Лекции по дискретной математике.

Лектор: Угольников Александр Борисович.

Москва, 2003. (от 30 декабря)

Часть I

Комбинаторика.

Лекция 1.

Элементарные понятия.

Пусть даны элементы $x_1, x_2, \ldots, x_n$.

Определение. Набор элементов $x_{i_1}, x_{i_2}, \ldots, x_{i_k}, k \leqslant n$ называется *k-выборкой.*

Выборки бывают:

1. *упорядоченные*
2. *неупорядоченные*

Определение. Упорядоченная k-выборка называется *k-перестановкой,* неупорядоченная k-выборка — *k-сочетанием.*

Кроме этого, выборки делятся еще на два типа — а) *без повторений* или б) *с повторениями.* Обычно, когда говорят перестановка(сочетание), подразумевают перестановку(сочетание) без повторений.

Посчитаем количество k-выборок во всех четырех случаях.

Случай 1а) $n(n-1)\ldots(n-k+1)$. Обозначение: $P(n,k) = \frac{n!}{(n-k)!}$. По определению $0! = 1$.

Случай 1б) n^k. В этом случае k может быть больше n.

Случай 2а) $C_n^k = \frac{n!}{k!(n-k)!}$. Каждое k-сочетание без повторений представляет собой $k!$ k-перестановок без повторений. Другое обозначение C_n^k — $\binom{n}{k}$

Случай 2б). Рассмотрим k-сочетание $x_{i_1}, x_{i_2}, \ldots, x_{i_k}$. Пусть число α_i обозначает количество вхождений элемента x_i в данную выборку. Тогда между всеми k-сочетаниями и наборами чисел $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{Z}$, таких что $\alpha_1 + \alpha_2 + \ldots + \alpha_n = k,\ \alpha_1, \alpha_2,\ \ldots, \alpha_n \geqslant 0$, можно установить взаимно однозначное соответствие. Следовательно, количество k-сочетаний с повторениями совпадает с количеством решений уравнения $\alpha_1 + \alpha_2 + \ldots + \alpha_n = k,\ \alpha_1, \alpha_2, \ldots,\ \alpha_n \geqslant 0$. Теперь рассмотрим последовательности из 0 и 1 следующего вида

$$\underbrace{00\ldots0}_{\alpha_1}1\underbrace{00\ldots0}_{\alpha_2}1\ldots1\underbrace{00\ldots0}_{\alpha_n}$$

Каждому решению уравнения соответствует ровно одна последовательность, и наоборот. Значит, количество решений совпадает с количеством таких последовательностей, т.е. равно C_{k+n-1}^k.

Пример. Посчитаем число k-сочетаний с повторениями, в которых все элементы встречаются более, чем один раз. Аналогично случаю 2б), количество таких сочетаний равно числу решений уравнения $\alpha_1 + \alpha_2 + \ldots + \alpha_n = k,\ \alpha_1, \alpha_2, \ldots, \alpha_n \geqslant 1$. Или уравнения $(\alpha_1 - 1) + (\alpha_2 - 1) + \ldots + (\alpha_n - 1) = k - n,\ \alpha_1, \alpha_2, \ldots, \alpha_n \geqslant 1$. Сделав замену $\alpha_i' = \alpha_i - 1$, получим задачу $\alpha_1' + \alpha_2' + \ldots + \alpha_n' = k - n,\ \alpha_1', \alpha_2', \ldots, \alpha_n' \geqslant 0$. Ответ к которой мы уже нашли C_{k-1}^{k-n}.

Перечислим некоторые **свойства.**

1. C_n^k - целое. Будем полагать, что при $k > n$ $C_n^k = 0$.

2. $C_n^k = C_n^{n-k}$.

3. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

Доказательство. Количество всех сочетаний делится на две группы. Первая — это те сочетания, которые содержат x_1 $\left(C_{n-1}^{k-1}\right)$. Вторая — это те, которые не содержат x_1 $\left(C_{n-1}^{k}\right)$.

4. **Биномиальная** теорема.

$$(1+x)^n = \sum_{k=0}^{n} C_n^k x^k$$

Доказательство. Представим левую часть в виде произведения n скобок.

$$\underbrace{(1+x)\dots(1+x)}_{n} = \dots + a_k x^k + \dots$$

Количество различных способов набрать x в степени k есть C_n^k. Это число и есть коэффициент при x^k.

5. $2^n = \sum\limits_{k=0}^{n} C_n^k$

6. $0 = \sum\limits_{k=0}^{n} (-1)^k C_n^k$

7. **Полиномиальная** теорема.

$$(x_1+\dots+x_m)^n = \sum_{r_1,\dots,r_m \geqslant 0} \frac{n!}{r_1!r_2!\dots r_m!} x_1^{r_1}\dots x_m^{r_m}$$

Доказательство.

$$\underbrace{(x_1+\dots+x_m)\dots(x_1+\dots+x_m)}_{n} = \dots + a_{r_1\dots r_m} x_1^{r_1}\dots x_m^{r_m} + \dots$$

Аналогично пункту 4, коэффициент при $x_1^{r_1}\dots x_m^{r_m}$ равен $C_n^{r_1} C_{n-r_1}^{r_2}\dots C_{n-\dots}^{r_m}$.

Пример. Сколько слов можно составить из букв слова "МАКАКА"?

$$(\text{М}+\text{А}+\text{К})^6 = \dots \frac{6!}{1!2!3!} \text{М}^1\text{К}^2\text{А}^3$$

Ответ: 60.

Формулы обращения.

Формулы включения и исключения.

Пусть заданы элементы $x_1, x_2, \dots, x_N$ и набор свойств $p_1, \dots, p_n$. Каждый элемент может обладать каким-либо набором свойств или не обладать ни одним.

Пусть $w(p_{i_1}, \dots, p_{i_k})$ — число элементов, которые обладают свойствами $p_{i_1}, \dots, p_{i_k}$ (может и еще какими-нибудь).

Пусть $W(k) = \sum\limits_{\substack{i_1,\dots i_k \\ 1\leqslant i_1 \leqslant \dots \leqslant i_k \leqslant n}} w(p_{i_1}, \dots, p_{i_k})$. В частности, $W(1) = w(p_1) + \dots + w(p_k)$.

И, наконец, $E(k)$ - число элементов обладающих k-свойствами.

Тогда имеет место следующая *формула*

$$E(0) = N - W(1) + W(2) + \dots + (-1)^n W(n).$$

Доказательство. Рассмотрим два случая.

а) x_1— не обладает никаким свойством. Тогда в левую часть формулы он добавит единицу. А справа будем считать, что его единица входит в число N.

б) x_1 обладает свойствами $p_{i_1}, \ldots, p_{i_k}$. Тогда вклад в левую часть есть 0. А в правую $1 - C_k^1 + C_k^2 + \ldots + (-1)^k C_k^k$. По свойству 6. эта сумма равна 0.

Упражнение. Докажите формулу

$$E(k) = W(k) - C_{k+1}^k W(k+1) + \ldots + (-1)^{n-k} C_n^k W(n).$$

Докажем некоторые **неравенства**.

Пусть $\sum_r^+ = N - W(1) + \ldots - W(r)$, где r нечетно.

$\sum_q^- = N - W(1) + \ldots + W(q)$, где q четно.

Утверждение. *$\forall r, q$ (r-нечетно, q-четно) верно следующее неравенство*

$$\textstyle\sum_r^+ \leqslant E(0) \leqslant \sum_q^-$$

Доказательство. Докажем оценку для $E(0)$ снизу. Если элемент x_1 не обладает никакими свойствами, то его вклад в $\sum_r^+$ и $E(0)$ есть единица. Пусть элемент x_1 обладает свойствами $p_{i_1}, \ldots, p_{i_k}$. Тогда $1 - C_k^1 + C_k^2 - \ldots - C_k^r$ вклад элемента x_1 в левую сумму. Если $k \leqslant r$, то он равен нулю. Покажем, что при $k > r$ он меньше либо равен нуля.

$$1 - C_k^1 + C_k^2 - \ldots - C_k^r =$$

$$= 1 - \left(C_{k-1}^0 + C_{k-1}^1\right) + \left(C_{k-1}^1 + C_{k-1}^2\right) + \ldots - \left(C_{k-1}^{r-1} + C_k^{r-1}\right) \leqslant 0.$$

Что и требовалось доказать.

Формула обращения Мебиуса.

Определим функцию Мебиуса. Пусть $n = p_1^{l_1} \ldots p_k^{l_k}$.

$$\mu(1) = 1, \quad \mu(n) = \begin{cases} (-1)^k, \ l_1 = l_2 = \ldots = l_k = 1, \\ \quad 0, \ \text{в противном случае.} \end{cases}$$

Лемма.

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \ n = 1 \\ 0, \ \textit{в противном случае.} \end{cases}$$

Доказательство. Пусть $n = p_1^{l_1} \ldots p_k^{l_k}, \quad \widehat{n} = p_1^{l_1} \ldots p_k^{l_k}$. При $n = 1$ лемма очевидна. Пусть $n > 1$.

$$\sum_{d|n} \mu(d) = \sum_{d|\widehat{n}} \mu(d) + \sum_{d|\widehat{n},\, d\nmid \widehat{n}} \mu(d).$$

Но второе слагаемое равно нулю по определению функции μ. Поэтому

$$\sum_{d|\widehat{n}} \mu(d) = 1 - C_k^1 + C_k^2 + \ldots + (-1)^k C_k^k = 0.$$

Что и требовалось доказать.

Теорема. *Пусть функции $f, g : \mathbb{N} \to \mathbb{R}$. Тогда, если $f(n) = \sum\limits_{d|n} g(d)$, то справедлива следующая формула $g(n) = \sum\limits_{d|n} f(\frac{n}{d})\mu(d)$.*

Доказательство. Из условия $f\left(\frac{n}{d}\right)=\sum\limits_{\hat{d}\mid\frac{n}{d}} g(\hat{d})$. Тогда

$$\sum_{d|n}\left(\sum_{\hat{d}\,|\,\frac{n}{d}} g(\hat{d})\right)\mu(d)=\sum_{d,\hat{d}\colon d\cdot\hat{d}\,|n} g(\hat{d})\mu(d)=\sum_{\hat{d}\,|n}\sum_{d|\frac{n}{\hat{d}}} g(\hat{d})\mu(d)=\sum_{\hat{d}\,|n} g(\hat{d})\sum_{d|\frac{n}{\hat{d}}}\mu(d)=g(n)$$

Что и требовалось доказать.

Пример. Сколько различных последовательностей из нулей и единиц длины n можно написать по кругу? Если последовательности можно совместить поворотом, они считаются одинаковыми.

Попробуем решить эту задачу с помощью выведенной формулы. Пусть $M(d)$ это число последовательностей длины d и периода d. Последовательность имеет *период* d, если при повороте по часовой стрелке на d элементов она совпадает с собой. Заметим, что если $d|n$, то $M_n(d)=M(d)$. Количество линейных последовательностей, образованных последовательностями длины n и периода d, есть $dM(d)$. Пусть $f(n)$ — количество всевозможных линейных последовательностей длины n.

$$f(n)=2^n=\sum_{d|n} dM(d)\,(=g(d))$$

$$n\cdot M(n)=\sum_{d|n}\mu(d)2^{\frac{n}{d}}$$

Отсюда,

$$M(n)=\frac{1}{n}\sum_{d|n}\mu(d)2^{\frac{n}{d}}$$

Следовательно, искомых последовательностей $T(n)=\sum\limits_{d|n} M(d)$.

Формула обращения Мебиуса для частично упорядоченных множеств с нулем.

Пусть P есть множество с отношениями сравнения "$\leqslant$" и равенства "$=$".

Определение. Если для множества P выполнены следующие аксиомы

1. $x\leqslant x\ \forall x\in P$.
2. $x\leqslant y,\ y\leqslant z\ \Rightarrow\ x\leqslant z$.
3. $x\leqslant y,\ y\leqslant x\ \Rightarrow\ x=y$,

то оно называется *частично упорядоченным* .

Замечание. Некоторые элементы могут быть несравнимы. $x\nleqslant y$.

Определение. Если элемент $\omega\in P$ такой, что $\omega\leqslant x\ \forall x\in P$, тогда ω называется *нулем* множества P.

Определение. Множество $[x,y]=\left\{\omega\in P\ \middle|\ x\leqslant\omega\leqslant y\right\}$ называется *интервалом.*

Определение. Если мощность любого интервала конечна, то множество называется *локально конечным* .

Пусть P локально конечное множество с нулем.

$$f(x,y):P\times P\longrightarrow\mathbb{R}\ \text{ и }\ f(x,y)=0\ \forall x\nleqslant y.$$

Введем некоторые операции в классе таких функций.
Сложение. $h=f+g$ означает, что $h(x,y)=f(x,y)+g(x,y)$.
Умножение на число. $h=af, a\in\mathbb{R}$ означает, что $h(x,y)=a\cdot f(x,y)$.

Операция "$\circ$". $h = f \circ g$ означает, что $h(x, y) = \sum\limits_{z:\ x \leqslant z \leqslant y} f(x, y) g(x, y)$.

Замечание. В силу локальной конечности множества P операция "$\circ$" определена корректна. Т.е. суммируется лишь конечное число слагаемых.

Определение. Множество функций с введенными операциями называется *алгеброй инцидентности* множества P и обозначается $A(P)$.

Перечислим некоторые свойства алгебры инцидентности.

1. Операция "$\circ$" ассоциативна.

2. Операция "$\circ$" дистрибутивна.

3. В $A(P)$ есть единица. Это функция

$$\delta(x, y) = \begin{cases} 1, & x = y \\ 0, & \text{в противном случае.} \end{cases}$$

Т.е. $\forall f \ f \circ \delta = \delta \circ f = f$.

Лекция 2 (10.09.03)

Лемма. *Пусть $f \in \mathcal{A}(P)$ Тогда существование у f левой и правой обратной функции равносильно следующему:*

$$\forall x \in P \quad f(x,x) \neq 0 \tag{1}$$

Доказательство. Очевидно, что если существует x, такой что $f(x,x) = 0$, то ни для какой функции $g \in \mathcal{A}(P) \quad f(x,x)g(x,x) \neq 1 = \delta(x,x)$.

Обратно. Пусть для f выполнено (1). Будем искать такую функцию $g_1 \in \mathcal{A}(P)$, что для любых $x, y \in P$

$$\delta(x,y) = \sum_{\substack{z: \\ x \leqslant z \leqslant y}} f(x,z)g_1(z,y)$$

Для каждого $x \in P$ положим:

$$g_1(x,x) := f^{-1}(x,x) \tag{2}$$

(условие (1) обеспечивает это). Далее для каждой пары $(x,y) : x < y$ рекурентно определим $g_1(x,y)$, считая, что значения $g_1(z,y)$ известны для всех $z : \ x < z \leqslant y$:

$$0 = \delta(x,y) = f(x,x)g_1(x,y) + \sum_{\substack{z: \\ x < z \leqslant y}} f(x,z)g_1(z,y)$$

откуда:

$$g_1(x,y) := -f^{-1}(x,x) \sum_{\substack{z: \\ x < z \leqslant y}} f(x,z)g_1(z,y) \tag{3}$$

Ввиду локальной конечности множества P формула (2) корректно определяет правую обратную функцию к функции f.

