Прикладная алгебра и теория чисел

Оглавление

1 Вводная информация **3**

1.1 Группы 3

1.2 Поля и кольца 4

2 Помехоустойчивое кодирование **5**

2.1 Метрика Хэмминга 5

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,* $ord\ \mathfrak{G}$ — *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 □

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

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. □