекает, что *степень произведения двух многочленов равна сумме степеней этих многочленов.*

Свойства операций сложения и умножения многочленов над полем F

1. Для любого многочлена $f(x)$ над полем F имеет место равенство

$$f(x) + 0 = f(x),$$

где 0 — нулевой многочлен.

2. Сложение обладает свойством коммутативности, то есть для любых многочленов $f(x)$ и $g(x)$ над полем F имеет место равенство

$$f(x) + g(x) = g(x) + f(x).$$

3. Сложение обладает свойством ассоциативности, то есть для любых многочленов $f(x)$, $g(x)$ и $h(x)$ над полем F имеет место равенство

$$f(x) + g(x) + h(x) = f(x) + [g(x) + h(x)].$$

4. Для любого многочлена $f(x)$ над полем F, определяемого формулой (3.1), существует противоположный ему многочлен

$$-f(x) = -a_k x^k - a_{k-1} x^{k-1} - \ldots - a_1 x - a_0.$$

5. Для любого многочлена $f(x)$ над полем F имеет место равенство

$$f(x) \cdot 1 = f(x),$$

где 1 — единичный многочлен.

6. Умножение обладает свойством коммутативности, то есть для любых многочленов $f(x)$ и $g(x)$ над полем F имеет место равенство

$$f(x) \cdot g(x) = g(x) \cdot f(x).$$

7. Умножение обладает свойством ассоциативности, то есть для любых многочленов $f(x)$, $g(x)$ и $h(x)$ над полем F имеет место равенство

$$f(x) \cdot g(x) \cdot h(x) = f(x) \cdot [g(x) \cdot h(x)].$$

8. Сложение и умножение многочленов связаны законом дистрибутивности, то есть для любых многочленов $f(x)$, $g(x)$ и $h(x)$ над полем F имеет место равенство

$$[f(x) + g(x)] \cdot h(x) = f(x) \cdot h(x) + g(x) \cdot h(x).$$

9. Для любых многочленов $f(x)$ и $g(x)$ над полем F имеет место равенство

$$-[f(x) \cdot g(x)] = [-f(x)] \cdot g(x) = f(x) \cdot [-g(x)].$$

10. Если $f(x)$ и $g(x)$ — два ненулевых многочлена над полем F, то их произведение — ненулевой многочлен.

11. Для любого многочлена $f(x)$ над полем $F(x)$ имеет место равенство

$$f(x) \cdot 0 = 0.$$

Из свойств 1–8 вытекает, что множество многочленов $F(x)$ с введенными операциями сложения и умножения является коммутативным кольцом.

Свойства умножения многочленов над полем $GF(2)$

1. Если $f(x)$ — многочлен над полем $GF(2)$, то

$$[f(x)]^2 = f(x^2).$$

2. Если $f(x)$ и $g(x)$ — многочлены над полем $GF(2)$, то

$$-[f(x) \cdot g(x)] = f(x) \cdot g(x).$$

Для любых двух многочленов $f(x)$ и $g(x)$ существуют такие многочлены $a(x)$ и $r(x)$, что $f(x) = a(x) \cdot g(x) + r(x)$, причем $\deg g(x) > \deg r(x)$. В этом случае многочлен $f(x)$ можно представить как делимое, многочлен $g(x)$ — как делитель, многочлен $a(x)$ — как частное и многочлен $r(x)$ — как остаток от деления.

Если остаток от деления многочлена $f(x)$ на многочлен $g(z)$ равен нулю, то говорят, что *многочлен $g(z)$ делит многочлен $f(x)$*.

Определение 3.3. Многочлен $f(x)$ над полем F называется *неприводимым* в этом поле, если кольцо многочленов над полем F не содержит ни одного многочлена степени большей нуля, но меньшей чем степень многочлена $f(x)$, который делил бы многочлен $f(x)$. В противном случае многочлен $f(x)$ называется *приводимым* в поле F.

