Прикладная алгебра и теория чисел

Оглавление

Глава 1

Вводная информация

Эта глава содержит определения, утверждения и теоремы о группах, кольцах и полях. Эта информация понадобится для понимания дальнейшего материала.

1.1 Группы

Определение 1 (Группа). *Группой* $\mathfrak{G}$ *называется четверка* $(G, *^{(2)}, e^{(0)}, -1^{(1)})$, *где*

$$\begin{cases} x * (y * z) = (x * y) * z, \\ x * e = x, \\ x * x^{-1} = e \end{cases}$$

Определение 2 (Абелева группа). *Абелевой группой называется группа, в которой* $*$ *коммутативна* ($x * y = y * x$).

Определение 3 (Порядок). *Порядок группы*, $\mathrm{ord}\ \mathfrak{G}$ *— количество элементов.*

Определение 4 (Циклическая группа).
$G = \{e, x^1, x^2, x^3, \ldots, x^{-1}, x^{-2}, x^{-3}, \ldots\}$

Определение 5 (Подгруппа). $\mathfrak{G}$ *- группа* $(G, *, e, -1)$. *И множество* $H \subseteq G$. *Тогда* $\mathfrak{H}$ *называется подгруппой, если замкнута относительно операций* $*, e, -1$.

Продолжение следует...

1.2 Поля и кольца

Будет написано...

Глава 2

Помехоустойчивое кодирование

2.1 Метрика Хэмминга

Рисунок

Определение 6 (Метрика Хэмминга)**.** *Σ - алфавит, n - длина слова. Слова u, $v \in \Sigma^n$. Тогда метрика Хэмминга, $\rho(u,v)$ — количество позиций в словах u, v, в которых они различаются.*

Теорема 1. *ρ — метрика.*

Доказательство. Проверим все свойства метрик:

- $\rho(u,v) = 0 \Leftrightarrow u = v$
- $\rho(u,v) = \rho(v,u)$
- $\rho(u,v) \geq 0$
- $\rho(u,v) + \rho(v,w) = \rho(u,w)$

Отрезки $\square$

$$\Sigma^m \xrightarrow{f} \Sigma^n \rightsquigarrow \Sigma^n \xrightarrow{g} \Sigma^m$$

c — кодовое слово

c' — слово с ошибками

Окружности

Теорема 2. *Код обнаруживает n ошибок* $\Leftrightarrow \rho(c_1, c_2) > n$ *для любых кодовых слов* c_1, c_2.

Доказательство. ($\Rightarrow$) Допустим $\rho(c_1, c_2) \leq n$. c_1 и c_2 отличаются не более чем в n позициях. Можно в c_1 сделать n ошибок и получить c_2.

($\Leftarrow$) $\rho(c_1, c_2) > n$. Слово c' содержит не больше n ошибок, c — исходное слово. Следовательно, если $c \neq c'$ — ошибки были. □

Определение 7 (Наименьшее расстояние)**.** *Наименьшее расстояние между кодовыми словами (м и н и м а л ь н о е р а а с т о я н и е к о д а) — число измененных символов, необходимое для перехода одного кодового слова в другое.*

Минимальное расстояние кода является главной характеристикой кода.

Теорема 3. *Код может исправить* $\leq n$ *ошибок* $\Leftrightarrow$ *минимальное расстояние этого кода* $> 2n$.

Доказательство. ($\Rightarrow$) Допустим, минимальное расстояние $\leq 2n$.

$$\rho(c_1, c_2) \leq 2n$$

Существует c': $\rho(c', c_1) \leq n$ и $\rho(c', c_2) \leq n$.
c' — принятое сообщение. Исправление невозможно.

($\Leftarrow$) $\rho(c_1, c_2) > 2n$.

c' — слово с не более чем n ошибками. Существует единственное кодовое слово c, для которого $\rho(c, c') \leq n$. Следовательно, c — единствено возможный результат декодирования. □

2.2 Примеры кодов

2.2.1 С проверкой на четность

Алфавит $\Sigma = \{0, 1\}$, m — длина слов. Тогда f — кодирующая функция:

$$f(u) = u\Big(\sum_{i=1}^{m} u\Big),$$

где $u \in \Sigma^m$.

Минимальное расстояние этого кода $= 2$. Следовательно, он может обнаружить 1 ошибку, но ни одной не может исправить.

2.2.2 Дублирующий код

Кодирующая функция f:

$$f(u) = \underbrace{uu\dots u}_{\text{k раз}},$$

где $u \in \Sigma^m$, $k \in \omega$.

Минимальное расстояние дублируещего кода равен количеству повторений (k). Следовательно, он может обнаружить $k-1$ ошибку, а исправить $\left[\frac{k-1}{2}\right]$. Основным минусом этого кода является то, что он порождает слишком длинные кодовые слова.

2.3 Код Хэмминга

$r \in \mathbb{Z}^+$. Числа $\neq 0$ с двоичной записью длины $\leq r$.

Матрица $r \times (2^r - 1)$. Пусть $r = 3$, получается матрица 3×8:

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

u — исходное слово, $|u| = 2^r - 1 - r$. v — проверочная часть, $|v| = r$. Тогда кодовое слово - uv. Получаем $(2^r - 1 - r, 2^r - 1)$-код.

v_i: i-й столбец, просуммировать u отмеченные 1.

$$v_i = \sum_u u_j \times a_{ij}$$

Минимальное расстояние: 3. Добавить пояснение

Пример

2.4 Оптимальность

$d > 2$

Рисунок

(m, n)-код. $2^m(1+n) \le 2^n$

Определение 8 (Совершенный код)**.** *С о в е р ш е н н ы й к о д — «шары» полностью закрывают пространство:* $2^m(1+n) = 2^n$.

Для кода Хэмминга: $2^{2^r-1-r}(1+2^r-1) = 2^{2^r-1}$.

2.5 Групповые и линейные коды

Определение 9. *К о д г р у п п о в о й, если множество кодовых слов — аддитивная группа. К о д л и н е й н ы й, если множество кодовых слов — подпространство.*