Аналогично рассуждая, получаем формулу для левой обратной функции g_2:

$$g_2(x,y) := -f^{-1}(y,y) \sum_{\substack{z: \\ x \leqslant z < y}} g_2(x,z)f(z,y) \tag{4}$$

В силу ассоциативности операции $\circ$ для g_1 и g_2 – соответственно правой и левой обратной функции к f справедлив общеалгебраический факт их равенства:

$$g_1 = \delta \circ g_1 = (g_2 \circ f) \circ g_1 = g_2 \circ (f \circ g_1) = g_2 \circ \delta = g_2$$

Определение. Дзета-функцией множества P называется функция

$$\zeta(x,y) := \begin{cases} 1, & x \leqslant y \\ 0, & \text{иначе} \end{cases}$$

По предыдущей лемме у функции ζ существует обратная функция μ, называемая функцией Мёбиуса. По формулам (2) – (4) имеем:

$$\mu(x,x) = 1$$

$$x < y : \quad \mu(x,y) = -\sum_{\substack{z: \\ x < z \leqslant y}} \mu(z,y) = -\sum_{\substack{z: \\ x \leqslant z < y}} \mu(x,z)$$

Теорема (формула обращения Мёбиуса для локально-конечного частично упорядоченного множества P с нулём)**.** *Пусть $f, g : P \to \mathbb{R}$, причём для любого $x \in P$ справедливо:*

$$g(x) = \sum_{\substack{y:\\ y \leqslant x}} f(y) \tag{5}$$

Тогда имеет место следующая формула обращения:

$$f(x) = \sum_{\substack{y:\\ y \leqslant x}} g(y)\mu(y, x) \tag{6}$$

Доказательство. Подставим в (6) выражение для $g(y)$ из (5) :

$$\sum_{\substack{y:\\ y \leqslant x}} \left(\sum_{\substack{z:\\ z \leqslant y}} f(z) \right) \mu(y, x) = \sum_{\substack{y,z:\\ z \leqslant y \leqslant x}} f(z)\mu(y, x) = \sum_{\substack{y,z:\\ z \leqslant y \leqslant x}} f(z)\zeta(z, y)\mu(y, x)$$

Последнее равенство в силу того, что $\zeta(z, y) = 1$ при $z \leqslant y$. Продолжаем цепочку равенств:

$$\sum_{\substack{y,z:\\ z \leqslant y \leqslant x}} f(z)\zeta(z, y)\mu(y, x) = \sum_{\substack{z:\\ z \leqslant x}} \sum_{\substack{y:\\ z \leqslant y \leqslant x}} f(z)\zeta(z, y)\mu(y, x) = \sum_{\substack{z:\\ z \leqslant x}} f(z) \left(\sum_{\substack{y:\\ z \leqslant y \leqslant x}} \zeta(z, y)\mu(y, x) \right) =$$

$$= \sum_{\substack{z:\\ z \leqslant x}} f(z)\delta(z, x) = f(x)$$

Что и требовалось доказать.

Пример 1. В качестве P возьмём множество натуральных чисел, в качестве отношения порядка на P – обычное отношение "больше - меньше"для натуральных чисел. Ясно, что роль нуля в P играет 1. Вычислим функцию Мёбиуса:

$$\mu(x, x) = 1$$

$$y = x + 1 \, : \, \mu(x, y) = -1$$

$$y \neq x + 1 \, : \, \mu(x, y) = 0$$

Пусть $S_n = \sum\limits_{1}^{n} a_n$, тогда формула обращения Мёбиуса утверждает, что

$$a_n = S_n - S_{n-1}$$

Пример 2. Из общей формулы обращения Мёбиуса получим формулу включения-исключения (см. Лекцию 1). Пусть $X = \{p_1, p_2, ..., p_n\}$ – множество возможных свойств изучаемых N объектов. Пусть $P = \{x \,|\, x \subseteq P\}$, введём отношение порядка на P : $x \leqslant y \overset{def}{\Leftrightarrow} y \subseteq x$, нулю при таком отношении порядка соответствует само множество P. Вычислим функцию Мёбиуса для P:

$$\mu(x, x) = 1$$

$$|y| = |x| - 1 \, : \, \mu(x, y) = -1$$

$$|y| = |x| - 2 \, : \, \mu(x, y) = -((-1) + (-1) + 1) = 1$$

– действительно, существует 2 множества z, таких что $y \subset z \subset x$ и $|z| = |x| - 1$. Далее пусть $\mu(x, y) = (-1)^m$ для $y \subset x$ таких, что $|y| = |x| - m$, при $m = 0, ..., k-1$. Покажем справедливость этой формулы при $m = k$. Действительно, для данных $y \subset x$ существует ровно C_k^l таких z, что $y \subset z \subseteq x$ и $|z| = |x| - (k - l)$, причём по предположению индукции для таких z значения $\mu(x, z) = (-1)^{k-l}$. Таким образом по формуле для вычисления функции μ имеем:

$$\mu(x, y) = -((-1)^{k-1}C_k^1 + (-1)^{k-2}C_k^2 + ... + C_k^k) = (-1)^k$$

(воспользовались известным тождеством $1 - C_k^1 + C_k^2 - ... + (-1)^k C_k^k = 0$ – см. Лекцию 1) .

Теперь на P определим функции $E(x)$ = количество объектов обладающих в точности набором свойств x, а также $\omega(x)$ = количество объектов обладающих набором свойств x (при этом, быть может, имеющих более широкий набор свойств). Ясно, что в наших обозначениях

$$\omega(x) = \sum_{\substack{y: \\ y \leqslant x}} E(x)$$

Поэтому можно применить формулу обращения Мёбиуса:

$$E(x) = \sum_{\substack{y: \\ y \leqslant x}} \omega(y)\mu(y, x)$$

в частности

$$E(\varnothing) = \sum_{k=0}^{n} (-1)^k \sum_{\substack{x: \\ |x|=k}} \omega(x)$$

(сравните с результатом полученным на Лекции 1).

Упражнение. Доказать формулу обращения Мёбиуса из Лекции 1 исходя из общей формулы обращения Мёбиуса.

Метод производящих функций

Рассмотрим $K[[x]]$ – кольцо формальных степенных рядов над полем K, т.е. множество бесконечных числовых последовательностей $a = (a_0, a_1, a_2, ..., a_k, ...)$ формально соотнесённых с бесконечной линейной комбинацией мономов $\{1, x, x^2, ..., x^k, ...\}$ по следующему правилу:

$$a(x) = a_0 + a_1 x + a_2 x^2 + ... + a_k x^k + ...$$

На множестве вводятся естественные операции сложения "+" и умножения " $\cdot$ ":

$$a(x) + b(x) = a_0 + b_0 + (a_1 + b_1)x + (a_2 + b_2)x^2 + ... + (a_k + b_k)x^k$$

$$a(x) \cdot b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + ... + (a_0 b_k + a_1 b_{k-1} + ... + a_{k-1} b_1 + a_k b_0)x^k + ...$$

Построенное множество с этими операциями образует ассоциативное коммутативное кольцо с единицей, роль нуля в кольце играет последовательность $a = (0, 0, 0, ..., 0, ...)$, роль единицы последовательность $a = (1, 0, 0, ..., 0, ...)$.

Утверждение. *Элемент* $a = (a_0, a_1, a_2, ..., a_k, ...) \in K[[x]]$ *обратим тогда и только тогда, когда* $a_0 \neq 0$.

Доказательство. Действительно, если $a_0 = 0$, то, очевидно, ни при каком b $a_0 b_0 \neq 0$. Обратно, пусть $a_0 \neq 0$, тогда положим $b_0 = a_0^{-1}$. Далее по рекурентным соотношениям вычисляем $b_1, b_2, b_3, ...$:

$$b_1 = -a_0^{-1} a_1 b_0$$

$$b_2 = -a_0^{-1}(a_1 b_1 + a_2 b_0)$$

$$. \quad . \quad .$$

Пример. $(1 - x^m)^{-1} = 1 + x^m + x^{2m} + x^{3m} + ...$ – проверяется перемножением.

Введём оператор $D: K[[x]] \to K[[x]]$

$$a(x) = \sum_{i=0}^{\infty} a_i x^i, \quad D(a(x)) = \sum_{i=0}^{\infty} (i+1) a_{i+1} x^i$$

<u>Свойства.</u>

1. $D(a(x) + b(x)) = D(a(x)) + D(b(x))$
2. (формула Лейбница) $D(a(x)b(x)) = D(a(x))b(x) + a(x)D(b(x))$

Следствие. Если $a^i(x), i = 1, ..., N$ – обратимы, то

$$D\left(\prod_{i=1}^{N} a^i(x)\right) = \sum_{i=1}^{N} D(a^i(x)) \prod_{j\neq i} a^j(x) = \prod_{i=1}^{N} a^i(x) \cdot \sum_{i=1}^{N} \frac{D(a^i(x))}{a^i(x)} \Rightarrow$$

$$\frac{D\left(\prod\limits_{i=1}^{N} a^i(x)\right)}{\prod\limits_{i=1}^{N} a^i(x)} = \sum_{i=1}^{N} \frac{D(a^i(x))}{a^i(x)} \tag{7}$$

Применим аппарат производящих функций (формальных рядов) для отыскания количества неприводимых двоичных многочленов степени n.

Итак, пусть $\mathcal{P} = \{\pi(x) | \, \pi(x) = c_0 + c_1 x + ... + c_k x^k, c_i \in \{0, 1\}, c_k = 1\}$ – множество ненулевых многочленов над $\mathbb{Z}_2$.

Из курса алгебры хорошо известно, что кольцо многочленов – факториальная область целостности, т.е. всякий ненулевой многочлен однозначным образом с точностью до порядка сомножителе и домножения на обратимый элемент записывается в произведение неприводимых. В кольце многочленов над $\mathbb{Z}_2$ кроме единицы кольца других обратимых элементов нет. Поставим задачу отыскания I_m – числа неприводимых двоичных многочленов степени m (например I_1, очевидно, равно 2).

Пусть $\mathcal{R} \subseteq \mathcal{P}$, $\mathcal{R}_k = \{\pi(x) \in \mathcal{R} | \, deg\, \pi = k\}$. Производящей функцией или нумератором множества $\mathcal{R}$ называется формальный ряд $c_{\mathcal{R}}(x) = c_0 + c_1 x + c_2 x^2 + ...$, где $c_k = |\mathcal{R}_k|$ для каждого k. Ясно, что $c_{\mathcal{P}}(x) = \sum\limits_{k=0}^{\infty} 2^k x^k = \dfrac{1}{1-2x}$.

Пусть $f_m^1(x), f_m^2(x), ..., f_m^{I_m}(x)$ – все неприводимые многочлены степени m. Пусть

$$R_m^i = \{\pi(x) \in \mathcal{P} | \, \pi(x) = (f_m^i(x))^k, k = 0, 1, 2, ...\}, \; i = 1, 2, ..., I_m.$$

Ясно, что $c_{R_m^i} = 1 + x^m + x^{2m} + x^{3m} + ... = \dfrac{1}{1-x^m}$.

Утверждение. *Справедлива следующая формула:*

$$c_{\mathcal{P}} = \prod_{m=1}^{\infty} \prod_{i=1}^{I_m} c_{R_m^i} \tag{8}$$

Доказательство. Коэффициент при x^k в левой части равенства (8) – количество двоичных многочленов степени k. В силу единственности представления многочлена в виде произведения неприводимых каждому двоичному многочлену $\pi(x)$ взаимнооднозначно можно сопоставить бесконечную последовательность чисел

$$t = (t_1^1, t_1^2, t_2^1, ..., t_2^{I_2}, ..., t_m^1, ..., t_m^{I_m}, ..., 0, 0, 0, ...),$$

всегда заканчивающуюся бесконечной последовательностью нулей, со следующим смыслом : $\pi(x) = \prod_{m=1}^{\infty}\prod_{i=1}^{I_m}(f_m^i(x))^{t_m^i}$. Причём $\sum_m \sum_{i=1}^{I_m} mt_m^i = deg\,\pi(x)$. Если в правой части равенства (8) привести подобные слагаемые, то коэффициент при x^k будет равен $\sum_{t\in A} 1$, где $A = \left\{ t \;\middle|\; \sum_m \sum_{i=1}^{I_m} mt_m^i = k \right\}$. В силу упомянутой взаимно однозначности эти коэффициенты равны. Что и требовалось доказать.

Следствие.

$$\frac{1}{1-2x} = \prod_{m=1}^{\infty} \frac{1}{(1-x^m)^{I_m}}. \tag{9}$$

Далее обратим обе части равенства (9):

$$1-2x = \prod_{m=1}^{\infty}(1-x^m)^{I_m}$$

Продифференцируем и полученное равенство умножим на равенство (9) :

$$\frac{-2}{1-2x} = \frac{D\left(\prod\limits_{m=1}^{\infty}(1-x^m)^{I_m}\right)}{\prod\limits_{m=1}^{\infty}(1-x^m)^{I_m}}.$$

Воспользовавшись равенством (7), имеем:

$$\frac{-2}{1-2x} = \sum_{m=1}^{\infty}\frac{D\left((1-x^m)^{I_m}\right)}{(1-x^m)^{I_m}} = \sum_{m=1}^{\infty} I_m \frac{D\,(1-x^m)}{1-x^m} = \sum_{m=1}^{\infty} mI_m\frac{-x^{m-1}}{1-x^m} \Rightarrow$$

$$\frac{1-2x-1}{1-2x} = \sum_{m=1}^{\infty} mI_m \frac{1-x^m-1}{1-x^m} \Rightarrow$$

$$1-\frac{1}{1-2x} = \sum_{m=1}^{\infty} mI_m\left(1-\frac{1}{1-x^m}\right) \Rightarrow$$

$$-1+\sum_{k=0}^{\infty}2^k x^k = \sum_{m=1}^{\infty} mI_m\left(-1+1+x^m+x^{2m}+...\right) \Rightarrow$$

$$\sum_{k=1}^{\infty}2^k x^k = \sum_{m=1}^{\infty} mI_m\left(x^m+x^{2m}+...\right) \Rightarrow$$

$$2^k = \sum_{m\colon m|k} mI_m.$$

Воспользовавшись формулой обращения Мёбиуса окончательно получаем:

Теорема.

$$I_m = \sum_{m\colon m|k}\mu(m)2^{k/m}$$

Если рассматривать многочлены над $\mathbb{Z}_p$ для простого p, то рассуждая аналогично, получаем для I_m^p – числа неприводимых многочленов степени $m > 0$ из $\mathbb{Z}_p[x]$ со старшим коэффициентом 1 формулу:

$$I_m^p = \sum_{m\colon m|k}\mu(m)p^{k/m}$$

Упражнение. Доказать.