Пример 3.1. Пусть $f(x) = x^2 + x + 1$ есть многочлен над полем $GF(2)$. Определим, является ли этот многочлен неприводимым в этом поле. Степень многочлена $f(x)$ равна двум. Многочленами, степень которых больше нуля, но меньше двух, являются только многочлены первой степени. Всего имеется два многочлена первой степени над полем $GF(2)$. Это многочлены x и $x + 1$. При делении многочлена $f(x)$ на каждый из этих двух многочленов получается остаток, равный числу 1. Следовательно, многочлен $f(x)$ неприводим в поле $GF(2)$.

Элемент a из поля F называется *корнем многочлена* $f(x)$ над полем F, если $f(a) = 0$.

Многочлен $f(x)$ над полем F является приводимым в этом поле, если он имеет корень в этом поле. Если поле F является конечным, то, вычисляя значения этого многочлена при всех значениях переменной x из этого поля, можно определить в некоторых случаях, является ли данный многочлен приводимым.

Пример 3.2. Пусть $f(x) = x^2 + 1$ есть многочлен над полем $GF(2)$. Определим, является ли этот многочлен приводимым в этом поле. С этой целью исследуем, имеет ли многочлен $f(x) = x^2 + 1$ корень в поле $GF(2)$. Поле $GF(2)$ содержит два элемента: 0 и 1. Подставляя вместо переменной x ее значения 0 и 1, получаем:

$$f(0) = 0^2 + 1 = 1 \neq 0; \quad f(1) = 1^2 + 1 = 1 + 1 = 2(\bmod 2) = 0.$$

Следовательно, многочлен $f(x)$ является приводимым в поле $GF(2)$.

Определение 3.4. Многочлены $f(x)$ и $g(x)$ из кольца $F(x)$ называются *взаимно простыми*, если это кольцо не содержит ни одного многочлена, который делил бы оба многочлена $f(x)$ и $g(x)$ и имел бы степень, большую нуля и меньшую по сравнению с меньшей из степеней этих двух многочленов.

Рассмотрим множество $F^k(x)$ многочленов степени менее k над полем F. Из свойств 1–4 операции сложения многочленов следует, что множество многочленов $F^k(x)$ является коммутативной группой по сложению.

Чтобы это множество было кольцом, нужно ввести операцию умножения многочленов таким образом, чтобы произведение любых двух многочленов из множества $F^k(x)$ было многочленом степени менее k и при этом операция умножения обладала свойствами 5–8.

Пусть $P(x)$ — заданный многочлен степени k над полем F.

Определение 3.5. Произведением двух многочленов $f(x)$ и $g(x)$ из коммутативной группы $F^k(x)$ по модулю многочлена $P(x)$ — символически $f(x) \cdot g(x)(\bmod P(x))$ — называется остаток от деления многочлена $f(x) \cdot g(x)$ на многочлен $P(x)$.

Если остаток от деления многочлена $f(x) \cdot g(x)$ на многочлен $P(x)$ обозначить $r(x)$, то данное определение 3.5 символически можно записать так:

$$f(x) \cdot g(x)(\bmod P(x)) = r(x).$$

Умножение по модулю многочлена $P(x)$ (степени k), заданное в коммутативной группе по сложению $F^k(x)$ определением 3.5, обладает свойствами 6–8 (с.12). Единичным элементом при умножении по модулю многочлена $P(x)$ является многочлен $f_1(x) = 1$. Стало быть, это умножение (по модулю многочлена $P(x)$) обладает и свойством 5. Отсюда следует, что коммутативная группа по сложению $F^k(x)$, в которой определена операция умножения по модулю многочлена $P(x)$ (степени k), является кольцом, называемым кольцом вычетов по модулю многочлена $P(x)$.

Утверждение (без доказательства). Кольцо вычетов по модулю многочлена $P(x)$ является полем лишь тогда, когда $P(x)$ — неприводимый многочлен.

Если задан неприводимый многочлен $P(x)$ степени n над полем $GF(q)$, то кольцо вычетов по модулю этого многочлена является конечным полем (то есть полем Галуа) $GF(q^n)$, содержащим q^n элементов. Обозначим это поле $F^n(P(x))$. Неприводимый многочлен $P(x)$ называется *производящим многочленом* этого поля.

