

Министерство образования и науки Российской Федерации
Федеральное агентство по образованию
Ярославский государственный университет им. П.Г. Демидова
Кафедра компьютерных сетей

Теория кодирования

Методические указания

Рекомендовано
Научно-методическим советом университета
для студентов, обучающихся по специальности
Прикладная математика и информатика

Ярославль 2006

УДК 007
ББК 181я73
К 78

*Рекомендовано
Редакционно-издательским советом университета
в качестве учебного издания. План 2006 года*

Рецензент
кафедра компьютерных сетей Ярославского государственного
университета им. П.Г. Демидова

Составитель: М.В. Краснов

Теория кодирования : метод. указания / сост.
К 78 М.В. Краснов; Яросл. гос. ун-т. – Ярославль : ЯрГУ, 2006. –
48 с.

Основное использование вычислительной техники связано с хранением и передачей информации. При хранении информации возникает задача экономного метода записи. При передаче информации возникает задача ее защиты от случайных помех. Описанию некоторых математических понятий и приемов, используемых при решении этих задач, и посвящена данная работа.

Предназначено для студентов, обучающихся по специальности 010501 Прикладная математика и информатика (дисциплина «Теория информации и кодирование», блок ДС), очной формы обучения.

УДК 007
ББК 181я73

© Ярославский государственный университет, 2006
© М.В. Краснов, 2006

Под кодированием в широком смысле понимается переход от одного способа задания информации к другому, допускающий восстановление исходной информации. Для уточнения термина «кодирование», используемого в работе, остановимся на двух случаях, которые рассматриваются далее: это передача данных по каналу связи с помехами и передача информации по каналу без помех. В первом случае будем говорить о кодах, исправляющих ошибки, а во втором – о методах сжатия информации.

1. Коды, исправляющие ошибки

В этом разделе рассматриваются способы исправления ошибок (помех) при передаче информации. Наиболее действенный способ борьбы с помехами – введение избыточности, то есть, кроме информационных символов, сообщение должно содержать некоторое число контрольных символов, служащих для обнаружения и исправления ошибок.

1.1. Основные определения

Пусть имеется сообщение $i = \{u_0, \dots, u_{k-1}\}$, состоящее из символов алфавита $A = \{0, \dots, q-1\}$, которое должно быть передано по каналу связи. Из-за существования помех передача сообщения в чистом виде исключается. Поэтому сообщение i кодируется другой последовательностью $c = \{c_0, \dots, c_{n-1}\}$, состоящей из символов того же алфавита $A = \{0, \dots, q-1\}$, по которой можно восстановить i . Последовательность c называется в этом случае кодовым словом, а i – информационным словом.

Определение 1.1 Блочным кодом ξ над алфавитом из q символов называется множество q -ичных последовательностей длины n . Мощность кода M – число этих последовательностей.

Определение 1.2. Блочный код ξ мощности q^k называется (n, k) -кодом.

При кодировании произвольной q -ичной последовательности (n, k) -кодом она разбивается на части из k -символов, и каждая часть кодируется элементом кода ξ .

О блоковом коде судят по трем параметрам: длине блока n , информационной длине k и минимальному расстоянию d^* . Минимальное расстояние вводится двумя следующими определениями.

Определение 1.3. Расстоянием по Хэммингу между двумя q -ичными последовательностями x и y длины n называется число позиций, в которых они различны. Это расстояние обозначается через $d(x, y)$.

Определение 1.4. Пусть $\xi = \{c_i, i = 0, \dots, M-1\}$ – код. Тогда минимальное расстояние кода ξ равно наименьшему из всех расстояний по Хэммингу между различными парами кодовых слов, то есть $d^* = \min_{c_i, c_j \in \xi, i \neq j} d(c_i, c_j)$.

Если $d^* \geq 2t+1$, то код может исправлять t ошибок. Исправление ошибок в этом случае заключается в замене принятого слова на ближайшее кодовое слово.

1.2. Некоторые сведения из алгебры

Определение 1.5. Бинарной операцией на множестве M называется произвольная функция $f: M \times M \rightarrow M$.

Определение 1.6. Множество G с бинарной операцией $*$ называется группой, если выполнены следующие аксиомы:

- ассоциативность. $(a * b) * c = a * (b * c)$ для любых $a, b, c \in G$;
- существует единичный элемент $e \in G$ такой, что $a * e = e * a = a$ для любого $a \in G$;
- для любого $a \in G$ существует обратный элемент $b \in G$, такой, что $a * b = b * a = e$.

Группа G называется абелевой группой, если $a * b = b * a$ для любых $a, b \in G$.

Группа G называется циклической (с образующим элементом a), если существует такой элемент $a \in G$, что любой элемент $b \in G$ является некоторой степенью a .

Определение 1.7. Кольцом R называется множество с двумя определенными на нем бинарными операциями; первая называется сложением (обозначается $+$), вторая называется умножением (обозначается $*$), причем имеют место следующие аксиомы:

- относительно сложения (+) R является абелевой группой (0 – единичный элемент);
- замкнутость: произведение $a * b$ принадлежит R для любых $a, b \in R$;
- $(a * b) * c = a * (b * c)$ для любых $a, b, c \in R$;
- существует элемент $1 \in R$ такой, что $a * 1 = 1 * a = a$ для любого элемента $a \in R$;
- $(a + b) * c = (a * c) + (b * c)$ для любых $a, b, c \in R$.

Определение 1.8. Полем называется множество с двумя определенными на нем операциями – сложением и умножением, причем имеют место следующие аксиомы:

- множество образует абелеву группу по сложению (0 – единичный элемент);
- поле замкнуто относительно умножения, и множество элементов ($\neq 0$) образует абелеву группу по умножению (1 – единичный элемент);
- закон дистрибутивности: $(a + b) * c = (a * c) + (b * c)$ для любых a, b, c из поля.

Определение 1.9. Пусть F – некоторое поле. Подмножество $S \subset F$ называется подполем, если оно само является полем относительно операций поля F . В этом случае поле F называется расширением поля S .

Определение 1.10. Множество V называется векторным пространством над полем F если

1) для пар элементов из V (векторов) определена операция векторного сложения;

2) для элемента из V и скаляра (элемент поля F) определена операция умножения на скаляр,

то результат выполнения операций дает элемент из V и выполняются следующие аксиомы:

- V является абелевой группой относительно векторного сложения;
- где $\forall a \in F$ и $\forall v_1, v_2 \in V$;
- $(a + b)v = av + bv$, где $\forall a, b \in F$ и $\forall v \in V$;
- $(ab)v = a(bv)$, где $\forall a, b \in F$ и $\forall v \in V$;
- $1v = v$, где $\forall v \in V$.