Лекция 3.

Рассмотрим некоторые следствия из теоремы о числе неприводимых многочленов, которую мы доказали на прошлой лекции.

Следствие. $I_m \geqslant 0, I_1 = 2.$

$$2^k = kI_k + I_1 + \sum_{\substack{m|k \\ m\neq 1,k}} mI_m \tag{1}$$

а) если k — простое, то $\sum\limits_{\substack{m|k \\ m\neq 1,k}} mI_m = 0$ и $I_k = \frac{2^k-2}{k}$.

б) если k — не простое, то

$$I_k \leqslant \frac{2^k-2}{k} \leqslant \frac{2^k}{k}. \tag{2}$$

Далее,

$$2^k = kI_k + \sum_{\substack{m|k \\ m>1}} mI_m < kI_k + \sum_{m=1}^{k/2} 2^m < kI_k + 2^{k/2+1} \Longrightarrow$$

$$\Longrightarrow I_k > \frac{2^k - 2^{k/2+1}}{k}$$

Следствие. $I_k > 0, \;\; I_k \sim \frac{2^k}{k}, k \to \infty.$

Рассмотрим пример применения метода производящих функций.

Пример. Сколько можно составить последовательностей из нулей и единиц длины n, в которых две единицы не стоят рядом?

Пусть число таких последовательностей есть u_n. Разобьем все последовательности на две кучи:
а) на первом месте стоит единица,
б) на первом месте стоит ноль.

В случае а) на втором месте по условию должен стоять ноль, поэтому количество последовательностей в этом случае u_{n-2}. А в случае б) их количество есть u_{n-1}

Отсюда, имеем рекурентное соотношение $u_n = u_{n-1} + u_{n-2}$. При этом, $u_1 = 2$, $u_2 = 3$.

Рекурентные соотношения с постоянными коэффициентами.

Рассмотрим рекурентное соотношение

$$u_{n+r} = a_1 u_{n+r-1} + a_2 u_{n+r-2} + \ldots + a_r u_n, \tag{3}$$

где коэффициенты $a_1, \ldots, a_r \in \mathbb{R}$ и $a_r \neq 0$. Наша задача — по известным значениям $u_0, \ldots, u_{r-1}$ найти значения u_n для любых n. Свяжем с последовательностью $u_0, u_1, \ldots$ формальный ряд $u(x) = u_0 + u_1 x + u_2 x^2 + \ldots$.

Рассмотрим ряд $k(x) = 1 - a_1 x - a_2 x^2 - \ldots - a_r x^r$. Пусть ряд $c(x)$ есть произведение рядов $u(x)$ и $k(x)$. Тогда

$$c_{n+r} = u_{n+r} - a_1 u_{n+r-1} - a_2 u_{n+r-2} - \ldots - a_r u_n = 0, \forall n \geqslant 0.$$

А, значит, $\deg c(x) \leqslant r - 1$.

Рассмотрим функцию $f(x) = x^r k(\frac{1}{x})$. Тогда $f(x) = x^r - a_1 x^{r-1} - \ldots - a_r$.

Определение. $f(x)$ называется *характеристичеким многочленом* .

Пусть $\alpha_1, \ldots, \alpha_s$ его корни, $l_1, \ldots, l_s$ соответственно их кратность. Тогда

$$f(x) = (x-\alpha_1)^{l_1} \cdot \ldots \cdot (x-\alpha_s)^{l_s} \Longleftrightarrow k(x) = (1-\alpha_1 x)^{l_1} \cdot \ldots \cdot (1-\alpha_s x)^{l_s}$$

$$u(x) = \frac{c(x)}{k(x)} = \frac{c(x)}{(1-\alpha_1 x)^{l_1} \cdot \ldots \cdot (1-\alpha_s x)^{l_s}} = \sum_{i=1}^{s} \sum_{k=1}^{l_s} \frac{\beta_{i,k}}{(1-\alpha_i x)^k},$$

где $\beta_{i,k} \in \mathbb{C}$. Последнее равенство есть следствие из теоремы о представлении правильной дроби в виде суммы простейших.

Далее,

$$(1-\alpha_i x)^{-k} = 1 + \sum_{n=1}^{\infty} \frac{-k(-k-1) \cdot \ldots \cdot (-k-n+1)}{n!} \alpha_i^n x^n,$$

т.е. коэффициент при x^n есть $\frac{k(k+1)\cdot\ldots\cdot(k+n-1)}{n!}\alpha_i^n$. Заметим, что

$$\frac{k(k+1) \cdot \ldots \cdot (k+n-1)}{n!} \alpha_i^n = \frac{(k-1)! k(k+1) \cdot \ldots \cdot (k+n-1)}{(k-1)! n!} \alpha_i^n = C_{k+n-1}^{k-1} = P(n),$$

где $P(n)$ при фиксированном k есть многочлен от n степени не больше, чем $k-1$.

Отсюда, формула для коэффициентов ряда $u(x)$ запишется в следующем виде

$$u_n = \sum_{i=1}^{s} P_i(n) \alpha_i^n, \qquad \deg P_i(n) \leqslant l_i - 1.$$

Тем самым мы доказали следующую теорему.

Теорема. *Пусть задано рекурентное соотношение* (3). $f(x)$ *его характеристическая функция.* $\alpha_1, \ldots, \alpha_s$ *— корни* $f(x)$, $l_1, \ldots, l_s$ *— их кратность. Тогда решение* (3) *записывается формулой*

$$u_n = \sum_{i=1}^{s} P_i(n) \alpha_i^n, \qquad \deg P_i(n) \leqslant l_i - 1.$$

Упражнение. Доказать, что коэффициенты многочленов $P_i(n)$ однозначно выражаются через $u_0, \ldots, u_{r-1}$.

Числа Фибоначчи.

Числа Фибоначчи задаются следующим рекурентным соотношением

$$u_{n+2} = u_{n+1} + u_n, \quad u_0 = 1, \; u_1 = 2.$$

Составим характеристический многочлен $x^2 - x - 1 = 0$. Его корни есть $\alpha_{1,2} = \frac{1 \pm \sqrt{5}}{2}$. Формула для u_n запишется в виде

$$u_n = C_1 \alpha_1^n + C_2 \alpha_2^n.$$

Коэффициенты C_1, C_2 находятся из системы

$$\begin{cases} C_1 + C_2 = 1 \\ C_1 \left(\frac{1+\sqrt{5}}{2}\right) + C_2 \left(\frac{1-\sqrt{5}}{2}\right) = 2. \end{cases}$$

Лекция 4 (24.09.03)

Рассмотрим применение метода производящих функций для решения задачи о нахождении чисел Каталани – количества способов перемножить n элементов, если умножение не ассоциативно. Обозначим искомое количество способов v_n.

Ясно, что $v_2 = 1$, $v_3 = 2$. Для удобства обозначим $v_1 := 1$. Если в некотором месте разбить n множителей на 2 части : от 1-го до k-го, и от $k+1$-го до n-го и считать, что сначала производятся перемножения внутри них, а потом перемножаются результаты, то при таком разделении существует $v_k v_{n-k}$ способов:

$$\underbrace{(x_1 ... x_k)}_{\substack{v_k \\ \text{способов}}} \underbrace{(x_{k+1} ... x_n)}_{\substack{v_{n-k} \\ \text{способов}}}$$

Поэтому, просуммировав по всем k, для v_n получаем:

$$v_n = v_1 v_{n-1} + v_2 v_{n-2} + ... + v_{n-1} v_1$$

Запишем формальный ряд:

$$v(x) = v_1 x + v_2 x^2 + ... ,$$

где v_i – интересующие нас числа Каталани. Заметим, что в этом случае $v(x)v(x) =$
$= v(x) - x$:

$$v(x)v(x) = v_1 v_1 x^2 + (v_1 v_2 + v_2 v_1)x^3 + ... + (v_1 v_{n-1} + v_2 v_{n-2} + ... + v_{n-1} v_1)x^n + ... =$$

$$= v_2 x^2 + v_3 x^3 + ... + v_n x^n + ...$$

Заметим, что уравнению $(u(x))^2 - u(x) + x = 0$ удовлетворяет функция

$$u(x) = \frac{1 - \sqrt{1-4x}}{2}$$

Эта функция в некоторой окрестности нуля разлагается в сходящийся к ней ряд Тейлора, причём этот ряд Тейлора сходится абсолютно. Следовательно для её ряда Тейлора выполняется то же соотношение. Как мы увидим ниже, этот ряд будет начинаться с члена x, с единичным коэффициентом. Сошлёмся на два факта из общей теории сходящихся рядов : из поточечного равенства сходящихся в некоторой окрестности точки рядов следует равенство их коэффициентов и абсолютно сходящиеся ряды можно перемножать почленно в произвольном порядке. Учитывая всё вышесказанное, становится ясно, что коэффициенты ряда Тейлора функции u – соответствующие числа Каталани. Вычислим их:

$$u(x) = \frac{1 - \sqrt{1-4x}}{2} = \frac{1}{2} \sum_{n=1}^{\infty} \frac{-1/2(1/2-1)...(1/2-n+1)}{n!}(-4)^n x^n$$

$$u_n = -\frac{1}{2}\frac{1}{2}\frac{(-\frac{1}{2})(-\frac{3}{2})...(\frac{-2n+3}{2})}{n!}(-4)^n =$$

$$= \frac{1}{4}\frac{(-1)^n}{2^{n-1}}\frac{(2n-3)!!}{n!}(-4)^n =$$

$$= \frac{1}{4}\frac{1}{2^{n-1}}\frac{(2n-2)!}{(2n-2)!!n!}(4)^n =$$

$$= \frac{4^n}{2^{2n}}\frac{(2n-3)!}{(n-1)!n!} = \frac{1}{n}C_{2n-2}^{n-1},$$

где под $n!!$ понимается произведение натуральных чисел не превосходящих n и той же чётности, что и n.

Откуда заключаем, что

$$v_n = \frac{1}{n} C_{2n-2}^{n-1}$$

Рассмотрим последний пример: подсчитаем количество выборок с повторениями при помощи аппарата производящих функций.

Рассмотрим произведение:

$$\underbrace{(1 + x + x^2 + ...)...(1 + x + x^2 + ...)}_{n} = \sum_{k=0}^{\infty} a_k x^k \qquad (1)$$

Коэффициент при x^k получается приведением подобных слагаемых вида $x^{m_1} x^{m_2} ... x^{m_n}$, т.ч. $m_1 + m_2 + .. + m_n = k$, при этом имеется ровно по одному слагаемому для каждого возможного набора $(m_1, ..., m_n)$ с целыми неотрицательными m_i. Каждому такому слагаемому соответствует выборка k из n элементов с повторениями: m_i – количество i-го элемента в выборке. Отсюда получаем:

$$a_k = \widehat{C}_n^k,$$

где $\widehat{C}_n^k$ – интересующее нас количество выборок из n элементов по k с повторениями.

Как показывалось ранее

$$\underbrace{(1 + x + x^2 + ...)...(1 + x + x^2 + ...)}_{n} = (1 - x)^{-n}$$

В некоторой окрестности нуля $(1-x)^{-n}$ – аналитическая функция, поэтому её можно единственным образом представить в виде сходящегося к ней ряда Тейлора:

$$(1 - x)^{-n} = \sum_{k=0}^{\infty} (-1)^k \frac{-n(-n-1)...(-n-k+1)}{k!} x^k =$$

$$= \sum_{k=0}^{\infty} \frac{(n+k-1)!}{(n-1)!k!} x^k = \sum_{k=0}^{\infty} C_{n+k-1}^k x^k$$

Произведение (1) – тоже сходящийся в некоторой окрестности нуля к функции
$(1 - x)^{-n}$ ряд Тейлора. Откуда заключаем, что

$$\widehat{C}_n^k = a_k = C_{n+k-1}^k$$

Конечные поля

Из курса алгебры известна следующая

Теорема. *Для всякого простого p и натурального n существует единственное с точностью до изоморфизма поле из p^n элементов.*

Ясно, что для $n = 1$ – это $\mathbb{Z}_p$. В этом пункте мы построим конечное поле порядка p^n для произвольного n. Такие поля называются полями Галуа и обозначаются $GF(p^n)$.

Рассмотрим $\mathbb{Z}_p[x]$ – кольцо многочленов одной переменной над полем $\mathbb{Z}_p$. По доказанному в одной из прошлых лекций существует $\pi_n(x) \in \mathbb{Z}_p[x]$ – неприводимый многочлен степени n. Рассмотрим фактор-кольцо $\mathbb{Z}_p[x] \big/ (\pi_n(x))$ и покажем, что оно является искомым полем. Во первых, очевидно, оно состоит только из остатков от деления на многочлен $\pi_n(x)$, т.е. только из многочленов степени не выше $n - 1$. Во вторых, всякий такой многочлен лежит в нём. Таким образом, $\left| \mathbb{Z}_p[x] \big/ (\pi_n(x)) \right| = p^n$. Далее покажем, что это кольцо – область целостности, т.е. в нём нет делителей нуля: действительно, если $P(x)Q(x) = 0$ в $\mathbb{Z}_p[x] \big/ (\pi_n(x))$, т.е. $\pi_n(x) \Big| P(x)Q(x)$, то, в силу неприводимости $\pi_n(x)$, либо $\pi_n(x) \Big| P(x)$, либо $\pi_n(x) \Big| Q(x)$, чего при ненулевых $P(x)$ и $Q(x)$ быть не может, т.к. их степень строго меньше степени $\pi_n(x)$. Из курса алгебры хорошо известно, что конечная область целостности является полем.

Теория Рамсея

Изложение серьёзного результата, доказанного Рамсеем, начнём с простой школьной задачи: для какого минимального N в полном N - вершинном графе, рёбра которого раскрашены в 2 цвета, можно гарантировать существование одноцветного треугольника? Оказывается, ответ: N=6 – существование треугольника для 6-ти вершинного графа легко доказывается рассмотрением произвольной вершины, из которой по принципу Дирихле выходит по крайней мере 3 ребра одного цвета, а затем разбором возможных вариантов цветов рёбер между этими тремя вершинами. Пример 5-ти вершинного графа без одноцветного треугольника легко строится.

Перейдём к общей постановке задачи. Пусть $X = \{x_1, ..., x_n\}$ – конечное n-элементное множество, $r \in \mathbb{N}$. Определим класс подмножеств мощности r:

$$T_r(X) = \{A \subseteq X \Big| \, |A| = r\}$$

По определению говорим, что две системы подмножеств α и β образуют разбиение $T_r(X)$, если $\alpha \cup \beta = T_r(X)$ и $\alpha \cap \beta = \varnothing$.