Пример 3.3. Пусть $P(x) = x^3 + x^2 + 1$. Этот многочлен неприводим над полем $GF(2)$, то есть он не делится на многочлены x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1. Кольцо вычетов по модулю многочлена $P(x)$ состоит из нулевого многочлена $f_0 = 0$ и всех многочленов над полем $GF(2)$ степени не более 2: 1, x, $x+1$, x^2, x^2+1, x^2+x, x^2+x+1. Пусть $f(x) = x^2+x+1$, $g(x) = x^2 + 1$. Найдем произведение этих многочленов по модулю многочлена $P(x)$.

$$c(x) = f(x) \cdot g(x) = (x^2 + x_1)(x^2 + 1) = x^4 + x^3 + x + 1.$$

Разделим теперь многочлен $c(x)$ на многочлен $P(x)$. Выполним это деление "столбиком".

$$\begin{array}{r|l} x^4+x^3+x+1 & x^3+x^2+1 \\ \underline{-\ x^4+x^3+x} & \\ 1 & x \end{array}$$

Итак, остаток от деления многочлена $c(x)$ на многочлен $P(x)$ есть многочлен $f_1(x) = 1$. Значит, $c(x)(\bmod P(x)) = 1$, то есть

$$f(x) \cdot g(x)(\bmod P(x)) = 1.$$

Следовательно, многочлен x^2+1 является обратным элементом для многочлена x^2+x+1 в поле $F^3(P(x))$.

Пусть $P(x)$ — неприводимый многочлен степени n над полем $GF(q)$. Так как кольцо вычетов по модулю многочлена $P(x)$ является конечным полем $GF(q^n)$, то множество всех ненулевых многочленов этого поля образует мультипликативную группу. Эта группа является циклической и содержит, по крайней мере, один примитивный элемент. Очевидно, что порядок этого примитивного элемента равен порядку данной мультипликативной группы, то есть $q^n - 1$.

Определение 3.6 Если $P(x)$ — неприводимый многочлен степени n над полем $GF(q)$, а мультипликативная группа поля $F^n(P(x))$ содержит хотя бы один примитивный элемент, являющийся корнем многочлена $P(x)$, то этот многочлен называется *примитивным*.

Не все неприводимые многочлены примитивны. Например, многочлен $P(x) = x^2+1$ над полем $GF(3)$ является неприводимым. Но он не является примитивным, так как среди его корней нет примитивных элементов мультипликативной группы поля $F^2(P(x))$ (его корнями являются многочлены x и $x = 1$).

Теорема 3.1 (без доказательства). Неприводимый многочлен степени m над полем $GF(q)$ является делителем многочлена $x^{q^m-1} - 1$.

Так как все примитивные многочлены неприводимы, то все они удовлетворяют утверждению теоремы 3.1.

Теорема 3.2 (без доказательства). Пусть $f(x) = x^n - 1$ и $g(x) = x^m - 1$ суть два многочлена над полем $GF(q)$. Если m — делитель числа n, то многочлен $g(x)$ — делитель многочлена $f(x)$. И наоборот, если многочлен $g(x)$ — делитель многочлена $f(x)$, то число m — делитель числа n.

2. Лабораторное задание

Дан многочлен $P(x)$ над данным полем $GF(q)$.

1. Проверить, будет ли кольцо вычетов многочленов по модулю многочлена $P(x)$ полем? Обосновать теоретически и с помощью вычислений сделанный вывод.

2. Если это кольцо является полем, то:

А. Проверить, является ли указанный в задании его элемент примитивным элементом этого поля? Обосновать теоретически и с помощью вычислений сделанный вывод.

Б. Проверить, является ли многочлен $P(x)$ примитивным?

Текст отчета должен быть напечатан или разборчиво написан от руки чернилами. Если отчет написан от руки, то в формулах высота основных символов должна быть равна 0,5 см. Каждый основной символ должен быть вписан в отдельную клетку высотой и шириной 0,5 см. Высота символов в показателе степени должна быть равна 0,25 см. Фамилия в заголовке должна быть написана печатными буквами.

Работа 4. Циклические коды

Определение 4.1. Пусть $\mathbf{a} = (a_0, a_1, \ldots, a_{n-1})$ — вектор с координатами из поля F. *Циклическим сдвигом* вектора $\mathbf{a}$ называется вектор

$$\mathbf{a}' = (a_{n-1}, a_0, a_1, \ldots, a_{n-2}).$$

Определение 4.2 *Циклическим кодом* называется линейный код, который вместе с любым своим кодовым вектором содержит также и его циклический сдвиг.

Далее рассматриваются лишь двоичные циклические коды.

Обозначим через $\mathbf{G}^n$ множество всех многочленов вида

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$$

с коэффициентами a_{n-1}, a_{n-2} $\ldots$, a_1, a_0 из поля $GF(2)$.

Определение 4.3. Два многочлена

$$f(x) = a_{n-1}x^{n-1} + a_{k-n}x^{n-2} + \ldots + a_1x + a_0 \tag{4.1}$$

и

$$g(x) = b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \ldots + b_1x + b_0 \tag{4.2}$$

из множества $\mathbf{G}^n$ называются *равными*, если $a_i = b_i$ при всех $i = 0, 1, \ldots \ldots, n-1$.

Принадлежащий множеству $\mathbf{G}^n$ многочлен, все коэффициенты которого являются нулями, называется *нулевым многочленом* и обозначается $\mathbf{0}$.

Операции сложения и умножения многочленов

Во множестве многочленов $\mathbf{G}^n$ операция сложения двух многочленов $f(x)$ и $g(x)$, определенных формулами (4.1) и (4.2) соответственно, определяется формулой

$$f(x) + g(x) = \sum_{i=0}^{n-1}(a_i + b_i)x^i,$$

где $a_i + b_i$ есть результат определенной в поле $GF(2)$ операции сложения элементов a_i и b_i этого поля, то есть результат сложения по модулю 2.

Свойства операции сложения многочленов из множества $\mathbf{G}^n$

1. Для любого многочлена $f(x)$ из множества $\mathbf{G}^n$ имеет место равенство $f(x)+\mathbf{0} = f(x)$.

2. Сложение обладает свойством коммутативности, то есть для любых многочленов $f(x)$ и $g(x)$ из множества $\mathbf{G}^n$ имеет место равенство

$$f(x) + g(x) = g(x) + f(x).$$

3. Сложение обладает свойством ассоциативности, то есть для любых многочленов $f(x)$, $g(x)$ и $h(x)$ из множества $\mathbf{G}^n$ имеет место равенство

$$f(x) + g(x) + h(x) = f(x) + [g(x) + h(x)].$$

4. Для любого многочлена $f(x)$ из множества $\mathbf{G}^n$, определяемого формулой (4.1), существует противоположный ему многочлен

$$-f(x) = a_{n-1}x^{n-1} + a_{k-2}x^{k-2} + \ldots + a_1x + a_0.$$

Так как операция сложения, введенная на множестве многочленов $\mathbf{G}^n$ обладает свойствами 1–4, то это множество является коммутативной группой.

Пусть $G(x)$ — многочлен из группы $\mathbf{G}^n$. Рассмотрим подмножество множества $\mathbf{G}^n$, состоящее из всех многочленов группы $\mathbf{G}^n$, делящихся без остатка на многочлен $G(x)$. Тот факт, что многочлен $f(x)$ делится без остатка на многочлен $G(x)$, будем обозначать так: $G(x) \mid f(x)$.

Если $G(x) \mid f(x)$ и $G(x) \mid g(x)$, то $G(x) \mid (f(x) + g(x))$. Таким образом, подмножество множества $\mathbf{G}^n$, состоящее из всех многочленов множества $\mathbf{G}^n$, делящихся без остатка на многочлен $G(x)$, является подгруппой группы $\mathbf{G}^n$.

Определение 4.4. Множество, состоящее из всех двоичных слов вида $a_0a_1 \ldots a_{n-2}a_{n-1}$ и таких, что многочлен

$$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$$

делится без остатка на многочлен $G(x)$, называется *кодом с порождающим многочленом* $G(x)$. Многочлен $a(x)$ называется *кодовым*.