Теорема. (Рамсей) *Для любых $p, q \geqslant r \in \mathbb{N}$ существует $N(p, q, r)$, такое что для любого $n \geqslant N$ для любого (α, β)-разбиения системы подмножеств $T_r(X)$ выполнено следующее:*

либо существует подмножество $A \subseteq X$ такое, что $|A| = p$ и $T_r(A) \subseteq \alpha$

либо существует подмножество $B \subseteq X$ такое, что $|B| = q$ и $T_r(B) \subseteq \beta$

Доказательство. Доказательство проведём по индукции.

Шаг 1. Для $r = 1$ $T_r(X)$ – множество одноэлементных подмножеств X, т.е., фактически, само X, тогда (α, β) – разбиение множества X. Аналогично $T_r(A) \simeq A$, $T_r(B) \simeq B$. Требуется предъявить такое N, что для любого $n > N$ либо в α будет p элементов, либо в β q. Ясно, что $N = p+q-1$ подходит.

Шаг 2. Разберём случай $q = r$. Пусть β – не пусто. Тогда возьмём в качестве B любой элемент из β – это и будет $q = r$-элементное подмножество в X. Если β – пусто, тогда α – все r-элементные подмножества X. Если $n \geqslant p$ возьмём в качестве A любое p-элементное подмножество X. Аналогично разбирается случай $p = r$ (N в этом случае равно q).

Шаг 3. Предыдущие два шага будем рассматривать как базу для индукции. Индукционный переход будем осуществлять по следующей схеме: считаем утверждение доказанным для троек $(p-1, q, r)$, $(p, q-1, r)$ и для всех троек вида $(p', q', r-1)$, где $p', q' = r-1, r, r+1, ...$ Индукционным переходом мы покажем справедливость утверждения для тройки (p, q, r), причём покажем, что в качестве $N(p, q, r)$ можно взять $N(p_1, q_1, r-1) + 1$, где $p_1 = N(p-1, q, r)$, $q_1 = N(p, q-1, r)$.

Итак, пусть $|X| = N(p_1, q_1, r-1)+1$, (α, β) – разбиение $T_r(X)$. Рассмотрим $X' = X \setminus \{x_1\}, |X'| = N(p_1, q_1, r-1)$. Пусть (α', β') – разбиение $T_{r-1}(X')$, порождённое (α, β), т.е. $D \in \alpha' \Leftrightarrow D \cup \{x_1\} \in \alpha$, $D \in \beta' \Leftrightarrow D \cup \{x_1\} \in \beta$. По индукционному предположению выполнено одно из следующих условий:

а) существует $A' \subseteq X'$, т.ч. $|A'| = p_1$, $T_{r-1}(A') \subseteq \alpha'$;

б) существует $B' \subseteq X'$, т.ч. $|B'| = q_1$, $T_{r-1}(B') \subseteq \beta'$.

Разберём, к примеру, случай а), случай б) разбирается аналогично. $|A'| = p_1 = N(p-1, q, r)$. Рассмотрим $(\hat{\alpha}, \hat{\beta})$ – разбиение $T_r(A')$, т.ч. $\hat{\alpha} \subseteq \alpha$, $\hat{\beta} \subseteq \beta$. Опять по предположению индукции возможна одна из ситуаций:

а1) существует $\hat{A} \subseteq A'$, т.ч. $|\hat{A}| = p-1$, $T_r(\hat{A}) \subseteq \hat{\alpha} \subseteq \alpha$;

а2) существует $\hat{B} \subseteq A'$, т.ч. $|\hat{B}| = q$, $T_r(\hat{B}) \subseteq \hat{\beta} \subseteq \beta$.

В случае а2) сразу кладём $B = \hat{B}$ – искомое множество.

В случае а1) положим $A = \hat{A} \cup \{x_1\}$. Покажем, что A удовлетворяет условию теоремы. Действительно, $|A| = p$ и остаётся проверить, что $T_r(A) \subseteq \alpha$. Для произвольного $D \in T_r(A)$ либо $x_1 \notin D$, либо $x_1 \in D$. В первом случае имеем: $D \in T_r(\hat{A}) \Rightarrow D \in \hat{\alpha} \Rightarrow D \in \alpha$. Во втором рассмотрим $D' = D \backslash \{x_1\}$. $D' \in T_{r-1}(\hat{A}) \subseteq T_{r-1}(A) \subseteq \alpha'$, откуда, по построению множества α', имеем $D \in \alpha$. Доказательство окончено.

Пример, разобранный в начале пункта, показывает, что во введённых обозначениях точная нижняя оценка на $N(3, 3, 2)$ есть 6. Если руководствоваться предложенным в теореме рекурентным соотношением на $N(p,q,r)$, получим

$$N(3,3,2) = N(N(2,3,2), N(3,2,2), 1) + 1 = 2N(3,2,2) = 2 \cdot 3 = 6.$$

В данном случае по предложенному правилу находится минимальное возможное N. Однако, как мы увидим ниже, это не всегда так, и рекурентные соотношения дают сильно завышенные значения N.

Ниже под $N(p,q,r)$ будем обозначать минимальное подходящее N.

Лекция 5.

Рассмотрим несколько следствий из теоремы Рамсея.

Следствие.

$$N(p,q,r) \leqslant N(N(p-1,q,r), N(p,q-1,r), r-1) + 1.$$

Следствие. $r = 2$.

$$N(p,q,2) \leqslant N(p-1,q,2) + N(p,q-1,2).$$

Следствие.

$$N(p,q,2) \leqslant \max(p,q)2^{p+q}.$$

Доказательство.

$$N(p,q,2) \leqslant \max(p-1,q)2^{p+q-1} + \max(p,q-1)2^{p+q-1} \leqslant \max(p,q)2^{p+q}.$$

Введем обозначение $N(p) = N(p,p,2)$.

Следствие. $N(p) \leqslant p\ 2^{2p}$.

Теорема. *(Эрдеша)* $\forall p \geqslant 2$

$$N(p) > \frac{1}{e}\ p\ 2^{\frac{p}{2}-1}.$$

Доказательство. Рассмотрим полный граф с n вершинами K_n. Будем красить его ребра в два цвета. В этом случае утверждение теоремы означает следующее. Какое наименьшее количество вершин должно быть в полном графе K_n, чтобы в нем нашелся полный подграф K_p, такой что все его ребра покрашены в один и тот же цвет. Если при данной раскраске такой полный подграф существует, назовем её "хорошей". Посчитаем число способ раскрасить ребра полного графа K_n так, чтобы всегда была "хорошая" раскраска. C_n^p — число способов выбрать p вершин будущего одноцветного полного подграфа K_p. Его ребра можно окрасить в два цвета. Остальные ребра можно раскрасить $2^{C_n^2 - C_p^2}$ способами. При этом, всего способов раскрасить ребра полного графа K_n в два цвета $2^{C_n^2}$. Значит, если

$$2\,C_n^p\,2^{C_n^2 - C_p^2} \leqslant 2^{C_n^2}, \tag{1}$$

то существует "не хорошая" раскраска. Следовательно, $N(p)$ должно быть больше, чем данное n. Покажем, что при $n = \frac{1}{e}\ p\ 2^{\frac{p}{2}-1}$ неравенство (1) выполняется. Тогда мы получим утверждение теоремы. Для этого сначала по индукции докажем следующее неравенство

$$\left(\frac{p}{e}\right)^p \leqslant p! \tag{2}$$

Пусть для p верно, докажем для $p+1$.

$$(p+1)! = (p+1)p! \geqslant (p+1)\left(\frac{p}{e}\right)^p = (p+1)\left(\frac{p}{e}\right)^p \frac{e}{e}\frac{(p+1)^p}{(p+1)^p} = \left(\frac{p+1}{e}\right)^{p+1}\left(\frac{p}{p+1}\right)^p e$$

Т.е. осталось показать, что

$$\left(\frac{p}{p+1}\right)^p e \geqslant 1 \Longleftrightarrow e \geqslant \left(1+\frac{1}{p}\right)^p$$

Последнее неравенство верно, так как $\lim\limits_{n\to\infty}\left(1+\frac{1}{n}\right)^n = e$, а последовательность $\left(1+\frac{1}{n}\right)^n$ монотонно возрастает при $n \to \infty$. Вернемся к доказательству теоремы.

$$C_n^p = \frac{n!}{(n-p)!p!} < \frac{n^p}{p!}, \quad p \geqslant 2.$$

Из (2) следует, что

$$C_n^p < \left(\frac{n}{p}\right)^p e^p \tag{3}$$

Неравенство (1) равносильно следующему

$$C_n^p < 2^{C_p^2 - 1} \tag{4}$$

Покажем теперь, что при $n = \frac{1}{e}\ p\ 2^{\frac{p}{2}-1}$ выполняется неравенство

$$\left(\frac{n}{p}\right)^p e^p \leqslant 2^{C_p^2 - 1} \tag{5}$$

и тогда по неравенству (3) будет следовать (4).

$$\left(\frac{1}{e}\frac{p\,2^{\frac{p}{2}-1}}{p}\right)^p e^p = 2^{\frac{p^2}{2}-p}$$

$$(5) \Longleftrightarrow 2^{\frac{p^2}{2}-p} \leqslant 2^{C_p^2-1} \Longleftrightarrow 2^{\frac{p^2}{2}-p} \leqslant 2^{\frac{p^2}{2}-\frac{p}{2}-1} \Longleftrightarrow p \geqslant \frac{p}{2}+1 \Leftrightarrow p \geqslant 2.$$

Тем самым теорема доказана.

Теорема. *(Рамсея, многоцветная раскраска)* $\forall k \geqslant 2, \forall l_1, \ldots, l_k \geqslant r \geqslant 1$ *существует наименьшее* $N = N(l_1, \ldots, l_k, r)$ *такое, что* $\forall n \geqslant N$ *и для любого разбиения* $\alpha_1, \alpha_2, \ldots, \alpha_k$ *множества* $T_r(X)$ $\exists i:\ 1 \leqslant i \leqslant k,\ \exists A_i \subseteq X$ *такое, что* $\mid A_i \mid = l_i$ *и* $T_r(A_i) \subseteq \alpha_i$.

Доказательство. Применим индукцию по k. База — $k = 2$. Пусть для всех $k' < k$ все доказано. Докажем для k.

$$N_k(l_1, \ldots, l_k, r) \leqslant N = N(N_{k-1}(l_1, \ldots, l_{k-1}, r), l_k, r).$$

По разбиению $\alpha_1, \ldots, \alpha_k$ строим разбиение α, β множества $T_r(X)$ следующим образом, $\beta = \alpha_k,\ \alpha = \alpha_1 \cup \ldots \cup \alpha_{k-1}$. По предыдущей теореме Рамсея может быть два случая.

1) $\exists A \subseteq X$ такое, что $\mid A \mid = N_{k-1}(l_1, \ldots, l_{k-1}, r)$ и $T_r(A) \subseteq \alpha$.

2) $\exists B \subseteq X$ такое, что $\mid B \mid = l_k$ и $T_r(B) \subseteq \beta$.

Во втором случае $i = k,\ A_k = B$. В первом — пользуемся предположением индукции. Теорема доказана.

Теорема. *(Шура)* $\forall k \geqslant 1\ \exists R = R(k)$ *такое, что* $\forall n \geqslant R$ *и для любого отображения* ϕ, $\phi : \{1, \ldots, n\} \longrightarrow \{c_1, \ldots, c_n\}$, *найдется одноцветное решение уравнения* $x + y = z$.

Доказательство. Пусть $R(k) = N_k(3, 3, 2)$ и $n \geqslant R(k)$. Построим отображение $\phi^*\ :\ T_2 \longrightarrow \{c_1, \ldots, c_k\}$. следующим образом. Если $(i, j) \in T_2(X),\ i \neq j$, то $\phi^*(i, j) = = \phi(|i - j|)$. По теореме Рамсея существует одноцветный треугольник $\Delta = \{i, j, k\}$. Пусть, для определенности, $i < j < k$. Тогда

$$\phi^*(i, j) = \phi^*(i, k) = \phi^*(j, k).$$

Но это равенство равносильно следующему

$$\phi(j - i) = \phi(k - i) = \phi(k - j).$$

Поэтому, если обозначить $x = j - i,\ y = k - j,\ z = k - i$, то мы нашли одноцветное решение уравнения $x + y = z$. Теорема доказана.

Теорема. *(Ферма для конечных полей)* $\forall m \geqslant 1\ \exists P = P(m)$ *такое, что для любого простого* $p \geqslant P$ *существует решение уравнения* $x^m + y^m = z^m$ $(mod\ p)$.

Доказательство. Рассмотрим кольцо вычетов по модулю p, $\mathbb{Z}_p = \{0, \dots, p-1\}$. В группе $\mathbb{Z}_p \backslash \{0\}$ есть первообразный корень g, т.е. $\{1, \dots, p-1\} = \{g^1, g^2, \dots, g^{p-1}\}$. Т.е. если $x \in \mathbb{Z}_p \backslash \{0\}$, то $x = g^{l_x}$, $1 \leqslant l_x \leqslant p-1$. Ясно, что l_x можно представить в виде $l_x = i_x + mj_x$ единственным образом. Устраиваем раскраску чисел из $\mathbb{Z}_p \backslash \{0\}$.

$$\phi : \mathbb{Z}_p \backslash \{0\} \longrightarrow \{c_1, \dots, c_m\}$$

$$\phi(x) = c_i \Longleftrightarrow i_x = i - 1$$

По теореме Шура для любого m существует такое $R = R(m)$, что для всех $p \geqslant R + 1$ существует одноцветное решение уравнения $x + y = z$, т.е. существуют такие $i_x, j_x, i_y, j_y, i_z, j_z$, что

$$g^{i_x + mj_x} + g^{i_y + mj_y} = g^{i_z + mj_z}.$$

Но поскольку решение одноцветное, то $i_x = i_y = i_z$, и выполнено равенство

$$g^{i + mj_x} + g^{i + mj_y} = g^{i + mj_z}.$$

Умножая на g^{-i} получаем

$$(g^{j_x})^m + (g^{j_y})^m = (g^{j_z})^m.$$

Что и требовалось доказать.

Часть II
Кодирование.

Лекция 6

Теория кодирования

Пусть A – конечный алфавит: $A = \{a_1, ..., a_m\}$, $m \geqslant 2$. B – двоичный алфавит: $B = \{0, 1\}$. Для произвольного алфавита $\mathcal{K}$ определим множество слов конечной длины:

$$\mathcal{K}^* = \bigcup_{n \geqslant 1} \mathcal{K}^n \cup \{\Lambda\}, \text{где}$$

$$\mathcal{K}^n = \{\alpha | \alpha = k_{i_1}...k_{i_n},\, k_{i_j} \in \mathcal{K}\},$$

Λ– пустое слово, обладающее свойством: $\Lambda\alpha = \alpha\Lambda = \alpha\,\forall\alpha$.

Положим $\lambda(\alpha)$ – длина слова α, так для любого $\alpha \in \mathcal{K}^n$ $\lambda(\alpha) = n$.