Таким образом, множество всех кодовых многочленов кода с порождающим многочленом $G(x)$ является подгруппой группы многочленов $\mathbf{G}^n$.

Векторное пространство, состоящее из всех n-мерных векторов с компонентами из поля $GF(2)$, обозначим $GF^n(2)$. Каждый кодовый вектор кода с порождающим многочленом $G(x)$ является вектором из этого пространства.

Если $f(x)$ и $g(x)$, определяемые формулами (4.1) и (4.2) соответственно, суть два кодовых многочлена кода с порождающим многочленом $G(x)$, то слова

$$a_0a_1 \ldots a_{n-2}a_{n-1} \quad \text{и} \quad b_0b_1 \ldots b_{n-2}b_{n-1}$$

будут кодовыми словами, а векторы

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \quad \text{и} \quad (b_0, b_1, \ldots, b_{n-2}, b_{n-1})$$

— кодовыми векторами этого кода.

Так как сумма многочленов $f(x)$ и $g(x)$ также является кодовым многочленом данного кода, то и их сумма тоже будет кодовым многочленом этого кода. Значит, слово

$$(a_0 + b_0)(a_1 + b_1) \ldots (a_{n-2} + b_{n-2})(a_{n-1}b_{n-1})$$

будет кодовым словом кода с порождающим многочленом $G(x)$, а сумма векторов

$$(a_0, a_1, \ldots, a_{n-2}, a_{n-1}) \quad \text{и} \quad (b_0b_1 \ldots b_{n-2}b_{n-1})$$

из векторного пространства $GF^n(2)$ является кодовым вектором этого кода. Отсюда следует, что множество кодовых векторов такого кода является подпространством векторного пространства $GF^n(2)$, а код с порождающим многочленом $G(x)$ — линейным.

Теорема. Для того, чтобы код с порождающим многочленом $G(x)$ был циклическим, необходимо и достаточно, чтобы порождающий многочлен $G(x)$ был делителем многочлена $x^n - 1$, где n — длина кода.

Доказательство. Выше было установлено, что код с порождающим многочленом $G(x)$ — линейный.

Докажем сначала достаточность. Предположим, что порождающий многочлен $G(x)$ кода является делителем многочлена x^n-1. Докажем, что код, порождаемый многочленом $G(x)$ — циклический.

Пусть $a(x) = a_{n-1}x^{n-1}+a_{n-2}x^{n-2}+\ldots+a_1x+a_0$ — многочлен, соответствующий кодовому слову $a_0, a_1, \ldots, a_{n-2}, a_{n-1}$. Через

$$b(x) = a_{n-2}x^{n-1} + a_{n-3}x^{n-2} + \ldots + a_0x + a_{n-1}$$

обозначим многочлен, соответствующий сдвигу кодового слова

$$a_0, a_1, \ldots, a_{n-2}, a_{n-1}$$

вправо. Многочлен $b(x)$ можно записать иначе:

$$b(x) = a(x)\dot{x} - a_{n-1}(x^n - 1)(\bmod (x^n - 1)). \tag{4.3}$$

Так как $a_0, a_1, \ldots, a_{n-2}, a_{n-1}$ — кодовое слово, то имеет место соотношение $G(x) \mid a(x)$. Если при этом $G(x) \mid (x^n - 1)$, то из представления многочлена $b(x)$ следует соотношение $G(x) \mid b(x)$. Стало быть, код, порождаемый многочленом $G(x)$ — циклический.