В теории кодирования рассматривается задача построения отображения

$$\mathcal{F} : A^* \to B^*$$

обладающего определёнными свойствами. Основной практический интерес представляют следующие свойства отображения $\mathcal{F}$:

1. Взаимнооднозначность – сообщение желательно уметь не только закодировать, но и раскодировать.
2. Сжатие – длина сообщения в алфавите B должна быть по возможности короткой.
3. Устойчивость к помехам – это так называемые *коды исправляющие ошибки*, о них пойдёт речь в следующих лекциях.
4. Шифрование – в целях конфиденциальности передачи информации используются специальные криптографические коды. В этом курсе лекций мы не будем их рассматривать.

Рассмотрим простейшее побуквенное кодирование. Оно строится следующим образом: сначала определяется отображение

$$\psi : A \to B^*$$

$$a_i \xrightarrow{\psi} v_i \in B^*$$

затем для произвольного слова $\alpha = a_{i_1}...a_{i_k} \in A^*$ полагают:

$$F(\alpha) = \beta = \psi(a_{i_1})...\psi(a_{i_k}) = v_{i_1}...v_{i_k} \in B^*.$$

Пустое слово из рассмотрения исключается. Множество $\{v_1, ..., v_m\}$ обозначается V и наравне с отображением F называется кодом.

Код называется *разделимым*, если из равенства $v_{i_1}v_{i_2}...v_{i_k} = v_{j_1}v_{j_2}...v_{j_l}$ следует $k = l$ и $i_1 = j_1$, $i_2 = j_2, ..., i_k = j_k$. Ясно, что если код разделимый, то кодирование взаимнооднозначно.

Введём ещё одно важное определение. Для двух слов $\alpha, \beta \in B^*$ α называется префиксом β, если $\beta = \alpha\alpha'$ для некоторого $\alpha' \in B^*$. Код называется *префиксным*, если для любых $i, j : i \neq j$ v_i не является префиксом v_j. Нетрудно понять, что если код префиксный, то он разделимый.

Теорема (Неравенство Крафта-Макниллана). *Пусть $V = \{v_1, .., v_m\}, m \geqslant 2$ – разделимый код. Тогда*

$$\sum_{i=1}^{m} 2^{-\lambda(v_i)} \leqslant 1. \tag{1}$$

Доказательство. Для произвольного $n \in \mathbb{N}$ определим

$$W = F(A^k) = \{w \in B^* | w = v_{i_1}...v_{i_n}, 1 \leqslant i_1, ..., i_n \leqslant m\}$$

$$W_k = \{w \in W | \lambda(w) = k\}$$

Пусть $\lambda_{max} = \max\limits_{v_i \in V} \lambda(v_i)$. Рассмотрим некоторые очевидные свойства этих множеств:

1)$W = \bigsqcup\limits_{k=1}^{n\lambda_{max}} W_k$, где объединение является объединением непересекающихся множеств (дизъюнктным).

2) $v_{i_1}...v_{i_n} \neq v_{j_1}...v_{j_n}$ при $(i_1, ..., i_n) \neq (j_1, .., j_n)$ – в силу разделимости кода V.

3) $|W| = \sum\limits_{k=1}^{n\lambda_{max}} W_k = m^n$.

4) $|W_k| \leqslant 2^k$.

Введём в рассмотрение две функции положительного аргумента x:

$$h_v(x) = \sum_{i=1}^{m} x^{-\lambda(v_i)},$$

$$h_w(x) = \sum_{w \in W} x^{-\lambda(w)}.$$

Заметим, что в силу свойства 2)

$$\sum_{w \in W} x^{-\lambda(w)} = \sum_{(i_1,...,i_n)} x^{-\lambda(v_{i_1}...v_{i_n})},$$

где суммирование ведётся по всем возможным индексам $(i_1, ..., i_n)$. Далее

$$\sum_{(i_1,...,i_n)} x^{-\lambda(v_{i_1}...v_{i_n})} = \sum_{(i_1,...,i_n)} x^{-(\lambda(v_{i_1})+...\lambda(v_{i_n}))} = \left(x^{-\lambda(v_1)} + ... + x^{-\lambda(v_m)}\right)^n = (h_v(x))^n.$$

Откуда

$$h_v(x) = (h_w(x))^{1/n}.$$

В силу свойств 1) и 4) имеем:

$$h_w(x) = \sum_{k=1}^{n\lambda_{max}} |W_k| x^{-k} \leqslant \sum_{k=1}^{n\lambda_{max}} 2^k x^{-k}.$$

Поэтому $h_v(2) \leqslant (n\lambda_{max})^{1/n}$. Построения верны для любого n, поэтому неравенство останется верным, если перейти к пределу при $n \to \infty$. Получим:

$$h_v(2) \leqslant 1.$$

Что и требовалось доказать.

Возможно ли для данного набора длин $\lambda(v_i)$, удовлетворяющих неравенству (1), построить разделимый код? Ответ даёт следующее

Утверждение. *Для данного набора чисел $l_1, ..., l_m \in \mathbb{N}, m \geqslant 2$, удовлетворяющих неравенству:*

$$\sum_{i=1}^{m} 2^{-l_i} \leqslant 1, \tag{2}$$

всегда существует префиксный код $V = \{v_1, ..., v_m\}$, *такой что* $\lambda(v_i) = l_i$, $i = 1, ..., m$.

Доказательство. Пусть среди набора чисел $\{l_i\}_{i=1}^m$ имеется ровно s различных: $\{t_j\}_{j=1}^s$, причём

$$1 \leqslant t_1 \leqslant ... \leqslant t_s.$$

Пусть v_j – количество чисел равных t_j среди чисел $\{l_i\}_{i=1}^m$. Неравенство (2) перепишется в виде:

$$\sum_{j=1}^{s} v_j 2^{-t_j} \leqslant 1. \tag{3}$$

Откуда, в частности, следует, что

$$v_1 \leqslant 2^{t_1}.$$

Поэтому найдётся v_1 различных слов длины t_1. Из (3) также следует, что

$$v_1 2^{-t_1} + v_2 2^{-t_2} \leqslant 1 \Rightarrow$$

$$v_2 \leqslant 2^{t_2} - v_1 2^{(t_2 - t_1)}.$$

Это означает, что найдётся v_2 слов длины t_2, таких что выбранные до этого v_1 слов длины t_1 не будут являться их префиксами. Рассуждаем аналогично. Пусть мы уже выбрали v_1 слов длины t_1, v_2 длины t_2 и так далее v_r длины t_r $(r < s)$. Покажем, что мы можем выбрать v_{r+1} слов длины t_{r+1} так, что никакие из ранее выбранных не будут являться префиксами новых. Действительно из (3) следует, что

$$\sum_{j=1}^{r+1} v_j 2^{-t_j} \leqslant 1. \Rightarrow$$

$$v_{r+1} \leqslant 2^{t_{r+1}} - v_1 2^{t_{r+1} - t_1} - ... - v_r 2^{t_{r+1} - t_r},$$

а это и означает требуемое условие. Таким образом мы и построим весь искомый префиксный код. Утверждение доказано.

Для произвольного кода $V = \{v_1, ..., v_m\}$ введём две характеристики:

$$L = \sum_{i=1}^{m} \lambda(v_i)$$

и M – максимальное число кодовых слов, которое можно подряд поместить внутри других кодовых слов: для произвольного v_j определяется k_j – наибольшее k, такое что существуют $v_{i_1}, ..., v_{i_k}$, такие что $v_j = \alpha v_{i_1} ... v_{i_k} \beta$, $M = \max_j k_j$.

Утверждение. *Пусть* V *– код, не являющийся разделимым.* α *– слово минимальной длины из* B^*, *допускающее двоякое толкование. Тогда*

$$\lambda(\alpha) \leqslant \lambda_{max} \frac{(L - m + 1)(M + 1)}{2}.$$

Доказательство. Слово α разбивается двумя способами на элементарные слова кода V. Назовём их верхнее и нижнее разбиения. Нанесём их одновременно на слово α. В результате получим некоторое сумарное разбиение на слова β_i. Причём, в силу минимальности слова α, первая точка сумарного разбиения принадлежащая сразу двум разбиениям (верхнему и нижнему) будет концом слова α. В сумарном разбиении все слова делятся на два класса – те, которые являются элементарными кодами, и остальные. Покажем, что все слова из второго класса – различны. Если существуют $\beta_1 = \beta_2 = \beta$ – слова из второго класса такие, что

$$\alpha = \beta' \beta_1 \beta'' \beta_2 \beta''',$$

для некоторых $\beta', \beta'', \beta'''$, то рассмотрим слово

$$\beta'\beta\beta'''.$$

Утверждается, что оно имеет по крайней мере 2 различных расшифровки. Действительно, возможны две ситуации (другие ситуации невозможны, в силу минимальности длины α):

1) β в обоих позициях является концом элементарного слова при первой расшифровке и началом элементарного слова при второй. Тогда слово $\beta'\beta\beta'''$ по первому способу расшифровывается как $\beta'\beta + \beta'''$ (отдельно расшифровывается $\beta'\beta$, отдельно β''', а потом приписываются друг к другу), по второму $\beta' + \beta\beta'''$. Ясно, что эти способы разные.

2) β в первом случае является концом слова при первой расшифровке и началом при второй, а во втором является началом слова при первом способе и концом при втором. В этом случае $\beta'\beta\beta'''$ расшифровывается как $\beta'\beta$ по первому способу "+" β''' по второму, а также β' по второму "+" $\beta\beta'''$ по первому – снова две различные расшифровки.

Но длина слова $\beta'\beta\beta'''$ строго меньше длины слова α – приходим к противоречию с выбором α.

Пусть g – число количество слов второго рода. Ясно, что g не превосходит число всевозможных префиксов элементарных слов из V, т.е.

$$g \leqslant (\lambda(v_1) - 1) + (\lambda(v_2) - 1) + ... + (\lambda(v_m) - 1) = L - m.$$

Между двумя последовательными словами второго рода не может быть больше M слов первого рода, ровно как и от начала слова до первого слова второго рода и от конца последнего слова второго рода до конца слова α – все эти участки (назовём их основными) являются вложенными для какого либо кодового слова, либо по первому разбиению, либо по второму. Таких участков всего не более чем $L - m + 1$. Каждому основному участку соответствует не более чем M слов из одного разбиения и ровно 1 из другого. Поэтому сумарно в двух разбиениях не более чем $(L-m+1)(M+1)$ слов. Т.е.

$$2\lambda(\alpha) \leqslant \lambda_{max}(L - m + 1)(M + 1) \Rightarrow$$

$$\lambda(\alpha) \leqslant \lambda_{max}\frac{(L - m + 1)(M + 1)}{2}$$

Теорема доказана.

Из этого важного утверждения следует способ проверки кода на разделимость: достаточно проверить на однозначную расшифровку все слова длиной не выше $\lambda_{max}\frac{(L - m + 1)(M + 1)}{2}$.

Лекция 7.

Пусть $C \subseteq B^*$. Будем обозначать $\overrightarrow{C}$ множество префиксов слов из C. Разделимый код V называется полным, если $\overrightarrow{(V^*)} = B^*$.

Утверждение. *Разделимый код V является полным тогда и только тогда, когда для любого $\beta \in B^*$, такого что $\lambda(\beta) \geqslant \lambda_{max}$, существует $v_i \in V$ такое, что $\beta = v_i\gamma$, для некоторого $\gamma \in B^*$, где $\lambda_{max} = \max\limits_{v \in V} \lambda(v)$.*

Доказательство. Необходимость. Возьмём произвольное слово β, длина которого строго больше длины любого слова из V. По определению оно является префиксом некоторого слова $v_{i_1}v_{i_2}...v_{i_k}$. Но его длина больше чем длина v_{i_1}, значит необходимое представление имеет место.

Достаточность. Пусть код V неполный, т.е. существует $\beta \in B^*, \beta \notin \overrightarrow{(V^*)}$. Выберем β так, чтобы $\lambda(\beta)$ было наименьшим. Пусть $v \in V$ такое, что $\lambda(v) = \lambda_{max}$. Пусть $\beta' = \beta v$, тогда $\beta' \in B^*, \lambda(\beta') \geqslant \lambda_{max}$, значит, по условию $\exists v_i \in V$ такое, что $\beta' = v_i\gamma$ или $\beta v = v_i\gamma$. По предположению $\beta \notin \overrightarrow{(V^*)}$, следовательно, β не является префиксом v_i. Значит, v_i — префикс β: $\beta = v_i\gamma$. Если $\gamma \in \overrightarrow{(V^*)}$, то, очевидно, и $\beta \in \overrightarrow{(V^*)}$, значит $\gamma \notin \overrightarrow{(V^*)}$, но $\lambda(\gamma) < \lambda(\beta)$ – противоречие с минимальностью длины β.

Теорема. (Критерий полноты разделимого кода) *Разделимый код $V = \{v_1, \dots, v_m\}$ является полным тогда и только тогда, когда код V является префиксным и выполнено равенство*

$$\sum_{i=1}^{m} 2^{-\lambda(v_i)} = 1. \qquad (1)$$

Доказательство. Пусть V – разделимый полный код. Выберем произвольное $n > \lambda_{max}$. Рассмотрим множество $B^n = \{\beta_1, ..., \beta_{2^n}\}$ – множество всех слов из B^* длины n, а также множества $V_i = \{\beta \in B^* | \lambda(\beta) = n, \beta = v_i\gamma\}$, $i = 1, ..., m$. Ясно, что $|V_i| = 2^{n-\lambda(v_i)}$. В силу предыдущего утверждения

$$B^n \subseteq \bigcup_{i=1}^{m} V_i,$$

откуда

$$2^n \leqslant \sum_{i=1}^{m} 2^{n-\lambda(v_i)},$$

причём равенство возможно лишь в случае $V_i \cap V_j = \varnothing$, при $i \neq j$, т.е. если код префиксный. В силу неравенства Крафта-Макмиллана

$$2^n \geqslant \sum_{i=1}^{m} 2^{n-\lambda(v_i)}.$$

Поэтому

$$2^n = \sum_{i=1}^{m} 2^{n-\lambda(v_i)},$$

и код префиксный.

Обратно, пусть код V – префиксный код, удовлетворяющий (1). В силу префиксности он разделимый, и нужно показать только полноту. Возьмём β, такое что $n = \lambda(\beta) > \lambda_{max}$. Т.к. код префиксный, то $V_i \cap V_j = \varnothing$, при $i \neq j$. Поэтому

$$\left|\bigcup_{i=1}^{m} V_i\right| = \left|\bigsqcup_{i=1}^{m} V_i\right| = \sum_{i=1}^{m} 2^{n-\lambda(v_i)}$$

Если β не представляется в виде $\beta = v_i\gamma$, то

$$|B^n| > \left|\bigcup_{i=1}^{m} V_i\right|,$$

т.е.

$$2^n > \sum_{i=1}^{m} 2^{n-\lambda(v_i)}$$

– противоречие с (1). Т.о. код V удовлетворяет условию предыдущего утверждения. Теорема доказана.