Докажем теперь необходимость. Допустим, что код, порождаемый многочленом $G(x)$ — циклический. Докажем, что многочлен $G(x)$ является делителем многочлена $x^n - 1$. Пусть

$$a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \ldots + a_1x + a_0$$

— кодовый многочлен, соответствующий кодовому слову

$$a_0, a_1, \ldots, a_{n-2}, a_{n-1}\,.$$

Тогда этот многочлен делится без остатка на многочлен $G(x)$. Так как код, порождаемый многочленом $G(x)$ — циклический, то сдвиг вправо этого кодового слова тоже является кодовым словом. Значит, соответствующий этому сдвигу многочлен

$$b(x) = a_{n-2}x^{n-1} + a_{n-3}x^{n-2} + \ldots + a_0x + a_{n-1}$$

делится без остатка на многочлен $G(x)$. Из определения многочленов $a(x)$ и $b(x)$ следует уравнение

$$x \cdot a(x) - b(x) = a_{n-1}(x^n - 1). \tag{4.4}$$

Так как имеют место соотношения $G(x) \mid a(x)$ и $G(x) \mid b(x)$, то левая часть уравнения (4.4) делится без остатка на многочлен $G(x)$. Поэтому и правая часть этого уравнения тоже делится без остатка на многочлен $G(x)$. Значит, и многочлен $x^n - 1$ делится без остатка на многочлен $G(x)$. Теорема доказана.

Из представления (4.3) многочлена $b(x)$ следует, что циклический сдвиг кодового слова вправо эквивалентен умножению кодового многочлена $a(x)$ на x (по модулю многочлена x^n-1). Если циклический сдвиг кодового слова i-кратный, то он эквивалентен умножению кодового многочлена $a(x)$ на x^i (по модулю многочлена $x^n - 1$). Соответственно циклический сдвиг влево на i разрядов эквивалентен умножению кодового многочлена $a(x)$ на x^{-i} (по модулю многочлена $x^n - 1$).

Если многочлен $G(x)$ имеет степень k и является делителем многочлена x^n-1, то можно построить циклический код с длиной n, удовлетворяющий условиям:

1) многочлен $G(x)$ является порождающим многочленом этого кода;

2) в каждом кодовом слове число информационных символов равно числу $m = n - k$.

Циклические коды длины n существуют при любом $n \geq 2$, так как при любом $n \geq 2$ многочлен $x^n - 1$ разлагается на множители:

$$x^n - 1 = (x - 1)(x^{n-1} + x^{n-2} + \ldots + x + 1)$$

— и оба сомножителя могут быть порождающими многочленами циклического кода.

Число циклических кодов длины n равно числу многочленов, являющихся делителями многочлена $x^n - 1$. Любой неприводимый делитель многочлена $x^n - 1$, а также их произведения могут быть порождающими многочленами циклического кода длины n.

Пример 4.1. Перечислим все порождающие многочлены циклического кода длины $n = 7$. Неприводимыми делителями многочлена x^7-1 являются все многочлены, входящие в разложение

$$x^7 - 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$$

многочлена $x^7 - 1$ на неприводимые множители.

Все возможные порождающие многочлены циклического кода длины $n = 7$ и параметры соответствующих им циклических кодов сведены в следующую таблицу.

Таблица

Порождающий многочлен	n	m
$x + 1$	7	6
$x^3 + x^2 + 1$	7	4
$x^3 + x + 1$	7	4
$(x + 1)(x^3 + x^2 + 1) = x^4 + x^2 + x + 1$	7	3
$(x + 1)(x^3 + x + 1) = x^4 + x^3 + x^2 + 1$	7	3
$(x^3 + x^2 + 1(x^3 + x + 1) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$	7	1

Если $G(x)$ — порождающий многочлен циклического кода, то каждый кодовый многочлен $F(x)$ делится на многочлен $G(x)$.

Пусть многочлен $G(x)$ является порождающим многочленом циклического кода длины n. Тогда многочлен $(x^n - 1)$ делится на многочлен $G(x)$. Значит, отношение $(x^n - 1)/G(x)$ есть многочлен

$$(x^n - 1)/G(x) = h_m x^m + h_{m-1} x^{m-1} + \ldots + h_1 x + h_0 = H(x). \qquad (4.7)$$

Определенный таким образом многочлен $H(x)$ называется *проверочным многочленом* циклического (n, m)-кода.

При данной длине n циклического кода многочлены $G(x)$ и $H(x)$ находятся во взаимно однозначном соответствии. Поэтому циклический код данной длины n может быть задан и порождающим многочленом, и проверочным многочленом.

Пример 4.2. Пусть $n = 7$, $G(x) = x^3+x^2+1$. По формуле (4.7) определим проверочный многочлен данного циклического кода

$$H(x) = (x^7 + 1)/(x^3 + x^2 + 1) = x^4 + x^3 + x + 1.$$

Пусть C есть циклический код. Проверочный многочлен циклического кода C является порождающим многочленом другого циклического кода, который мы обозначим $C1$. При этом порождающий многочлен кода C является проверочным многочленом кода $C1$. Коды C и $C1$ называются *дуальными (двойственными)*. Они имеют одинаковую длину n.

Число m информационных символов циклического (n, m)-кода равно степени проверочного многочлена, а число проверочных символов $k = n - m$ равно степени порождающего многочлена.

Простым способом кодирования в циклическом (n, m)-коде является следующий способ. Пусть $a_0a_1 \dots a_{m-1}$ есть подлежащее кодированию сообщение. Этому сообщению взаимно однозначно соответствует информационный многочлен $a(x) = a_0 + +a_1x + \dots + a_{m-1}x^{m-1}$. Тогда в качестве кодового многочлена этого кода принимают многочлен

$$F(x) = a(x) \cdot G(x). \tag{4.5}$$

Пример 4.3. Пусть $G(x) = x^3 + x^2 + 1$ — порождающий многочлен циклического $(7, 4)$-кода. Закодируем слово 1010. Информационным многочленом этого слова является многочлен $a(x) = 1 + x^2$. По формуле (4.5) кодовым многочленом, соответствующим слову 1010, является многочлен $F(x) = (1 + x^2)(1 + x^2 + x^3) = 1 + x^3 + x^4 + x^5$. Кодовым словом, соответствующим кодовому многочлену $F(x)$, является слово $F = 1001110$. Этим словом и кодируется в данном циклическом коде слово 1010.

Если $G(x) = g_kx^k + g_{k-1}x^{k-1} + \dots + g_1x + g_0$ — порождающий многочлен циклического кода, то порождающая матрица этого кода имеет вид

$$\mathbf{G} = \begin{pmatrix} g_0 & g_1 & \dots\dots & g_k & 0 & \dots\dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{k-1} & g_k & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & \dots & 0 & g_0 & g_1 & \dots\dots & g_k \end{pmatrix}. \tag{4.6}$$

В этой матрице элементами первой строки являются коэффициенты многочлена $G(x)$, элементами второй строки являются коэффициенты многочлена $x \cdot G(x)$ и т.д. То есть элементами i-ой строки являются коэффициенты многочлена $x^{i-1} \cdot G(x)$, где $0 < i \leq m-1$.

Очевидно, что сумме строк с номерами l_1, l_2, …, l_p взаимно однозначно соответствует сумма многочленов x^{l_1}, x^{l_2}, …, x^{l_p}. Так как эта сумма многочленов не является нулевым многочленом, то любая сумма строк матрицы G не равна строке, составленной из нулей. Отсюда следует, что строки матрицы G линейно независимы. Значит, матрица G является порождающей матрицей данного кода.

Проверочная матрица циклического кода (n, m)-кода получается из проверочного многочлена $H(x) = h_0 + h_1x + \dots h_mx^m$. Эта матрица имеет вид

$$\mathbf{H} = \begin{pmatrix} 0 & \dots\dots & 0 & h_m & \dots & h_1 & h_0 \\ 0 & \dots & 0 & h_m & h_{m-1} & \dots & h_0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ h_m & h_{m-1} & \dots & h_1 & h_0 & 0 & \dots & 0 \end{pmatrix}. \tag{4.7}$$

Первая строка этой матрицы составлена из коэффициентов многочлена $H(x)$, расположенных в порядке убывания их индексов, то есть в порядке убывания степеней переменной. Последующие строки составлены из коэффициентов многочленов $xH(x)$, $x^2H(x)$, …, $x^{k-1}H(x)$, расположенных в порядке убывания степеней переменной.