Следствие. *Пусть* $V = \{v_1, ..., v_m\}$ *– префиксный код, тогда существует префиксный и полный код* V' *такой, что выполнено неравенство* $\lambda(v'_i) \leqslant \lambda(v_i)$.

Доказательство. Пусть $l_i = \lambda(v_i)$. По неравенству Крафта-Макмиллана

$$\sum_{i=1}^{m} 2^{-l_i} \leqslant 1.$$

Если

$$\sum_{i=1}^{m} 2^{-l_i} = 1,$$

то по критерию полноты получаем, что V – полный. Разберём случай

$$\sum_{i=1}^{m} 2^{-l_i} < 1.$$

В этом случае справедливо

$$\sum_{i=1}^{m} 2^{-l_i} + 2^{-\lambda_{max}} \leqslant 1.$$

Пусть $l_j = \lambda_{max}$. Тогда

$$1 - \sum_{\substack{i=1 \\ i \neq j}}^{m} 2^{-l_i} \geqslant 2^{-l_j} + 2^{-l_j} = 2^{-(l_j-1)}.$$

Положим

$$l'_i = \begin{cases} l_i, & i \neq j \\ l_j - 1, & i = j \end{cases}$$

Для чисел l'_i выполняется

$$\sum_{i=1}^{m} 2^{-l'_i} \leqslant 1. \tag{2}$$

Значит, по утверждению из предыдущей лекции существует префиксный код $V' = \{v'_1, ..., v'_m\}$ с длинами кодовых слов l'_i, таких что $\sum\limits_{i=1}^{m} l'_i < \sum\limits_{i=1}^{m} l_i$. Если в (2) по прежнему строгое неравенство, то применим описанную процедуру к нему, и т.д. Ведя индукцию по $\sum\limits_{i=1}^{m} l'_i$ получим, что рано или поздно в неравенстве Крафта-Макмиллана достигнется равенство. Следствие доказано.

Пусть $A = \{a_1, ..., a_m\}$, $P = \{p_1, ..., p_m\}$ – распределение вероятностей появления букв в тексте:

$$\sum_{i=1}^{m} p_i = 1.$$

Поставим задачу: для заданного P построить разделимый код V оптимальный в смысле математического ожидания длины кодирующего слова. Формально: введём

$$L_V(P) = \sum_{i=1}^{m} p_i \lambda(v_i)$$

и
$$L(P) = \inf_{V-\text{разд.}} L_V(P).$$
Если $L_V(P) = L(P)$, тогда V называется *оптимальным.*

Рассмотрим свойства оптимальных кодов:

1) Оптимальный код существует. Действиетльно, для любого V $L_V(P) \geqslant 1$, кроме того для любого M существует лишь конечное число различных кодов V, таких что $L_V(P) < M$. Поэтому нижняя грань по $L_V(P)$ достигается обязательно на каком либо коде V.

2) Если V – оптимальный код, то существует V' – оптимальный и при этом префиксный код – по следствию из критерия полноты.

3) Для оптимального кода $V = \{v_1, ..., v_m\}$ справедливо
$$p_i > p_j \Rightarrow \lambda(v_i) \leqslant \lambda(v_j)$$
– в противном случае, поменяв местами v_i и v_j получим код с меньшим $L_V(P)$.

4) Если V – оптимальный префиксный код, то существуют v_i и v_j, такие что $\lambda(v_i) = \lambda(v_j) = \lambda_{max}$ и $v_i = v0, \ v_j = v1$, для некоторого $v \in B^*$.

Теорема (Редукции). *Пусть* $V = \{v_1, \ldots, v_m\}, m \geqslant 2$, *оптимальный префиксный код при распределении* $P = \{p_1, \ldots, p_m\}, p_1 \geqslant p_2 \geqslant \ldots \geqslant p_m$. *Пусть числа* q_0, q_1 *таковы, что*
$$q_0 + q_1 = p_i$$
для некоторого $1 \leqslant i \leqslant m$, *и*
$$p_m \geqslant q_0 \geqslant q_1.$$
Тогда $W = \{v_1, ..., v_{i-1}, v_{i+1}, ..., v_m, v_i0, v_i1\}$ *– оптимальный префиксный код для* $P' = \{p_1, ..., p_{i-1}, p_{i+1}, ..., p_m, q_0, q_1\}$.

Доказательство. $L_W(P') = L_V(P) - p_i\lambda(v_i) + q_0\lambda(v_i0) + q_1\lambda(v_i1) = L_V(P) + p_i$. Пусть $\widehat{W}$ – оптимальный код при распределении P'. Тогда согласно свойствам 3) и 4) оптимальных кодов $\widehat{W}$ имеет следующую структуру:
$$\widehat{W} = \{w_1, w_2, ..., w_{i-1}, w_{i+1}, ..., w_m, w0, w1\}.$$
Рассмотрим код
$$\widehat{V} = \{w_1, w_2, ..., w_{i-1}, w, w_{i+1}, ..., w_m\}.$$
Ясно, что
$$L_{\widehat{W}}(P') = L_{\widehat{V}} + p_i.$$
Но, в силу оптимальности V,
$$L_V \leqslant L_{\widehat{V}}.$$
Откуда
$$L_W \leqslant L_{\widehat{W}}.$$
Что и требовалось доказать.

Алгоритм Хаффмана построение оптимального кода.

Пусть требуется построить оптимальный код для заданного упорядоченного распределения $p_1 \geqslant ... \geqslant p_m$,

1)Если $m = 2$ переходим к пункту 4;

2)Положим $p' = p_{m-1} + p_m$;

3)Отсортируем набор $p_1, ..., p_{m-2}, p'$;

4)Для двух чисел $\hat{p}_1, \hat{p}_2$ строим кодовые слова 0 и 1;

5)”Раскручиваем” набор вероятностей в ”обратную” сторону, приписывая к кодовым словам 0 и 1.

Пример.

$$\begin{aligned}
p_1^{(0)} &= 0,2 \\
p_2^{(0)} &= 0,2 \\
p_3^{(0)} &= 0,15 \\
p_4^{(0)} &= 0,15 \\
p_5^{(0)} &= 0,1 \\
p_6^{(0)} &= 0,1 \\
p_7^{(0)} &= 0,05 \\
p_8^{(0)} &= 0,05
\end{aligned}
\qquad
\begin{aligned}
p_5^{(1)} &= p_7^{(0)} + p_8^{(0)} : \\
p_1^{(1)} &= 0,2 \\
p_2^{(1)} &= 0,2 \\
p_3^{(1)} &= 0,15 \\
p_4^{(1)} &= 0,15 \\
p_5^{(1)} &= 0,1 \\
p_6^{(1)} &= 0,1 \\
p_7^{(1)} &= 0,1
\end{aligned}
\qquad
\begin{aligned}
p_1^{(2)} &= p_6^{(1)} + p_6^{(1)} : \\
p_1^{(2)} &= 0,2 \\
p_2^{(2)} &= 0,2 \\
p_3^{(2)} &= 0,2 \\
p_4^{(2)} &= 0,15 \\
p_5^{(2)} &= 0,15 \\
p_6^{(2)} &= 0,1
\end{aligned}
\qquad
\begin{aligned}
p_1^{(3)} &= p_5^{(2)} + p_6^{(2)} : \\
p_1^{(3)} &= 0,25 \\
p_2^{(3)} &= 0,2 \\
p_3^{(3)} &= 0,2 \\
p_4^{(3)} &= 0,2 \\
p_5^{(3)} &= 0,15
\end{aligned}$$

$$\begin{aligned}
p_1^{(4)} &= p_4^{(3)} + p_5^{(3)} : \\
p_1^{(4)} &= 0,35 \\
p_2^{(4)} &= 0,25 \\
p_3^{(4)} &= 0,2 \\
p_4^{(4)} &= 0,2
\end{aligned}
\qquad
\begin{aligned}
p_1^{(5)} &= p_3^{(4)} + p_4^{(4)} : \\
p_1^{(5)} &= 0,4 \\
p_2^{(5)} &= 0,35 \\
p_3^{(5)} &= 0,25
\end{aligned}
\qquad
\begin{aligned}
p_1^{(6)} &= p_2^{(5)} + p_3^{(5)} : \\
p_1^{(6)} &= 0,6 \\
p_2^{(6)} &= 0,4
\end{aligned}$$

Делаем обратный ход:

$$\begin{aligned}
v_1^{(6)} &= 0 \\
v_2^{(6)} &= 1
\end{aligned}
\qquad
\begin{aligned}
v_1^{(5)} &= 1 \\
v_2^{(5)} &= 00 \\
v_3^{(5)} &= 01
\end{aligned}
\qquad
\begin{aligned}
v_1^{(4)} &= 00 \\
v_2^{(4)} &= 01 \\
v_3^{(4)} &= 10 \\
v_4^{(4)} &= 11
\end{aligned}
\qquad
\begin{aligned}
v_1^{(3)} &= 01 \\
v_2^{(3)} &= 10 \\
v_3^{(3)} &= 11 \\
v_4^{(3)} &= 000 \\
v_5^{(3)} &= 001
\end{aligned}
\qquad
\begin{aligned}
v_1^{(2)} &= 10 \\
v_2^{(2)} &= 11 \\
v_3^{(2)} &= 000 \\
v_4^{(2)} &= 001 \\
v_5^{(2)} &= 010 \\
v_6^{(2)} &= 011
\end{aligned}$$

$$\begin{aligned}
v_1^{(1)} &= 11 \\
v_2^{(1)} &= 000 \\
v_3^{(1)} &= 001 \\
v_4^{(1)} &= 010 \\
v_5^{(1)} &= 011 \\
v_6^{(1)} &= 100 \\
v_7^{(1)} &= 101
\end{aligned}
\qquad
\begin{aligned}
v_1^{(0)} &= 11 \\
v_2^{(0)} &= 000 \\
v_3^{(0)} &= 001 \\
v_4^{(0)} &= 010 \\
v_5^{(0)} &= 100 \\
v_6^{(0)} &= 101 \\
v_7^{(0)} &= 0110 \\
v_8^{(0)} &= 0111
\end{aligned}$$

В заключение приведём одно очевидное

Утверждение. *Если V — оптимальный префиксный код, тогда V – полный.* **Доказательство.** По следствию из критерия полноты.

<u>Лекция 8</u> (22.10.03)

Коды, исправляющие ошибки

Постановка задачи. Имеется канал связи, по которому необходимо передавать сообщения – двоичные коды (общая теория не сильно изменится, если в качестве алфавита сообщений взять более широкий алфавит, чем двоичный). Канал связи искажает сообщения следующими способами:

1. Ошибки типа замещения: некоторые биты сообщения заменяются на противоположные.
2. Некоторые биты сообщения могут теряются при передаче.
3. В сообщении могут появляться новые биты.

Введём некоторые обозначения. Пусть $\mathcal{B}^n = \{\alpha = (\alpha_1, ..., \alpha_n), \alpha_i \in \{0,1\}\}$ – пространство слов длины n, $|\mathcal{B}^n| = 2^n$. $\mathcal{B}^n$ обладает структурой линейного пространства над полем $\mathbb{Z}_2$. Норма в $\mathcal{B}^n$ задаётся следующим образом: $\|\alpha\| = \sum\limits_{i=1}^{n} \alpha_i$. Введём в $\mathcal{B}^n$ метрику $\rho(\alpha,\beta) = \sum\limits_{i=1}^{n} |\alpha_i - \beta_i| = \|\alpha + \beta\|$, где разность берётся по модулю 2.

Обозначим через $S_n^t(\alpha)$ множество слов, в которое может перейти α при условии возникновения не более чем t ошибок. Пусть $\mathcal{B}^n \supseteq V_n^t = \{\alpha^1, \alpha^2, ..., \alpha^N\}$ – код для слов длины n, устойчивый к не более чем t ошибкам, т.е. $S_n^t(\alpha^i) \cap S_n^t(\alpha^j) = \varnothing$, при $i \neq j$.

Далее мы будем изучать только каналы с возможностью появления ошибок только типа замещения, при том в количестве не более, чем t. В этом случае $S_n^t(\alpha) =$
$= Ш_n^t(\alpha) = \{\beta \in \mathcal{B}^n \big| \|\alpha - \beta\| \leqslant t\}$ – шар в $\mathcal{B}^n$ с центром в α радиуса t. Ясно, что условие $Ш_n^t(\alpha^i) \cap Ш_n^t(\alpha^j) = \varnothing$ равносильно следующему

$$\rho(\alpha^i, \alpha^j) \geqslant 2t + 1. \tag{1}$$

Элементарные оценки. Для любого $0 \leqslant i \leqslant n$ существует ровно C_n^i слов, отличающихся от данного ровно в i разрядах. Поэтому для любого α

$$|Ш_n^t(\alpha)| = \sum_{i=0}^{t} C_n^i$$

Тривиальные оценки числа сочетаний дают

$$\left(\frac{n}{t}\right)^t \leqslant C_n^i \leqslant \frac{n^t}{t!}$$

Откуда

$$c_1(t) n^t \leqslant |Ш_n^t(\alpha)| \leqslant c_2(t) n^t \tag{2}$$

Из условия количества всех слов и пустоты пересечения шаров для кодовых слов получаем

$$\sum_{i=1}^{N} |Ш_n^t(\alpha_i)| = N|Ш_n^t(\alpha)| \leqslant 2^n$$

Откуда, учитывая оценку (2), получаем

$$N \leqslant \frac{2^n}{n^t} c_2(t) \tag{3}$$

$$\log_2 N \leqslant n - t \log_2 n + c_3(t) \tag{4}$$

Оценка (3) носит название "граница сферической упаковки" или "граница Хемминга".

Покажем, что имея в распоряжении некоторые n и t, всегда можно построить некоторый достаточно большой код V_n^t. Для этого условие $Ш_n^t(\alpha^i) \cap Ш_n^t(\alpha^j) = \varnothing$ перепишем в эквивалентном виде:

$$\alpha_j \notin Ш_n^{2t}(\alpha_i)$$

Далее поступаем следующим образом: выбираем произвольное

$$\alpha_1 \in \mathcal{B}^n$$

α_2 выбираем из условия

$$\alpha_2 \notin \text{Ш}_n^{2t}(\alpha_1)$$

α_3 – из условия

$$\alpha_3 \notin \text{Ш}_n^{2t}(\alpha_1) \cup \text{Ш}_n^{2t}(\alpha_2)$$

и т.д. Условие на выбор α_{i+1} запишется следующим образом:

$$\alpha_{i+1} \notin \bigcup_{k=1}^{i} \text{Ш}_n^{2t}(\alpha_i)$$

Ясно, что очередное α_{N+1} не удастся выбрать, только когда

$$\bigcup_{i=1}^{N} \text{Ш}_n^{2t}(\alpha_i) = \mathcal{B}^n$$

Для построенного кода справедлива оценка

$$\sum_{i=1}^{N} |\text{Ш}_n^{2t}(\alpha_i)| \geqslant 2^n$$

т.е.

$$N|\text{Ш}_n^{2t}(\alpha)| \geqslant 2^n$$

Учитывая оценку (2) получаем:

$$N \geqslant c_1(2t)\frac{2^n}{n^{2t}} \tag{5}$$

$$\log_2 N \geqslant n - 2t\log_2 n + c_1 2t \tag{6}$$

Т.о. заключаем, что нельзя построить код, не удовлетворяющий оценке (3) и заведомо можно, удовлетворяющий оценке (5).