Пример 4.4. Найдем порождающую и проверочную матрицы циклического $(7, 4)$-кода с порождающим многочленом $G(x) = 1 + x^2 + x^3$. Сначала найдем по формуле (4.6) порождающую матрицу

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

Найдем теперь проверочный многочлен

$$H(x) = (x^7 - 1)/G(x) = (x^7 - 1)/(x^3 + x^2 + 1) = x^4 + x^3 + x^2 + 1.$$

Отсюда найдем по формуле (4.7) проверочную матрицу

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

Легко проверить, что $\mathbf{G} \cdot \mathbf{H} = \mathbf{0}$.

По порождающей матрице $\mathbf{G}$ легко найти кодовое расстояние d. Так, в предыдущем примере кодовое расстояние $d = 3$.

Циклический код, получающийся умножением информационного многочлена $a(x)$ на порождающий многочлен $G(x)$, является обычно несистематическим.

Чтобы реализовать систематический циклический код длины n с m информационными символами, порождаемый многочленом $G(x)$ надо:

1. Умножить информационный многочлен $a(x)$ на x^{n-m}.

2. Разделить полученное в п.1 произведение на порождающий многочлен $G(x)$.

3. Сложить полученное в п.1 произведение $a(x) \cdot x^{n-m}$ и остаток от деления, произведенного в п.2.

Таким образом, указанная процедура кодирования представляется формулой

$$F(x) = a(x) \cdot x^{n-m} + r(x),$$

где $r(x) = [a(x) \cdot x^{n-m}/G(x)](\mathrm{mod}\ G(x))$. Кодовый многочлен $F(x)$ делится без остатка на порождающий многочлен $G(x)$ и, следовательно, принадлежит данному коду. Каждый из членов многочлена $a(x) \cdot x^{n-m}$ имеет степень не менее $n - m$, тогда как степень остатка $r(x)$ не превышает числа $n - m - 1$. Поэтому при $i = 0, 1, \ldots, m - 1$ коэффициент f_{i+n-m} кодового многочлена $F(x) = f_{n-1}x^{n-1} + f_{n-2}x^{n-2} + \ldots + f_1x + f_0$ совпадает с соответствующим коэффициентом a_i информационного многочлена $a(x)$. Значит, при такой системе кодирования получается систематический циклический код.

Пример 4.5. Пусть $G(x) = 1+x^2+x^3$ есть порождающий многочлен систематического циклического кода длины $n = 7$. Закодируем с помощью описанной процедуры слово 1101. Этому информационному слову соответствует информационный многочлен $a(x) = 1 + x + x^3$. В данном случае число информационных символов $m = 4$. Отсюда следует: $n-m = 7-4 = 3$ и $a(x)\cdot x^{n-m} = (1+x+x^3)\cdot x^3 = x^3+x^4+x^6$. Поэтому в результате деления произведения $a(x) \cdot x^{n-m}$ на порождающий многочлен $G(x)$ получается остаток $r(x) = x^2$. Складывая этот остаток и произведение $a(x) \cdot x^{n-m}$, получаем кодовый многочлен $F(x) = x^2 + x^3 + x^4 + x^6$. Этому кодовому многочлену соответствует кодовое слово 0011101. В этом слове последние четыре символа, если их считать в порядке слева направо, образуют подслово 1101, являющееся информационным словом. Таким образом, информационное слово, действительно, не искажается при кодировании.

Этот пример подтверждает, что реализованная в нем система кодирования реализует систематический циклический код.

2. Лабораторное задание

1. Построить все многочлены, порождающие циклические коды заданной длины. Для каждого порождающего многочлена указать число информационных и проверочных символов в порожденном им коде и найти проверочный многочлен этого кода.

2. Построить порождающую и проверочную матрицы для циклического кода заданной длины, содержащего указанное число k проверочных символов.

Текст отчета должен быть напечатан или разборчиво написан от руки чернилами. Если отчет написан от руки, то в формулах высота основных символов должна быть равна 0,5 см. Каждый основной символ должен быть вписан в отдельную клетку высотой и шириной 0,5 см. Высота символов в показателе степени должна быть равна 0,25 см. Фамилия в заголовке должна быть написана печатными буквами.