Код называют совершенным, если $\bigcup\limits_{i=1}^{N} \text{Ш}_n^t(\alpha^i) = \mathcal{B}^n$, т.е. если $2^n = N|\text{Ш}_n^t(\alpha)|$.

Коды Хэмминга. Коды Хэмминга – коды исправляющие 1 ошибку типа замещения. Для данного n найдём такое k, что $2^{k-1} \leqslant n \leqslant 2^k$. Для каждого целого числа $0 \leqslant m < 2^k$ положим $e^k(m)$ – двоичная запись числа m с использованием k разрядов.

Пример. $e^3(1) = 001$, $e^3(2) = 010$, $e^3(3) = 011$.

Определим обратную операцию: $N(\gamma) = N(\gamma_1 ... \gamma_k) = \sum\limits_{i=1}^{k} \gamma_i 2^{k-i}$, т.е. $N\left(e^k(m)\right) = m$. Теперь определим линейное отображение

$$H : \mathcal{B}^n \to \mathcal{B}^k$$

$$H(\alpha) = H(\alpha_1 ... \alpha_n) = \alpha_1 e^k(1) + ... + \alpha_n e^k(n).$$

Пусть V – ядро этого отображения, т.е. $V = \{\alpha \in \mathcal{B}^n \,|\, H(\alpha) = 0...0\}$. V и называется кодом Хэмминга. Изучим его свойства:

1. $|V| = 2^{n-k}$: множество $\{H(\alpha^{2^i})\, i = 0, ..., k-1\}$, где α^t – строка с единицей на t-ом месте и нулями на остальных, образует базис пространства $\mathcal{B}^k$. Поэтому отображение H – сюръективно, следовательно размерность ядра – $n-k$. Кроме того, система уравнений $H(\alpha) = 0...0$ разрешима относительно первых k элементов, что даёт нам право назвать первые k разрядов кода проверочными, а остальные – информационными, т.е. подпространство в V, натянутое на последние $n-k$ координат, есть $\mathcal{B}^{n-k}$.

2. V есть код, исправляющий одну ошибку типа замещения. При этом алгоритм дешифровки сообщения состоит в следующем: пусть сообщение α при прохождении через канал связи превратилось в строку β. Возможны две ситуации

   а) $H(\beta) = 0 \Leftrightarrow N(H(\beta)) = 0$. В этом случае в предположении, что в канале связи более одной ошибки произойти не могло, делаем вывод, что $\alpha = \beta$.

   б) $H(\beta) \neq 0 \Leftrightarrow N(H(\beta)) = j \neq 0$. В этом случае, всё в том же предположении о количестве ошибок в канале, делаем вывод, что ошибка в j-м разряде и заменяем его на противоположный. Действительно, ошибка в j-ом разряде означает, что $\beta = \alpha + \alpha^j$. Поэтому $N(H(\beta)) = N(H(\alpha + \alpha^j)) = N(\mathrm{H}(\alpha) + H(\alpha^j)) =$
   $= N(H(\alpha)) + N(H(\alpha^j)) = 0 + N(e^k(j)) = j.$

3. Для любых $\alpha, \beta \in V$ $\rho(\alpha, \beta) \geqslant 3$ – выше мы получали, что для любых $\alpha, \beta \in V_n^t$
   $\rho(\alpha, \beta) \geqslant 2t + 1$, по предыдущему свойству V является V_n^1.

4. V является линейным пространством, как ядро линейного оператора. Построенный код V является частным случаем более общих линейных кодов БЧХ, в чём мы убедимся позже.

5. По свойству 3 для любого $\alpha \in V$ $\|\alpha\| = \rho(0, \alpha) \geqslant 3$.

6. Если $n = 2^k - 1$, то $|V| = 2^{n-k} = \frac{2^n}{n+1} \Rightarrow 2^n = |V| \cdot (n+1) = |V| \cdot |SH_n^1(\alpha)|$, т.е. V в этом случае является совершенным.

Линейные коды. Предыдущие построения можно обобщить на случай большего количества проверочных разрядов. Пусть H – $(n-k) \times n$ матрица над $(Z)_2$, имеющая следующую структуру:

$$H = (A | I_{n-k}),$$

где A – некоторая $(n-k) \times k$ матрица, I_{n-k} – единичная матрица порядка $n-k$. Пусть

$$V = \{x \in \mathcal{B}^n \mid Hx^T = 0\}$$

– ядро оператора H. Ясно, что в виду специальной структуры матрицы H система уравнений

$$Hx^T = 0$$

разрешима относительно последних $(n-k)$ координат, т.е. V можно переписать по другому:

$$V = \{x \in \mathcal{B}^n \,| x^T = G^T u^T,\, u \in \mathcal{B}^k\},$$

где

$$G^T = \left(\frac{I_k}{A}\right).$$

Матрица $G = \left(I_k | A^T\right)$ называется порождающей матрицей. Ясно, что $\dim V = k$. V, как ядро линейного оператора, является линейным пространством. Введём d – минимальное расстояние кода:

$$d = \min_{\substack{\alpha,\beta \in V \\ \alpha \neq \beta}} \rho(\alpha, \beta) = \min_{\substack{\alpha \in V \\ \alpha \neq 0}} \|\alpha\|.$$

n, k и d являются параметрами линейного кода, поэтому линейный код, отвечающий этим параметрам обозначают $[n, k, d]$-код. Ясно, что в силу (1) $[n, k, d]$-код исправляет $\left[\frac{d-1}{2}\right]$ ошибок.

Связь между минимальным расстоянием кода и рангом его проверочной матрицы устанавливает следующее

Утверждение. *Пусть V – линейный код с проверочной матрицей H. Тогда V имеет минимальное расстояние d равносильно одновременному выполнению следующих двух условий:*

а) любые $(d-1)$ столбцов в H линейно независимы;

б) существуют d линейно зависимых столбцов

(условия а) и б) вместе означают, что ранг матрицы H равен $d-1$).

Доказательство. Пусть V имеет минимальное кодовое расстояние d. Тогда существует такое $x = (x_1, ..., x_n)$, что $Hx^T = 0$, причём x имеет ровно d ненулевых компонент. Это значит, что столбцы матрицы H с номерами этих ненулевых компонент будут линейно зависимы. $d-1$ же линейно зависимых столбцов нет, иначе существовал бы $x \in V$ с меньшей нормой – противоречие с минимальностью d. Обратно, если существует d линейно зависимых столбцов, то $x = (x_1, ..., x_n)$, имеющий на местах с этими номерами единицы, а на остальных – нули, лежит в V. В то же время, если бы кодовое расстояние V было меньше d, то по доказанному выше существовали бы $d-1$ линейно зависимых столбцов у H – противоречие с а). Доказательство окончено.

<u>Лекция 9</u> (29.10.03)

Коды БЧХ (Боуз, Чоудхури, Хоквингем)

Пусть мы хотим построить линейный код исправляющий t ошибок, т.е. хотим, чтобы для кодового расстояния d было справедливо неравенство:

$$d \geqslant 2t + 1.$$

Как следует из утверждения, доказанного в конце предыдущей лекции, для этого достаточно, чтобы любые $2t$ столбцов проверочной матрицы H были линейно независимы.

Пусть теперь $t = 1$. Условие линейной независимости любых двух столбцов означает одновременное выполнение следующих 2-х условий:

1) $h_i \neq 0$, $i = 1, ..., n$;

2) $h_i \neq h_j$, при $i \neq j$, $i, j = 1, ..., n$,

где h_i, $i = 1, ..., n$ – столбцы матрицы H. Если теперь в качестве столбцов матрицы H взять $h_i = e^{n-k}(i)$ – в обозначениях введённых на прошлой лекции, то получим код Хэмминга. Правда, такая матрица не будет иметь канонической структуры (7) из предыдущей лекции – для этого надо переставить её столбцы.

Займёмся теперь построением кодов БЧХ для произвольного t. Пусть нам даны параметры k и t, выберем параметры n и m, так чтобы выполнялись соотношения :

$$n = 2^m - 1,$$

$$k \geqslant n - tm.$$

На одной из прошлых лекций мы построили поле $GF(2^m)$ – фактор кольца двоичных многочленов по неприводимому многочлену $\pi(x)$ степени m. Элементами в нём являются многочлены $0, \alpha_1, \alpha_2, ..., \alpha_{2^m-1}$, и умножение производится по модулю того самого многочлена $\pi(x)$. Пусть $\alpha_i = a^i_{m-1}x^{m-1} + ... + a^i_0$. Обозначим

$$\gamma_i = \begin{pmatrix} a^i_0 \\ \vdots \\ a^i_{m-1} \end{pmatrix}$$

– столбец коэффициентов α_i. Для столбцов высоты m определим произведение, как столбец, соответствующий многочлену, равному произведению соответствующих многочленов из $GF(2^m)$. Введём в рассмотрение матрицу A с коэффициентами из $GF(2^m)$ (как отмечалось выше, $n = 2^m - 1$):

$$A = \left.\begin{pmatrix} \alpha_1 & \dots & \alpha_n \\ \alpha_1^3 & \dots & \alpha_n^3 \\ \vdots & & \vdots \\ \alpha_1^{2t-1} & \dots & \alpha_n^{2t-1} \end{pmatrix}\right\} t$$

и соответствующую ей матрицу H с коэффициентами из $\mathbb{Z}_2$:

$$H = \left.\begin{pmatrix} \gamma_1 & \dots & \gamma_n \\ \gamma_1^3 & \dots & \gamma_n^3 \\ \vdots & & \vdots \\ \gamma_1^{2t-1} & \dots & \gamma_n^{2t-1} \end{pmatrix}\right\} tm$$

Перед доказательством следующего утверждения отметим, что $GF(2^m)$ – поле характеристики 2 (очевидно). Отсюда следует, что для любых $x_1, .., x_s \in GF(2^m)$ справедливо равенство:

$$(x_1 + ... + x_s)^2 = x_1^2 + ... + x_s^2.$$

По индукции легко показать справедливость следующего равенства:

$$(x_1 + ... + x_s)^{2^u} = x_1^{2^u} + ... + x_s^{2^u}. \tag{1}$$

Утверждение. *В матрице H любые $2t$ столбцов линейно независимы.*

Доказательство. Допустим противное. Т.е. найдутся $l \leqslant 2t$ столбцов с номерами $i_1, ..., i_l$, такие что $h_{i_1} + ... + h_{i_l} = 0$, где $h_i, i = 1, ..., n$ – столбцы матрицы H. Это означает одновременное выполнение следующих равенств:

$$\begin{cases} \gamma_{i_1} & + \ldots + & \gamma_{i_l} & = 0 \\ \gamma_{i_1}^3 & + \ldots + & \gamma_{i_l}^3 & = 0 \\ \vdots & & \vdots & \\ \gamma_{i_1}^{2t-1} & + \ldots + & \gamma_{i_l}^{2t-1} & = 0 \end{cases}$$

что в свою очередь означает

$$\begin{cases} \alpha_{i_1} & + \ldots + & \alpha_{i_l} & = 0 \\ \alpha_{i_1}^3 & + \ldots + & \alpha_{i_l}^3 & = 0 \\ \vdots & & \vdots & \\ \alpha_{i_1}^{2t-1} & + \ldots + & \alpha_{i_l}^{2t-1} & = 0 \end{cases} \tag{2}$$

Покажем, что для любого чётного $2 \leqslant q \leqslant 2t$ справедливо:

$$\alpha_{i_1}^q + ... + \alpha_{i_l}^q = 0. \tag{3}$$

Действительно, q можно представить в виде: $q = 2^u(2v - 1)$, $v \leqslant t$. Поэтому:

$$\alpha_{i_1}^q + ... + \alpha_{i_l}^q = \alpha_{i_1}^{2^u(2v-1)} + ... + \alpha_{i_l}^{2^u(2v-1)} \overset{(1)}{=} \left(\alpha_{i_1}^{(2v-1)} + ... + \alpha_{i_l}^{(2v-1)}\right)^{2^u} = 0,$$

т.к.

$$\alpha_{i_1}^{(2v-1)} + ... + \alpha_{i_l}^{(2v-1)} = 0.$$

Таким образом, из (2) и (3) получаем для любого $1 \leqslant q \leqslant 2t$

$$\alpha_{i_1}^q + ... + \alpha_{i_l}^q = 0. \tag{4}$$

Рассмотрим определитель

$$W = \begin{vmatrix} \alpha_{i_1} & \ldots & \alpha_{i_l} \\ \alpha_{i_1}^2 & \ldots & \alpha_{i_l}^2 \\ \vdots & & \vdots \\ \alpha_{i_1}^{i_l} & \ldots & \alpha_{i_l}^{i_l} \end{vmatrix} = \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_l} \begin{vmatrix} 1 & \ldots & 1 \\ \alpha_{i_1} & \ldots & \alpha_{i_l} \\ \vdots & & \vdots \\ \alpha_{i_1}^{i_l-1} & \ldots & \alpha_{i_l}^{i_l-1} \end{vmatrix} \neq 0,$$

как определитель Вандермонда, учитывая, что $\alpha_i \neq \alpha_j$, при $i \neq j$, и $\alpha_i \neq 0$ для любого $1 \leqslant i \leqslant n$. Получаем противоречие с (4). Утверждение доказано.

Из Утверждения следует, что матрица H задаёт линейный $[n, k, d]$ - код, со следующими параметрами

$$n = 2^m - 1,$$

$$k \geqslant n - tm,$$

$$d \geqslant 2t + 1.$$

Алгоритм распознавания ошибок в общем случае очень не простой. Мы рассмотрим его для $t = 2$.

В этом алгоритме априори предполагается, что в результате передачи сообщения не может произойти более двух ошибок. Пусть исходное сообщение $x \in KerA$ (важно понимать, что хотя в теории мы оперируем с матрицей A, на деле все вычисления ведутся с матрицей H) после прохождения по каналу связи переходит в сообщение y. Вычислим *синдром:*

$$S = Ay = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}, \ z_1, z_2 \in GF(4)$$

Ясно, что по предположению на количество ошибок $x = y$ равносильно $S = \binom{0}{0}$. Пусть теперь произошла одна ошибка в разряде i, т.е. $y = x + e_i$ (e_i – базисный вектор $\mathbb{Z}_2^n$ с единицей только на i-м месте). Тогда

$$S = A(x + e_i) = Ae_i = \left(\alpha_i \alpha_i^3\right).$$

Т.е. $z_1 = \alpha_i, \ z_2 = \alpha_i^3$ – по известному z_1 находим i – номер разряда и делаем вывод, что ошибка в нём. Пусть теперь произошло 2 ошибки: в разрядах i и j :

$$S = A(x + e_i + e_j) = \begin{pmatrix} \alpha_i + \alpha_j \\ \alpha_i^3 + \alpha_j^3 \end{pmatrix}$$

Для определения α_i и α_j требуется решить систему алгебраических уравнений

$$\begin{cases} \alpha_i + \alpha_j & = & z_1 \\ \alpha_i^3 + \alpha_j^3 & = & z_2 \end{cases} \tag{5}$$

в $GF(4)$. Решение алгебраических уравнений в конечных полях – непростая наука. В связи с этим возникают трудности при распознавании ошибок при больших t. В случае системы (5) поступаем следующим образом:

$$z_2 = \alpha_i^3 + \alpha_j^3 = (\alpha_i + \alpha_j)(\alpha_i^2 + \alpha_i\alpha_j + \alpha_j^2) = z_1(z_1^2 + \alpha_i\alpha_j)$$

– при переходах воспользовались тем, что $GF(4)$ – поле характеристики 2. Имеем:

$$\begin{cases} \alpha_i + \alpha_j & = & z_1 \\ \alpha_i\alpha_j & = & z_1^2 + z_2/z_1 \end{cases} \tag{6}$$

Т.е. α_i, α_j – два различных корня уравнения

$$x^2 + z_1 x + (z_1^2 + z_2/z_1) = 0 \tag{7}$$

над $GF(4)$. Уравнение (7) решается стандартным способом.

Выпишем окончательный **алгоритм:**

1. Вычисляем синдром $S = Ay = \begin{pmatrix} z_1 \\ z_2 \end{pmatrix}$.
2. Если $z_1 = z_2 = 0$ – делаем вывод об отсутствии ошибок.
3. Если $z_1 \neq 0, \ z_2 = z_1^3 \Rightarrow$ произошла одна ошибка в разряде i, где $i : \alpha_i = z_1$.
4. Если $z_1 \neq 0, \ z_2 \neq z_1^3 \Rightarrow$ находим α_i, α_j – различные корни уравнения (7), делаем вывод, что ошибки произошли в разрядах с номерами i и j.

В предположении, что более 2-х ошибок произойти не может, алгоритм всегда срабатывает. Если же, допустить, что произошло большее количество ошибок, то действуя по этому алгоритму, мы либо не попадём ни в один пункт, либо убедимся в отсутствии корней уравнения (7), либо обработаем один из вариантов 2 – 4, но результат не будет иметь никакого отношения к действительно произошедшим ошибкам.

Приведём алгоритм построения матрицы $H_{r\times n}$ такой что любые её $(d-1)$ столбцов линейно независимы. Для этого выберем первый столбец $h_1 \neq 0$. На $i+1$-м шаге имеем i линейно независимых столбцов $\{h_1, ..., h_i\}$ и выбираем произвольный ненулевой столбец h_{i+1} отличающийся от любой линейной комбинации (по модулю 2) ранее выбранных столбцов. Ясно, что ввиду линейной независимости $\{h_1, ..., h_i\}$ все линейные комбинации вида $h_{i_1} + ...h_{i_p},\ p = 1, ..., d-2$ различны. Поэтому мы можем выбрать h_{i+1} если, и только если

$$C_i^1 + ... + C_i^{d-2} < 2^r - 1$$

Из этих рассуждений следует следующая

Теорема (Граница Варшамова-Гильберта) *Если выполняется неравенство*

$$1 + C_{n-1}^1 + C_{n-1}^2 + ... + C_{n-1}^{d'-2} < 2^r,$$

то существует V – линейный $[n,k,d]$-код, для параметров которого справедливо:

$$k \geqslant n - r,\ d(V) \geqslant d'.$$

Пусть V_n^t – код со словами длины n, устойчивый к t ошибкам (см. предыдущую лекцию). Пусть

$$M(n,t) = \max_{V_n^t} |V_n^t|$$

Ранее нами была выведена оценка, называемая границей Хэминга, которая даёт

$$\log_2 M(n,t) \leqslant n - t\log_2 n + c.$$

Если же V – БЧХ код с параметрами $[n,k,d]$, то

$$\log_2 |V| = k \geqslant n - tm = n - t\log_2 n + c'.$$

Т.е. ассимптотически по n коды БЧХ являются максимальными по мощности.

Часть III

Булевы функции.

Лекция 10.

Введем несколько определений. Пусть $B=\{0,1\}$, B^n — множество всевозможных наборов из нулей и единиц длинны n. X — алфавит переменных. Будем считать его счетным множеством. $f(x_1,\ldots,x_n)\in B$ — функция отображающая B^n в B.

Определение. Переменная x_1 называется существенной для функции f, если существуют $\alpha_2,\ldots,\alpha_n\in B$ такие, что

$$f(0,\alpha_2,\ldots,\alpha_n)\neq f(1,\alpha_2,\ldots,\alpha_n).$$

В противном случае переменная x_1 называется несущественной.

Мы будем считать равными две функции, если они отличаются только несущественными переменными. Поясним это определение. Пусть функция f зависит от переменных $x_1,\ldots,x_n$, функция g — от переменных $y_1,\ldots,y_m$. Причем для функции f существенными являются переменные $x_{i_1},\ldots,x_{i_k},\quad i_1\leqslant\ldots\leqslant i_k$, а для функции g — $y_{j_1},\ldots,y_{j_k},\quad j_1\leqslant\ldots\leqslant j_k$. Тогда будем считать, что $f=g$, если для любых наборов $x_1,\ldots,x_n,y_1,\ldots,y_m$ таких, что $x_{i_1}=y_{j_1},\ldots,\ x_{i_k}=y_{j_k}$

$$f(x_1,\ldots,x_n)=g(y_1,\ldots,y_m).$$

Обозначим множество всех булевых функций P_2. Пусть $R\subset P_2$. Множество всех булевых функций из R, зависящих от n переменных, обозначим $R(n)$.

Рассмотрим важный вопрос — задание функции в виде формулы над $\Im\subseteq P_2$, $\Im\neq\varnothing$.

Функции из $\Im$, зависящие от n переменных будем обозначать f^n. Итак, введем **определение** формулы.

1) $f^n(x_{i_1},\ldots,x_{i_n})$ называется формулой над $\Im$.
2) $g^m(A_1,\ldots,A_m)$ называется формулой над $\Im$, если $g^m\in\Im$ и $A_1,\ldots,A_m$ — либо формулы над $\Im$, либо переменные из X.
3) Других формул над $\Im$ нет.

Еще один способ задания функций – задание ее значений на всех наборах переменных.

Примеры.

Функции от одной переменной.

x	0	1	x	$\overline{x}$
0	0	1	0	1
1	0	1	1	0

Функции от двух переменных.

xy	$x\vee y$	$x\&y$	$x+y$	$x\to y$
00	0	0	0	1
01	1	0	1	1
10	1	0	1	0
11	1	1	0	1

Замечание. $|P_2(n)|=2^{2^n}$.

Пусть есть система функций $\Im,\Im\neq\varnothing,\Im\subseteq P_2$.

Определение. Будем называть замыканием $\Im$ и обозначать $[\Im]$ множество функций, заданных в виде всевозможных формул над $\Im$.

Определение. Если система $F = [F]$, то она называется замкнутым классом Поста.

Определение. Если $[\Im] = F$, то будем говорить, что система $\Im$ порождает F.

Определение. Если существует система $\Im$ такая, что $[\Im] = F$ и $|\Im| < \infty$, тогда система F называется конечно порожденной.

Мы будем изучать два вопроса.
1. В каком случае система F будет замкнутым классом Поста.
2. Верно ли, что любая система $F \subseteq P_2$ является конечно порожденной.

Для начала установим, является ли P_2 конечно порожденным.

Утверждение. $\forall f \in P_2$, *верно представление*

$$f(x_1, \dots, x_n) = x_1(f(1, x_2, \dots, x_n) + f(0, x_2, \dots, x_n)) + f(0, x_2, \dots, x_n). \tag{1}$$

Доказательство. Подставим набор $(0, x_2, \dots, x_n)$ в формулу (1).

$$f(0, x_2, \dots, x_n) = 0 \cdot (f(1, x_2, \dots, x_n) + f(0, x_2, \dots, x_n)) + f(0, x_2, \dots, x_n) = f(0, x_2, \dots, x_n).$$

Подставим набор $(1, x_2, \dots, x_n)$ в формулу (1).

$$f(1, x_2, \dots, x_n) = 1 \cdot (f(1, x_2, \dots, x_n) + f(0, x_2, \dots, x_n)) + f(0, x_2, \dots, x_n) = f(1, x_2, \dots, x_n).$$

Что и требовалось доказать.

Следствие 1. Система $\{xy, x + y, 0, 1\}$ порождает P_2.

Следствие 2. Представление булевой функции в виде полинома Жегалкина.

$$f(x_1 \dots, x_n) = \sum_{i=1}^{2^n} c_i K_i,$$

где $c_i \in B$, K_i — всевозможные элементарные конъюнкции.

Следует пояснить термин элементарная конъюнкция. Пусть нам задан набор переменных $x_1, \dots, x_n$. Элементарной конъюнкцией называется функция

$$f(x_{i_1}, \dots, x_{i_n}) = x_{i_1} \cdot \ldots \cdot x_{i_k},$$

при $k \geqslant 1$, и функция — тождественная единица. Тогда всего элементарных конъюнкций будет

$$1 + C_n^1 + \ldots + C_n^n = 2^n.$$

Теорема. *(Жегалкин) Любая функция $f \in P_2$ единственным образом представляется в виде полинома Жегалкина.*

<u>**Пример.**</u> $f(x, y) = x \vee y$.

$$x \vee y = f(x, y) = x(f(1, y) + f(0, y)) + f(0, y) = x(1 + y) + y = xy + x + y.$$

Определение. Система $\Im$ называется полной, если $[\Im] = P_2$.

Мы уже доказали, что система $\{xy, x + y, 0, 1\}$ полна. Теперь, нам интересно — будет ли полна какая-нибудь другая система? Изложим метод <u>*сведения*</u> , которой может дать ответ на наш вопрос.

Пусть система $\Im = \{f_1, \ldots, f_n\}$ является полной, и задана система $\beth = \{g_1, \ldots, g_k\}$. Если

1) функции $f_1, \ldots, f_n$ выражаются через функции $g_1, \ldots, g_k$,

2) все функции g_i принадлежат замыканию системы $\Im$,

то система $\beth$ полна.

<u>**Пример.**</u> Покажем, что система $\{xy, \overline{x}\}$ является полной. Проверим первый пункт.

$$x + y = \overline{\overline{\overline{x}y} \cdot \overline{x\overline{y}}},$$

$$0 = x\overline{x},\ 1 = \overline{x\overline{x}}.$$

Заметим, что $\overline{x} = x + 1 \in [\{xy, x + y, 0, 1\}]$. Значит выполняется второй пункт. Следовательно, система $\{xy, \overline{x}\}$ полна.

Определение. Множество линейных функций называется множество следующего вида $L = \{f(x_1, \ldots, x_n) = c_0 + c_1x_1 + \ldots + c_nx_n, c_i \in \{0, 1\}, n \geqslant 1\}$

Перечислим свойства множества L:

1. $[L] = L$.
2. Функции $0, 1, x, x + y, x + 1 \in L$, а функция $xy \notin L$.
3. Если функция $f(x_1, \ldots, x_n)$ существенно зависит от всех своих переменных, то она имеет следующий вид

$$f(x_1, \ldots, x_n) = c_0 + x_1 + \ldots + x_n$$

Следствие 3. $[\{0, 1, x + y\}] = L$.

Пусть $F \subseteq P_2$. Введем следующее обозначение. У функции, принадлежащей P_2, но не принадлежащей системе F, будем приписывать нижний индекс F. Т.е. $f_F(x_1, \ldots, x_n) \in P_2$, и $f_F(x_1, \ldots, x_n) \notin F$.

Лемма 1. *Пусть нам задана функция $f_L(x_1, \ldots, x_n), n \geqslant 2$. Тогда подстановкой 0 и функции вида x можно получить $g_L(x, y)$.*

Доказательство. Рассмотрим представление функции $f_L(x_1, \ldots, x_n)$ в виде полинома Жегалкина. Возьмем элементарную конъюнкцию, в которой количество переменных есть число $k \geqslant 2$. Поскольку функция нелинейная, то ясно, что такая конъюнкция существует. Без ограничения общности можно считать, что эта конъюнкция есть $x_1x_2 \cdot \ldots \cdot x_k$. Тогда

$$f_L(x, \underbrace{y, \ldots, y}_{k-1}, 0, \ldots, 0) = g(x, y) = xy + ax + by + c,$$

так как $y \cdot y = y$. Что и требовалось доказать.

Следствие 4. $xy \in [\{f_L, 0, \overline{x}\}]$

Доказательство. Применяя лемму получаем функцию $g_L(x, y) = xy + ax + by + c$

$$g_L(b + x, a + y) = xy + xa + by + ba + ax + ab + by + ba + c = xy + (c + ab).$$

Если $c + ab \neq 0$, то применим формулу $\overline{x} = x + 1$. Следствие доказано.

Введем новые обозначения.

$$K = \{f(x_1, \ldots, x_n) = c_0(c_1 \vee x_1) \cdot \ldots \cdot (c_n \vee x_n), c_i \in \{0, 1\}, i = 1 \ldots n, n \geqslant 1\}$$

Свойства системы функций K:

1. $[K] = K$.
2. $0, 1, x, xy \in K,\ x \vee y \notin K$.

3. $[\{0,1,xy\}] = K$.

$$D = \{f(x_1,\ldots,x_n) = c_0 \vee (c_1x_1) \vee \ldots \vee (c_nx_n), c_i \in \{0,1\}, i = 1\ldots n, n \geqslant 1\}$$

Свойства системы функций D:
1. $[D] = D$.
2. $0, 1, x, x \vee y \in D,\ xy \notin D$.
3. $[\{0,1,x\vee y\}] = D$.

Упражнение. Проверить свойства для систем K и D.

Введем определения монотонных функций. Для этого зададим частичный порядок множества B^n. Пусть $\alpha = (\alpha_1,\ldots,\alpha_n),\ \beta = (\beta_1,\ldots,\beta_n) \in B^n$. Тогда $\alpha \leqslant \beta$, если $\alpha_1 \leqslant \beta_1,\ldots,\alpha_n \leqslant \beta_n$.
Отметим, что не все наборы сравнимы. Например, наборы $(0,1)$ и $(1,0)$.

Определение. Функция f называется монотонной, если $\forall \alpha,\beta \in B^n$ таких, что $\alpha \leqslant \beta$, выполнено неравенство $f(\alpha) \leqslant f(\beta)$.
Множество всех монотонных функций обозначается M.
Свойства множества монотонных функций:
1. $[M] = M$.
2. $0, 1, x, x\vee y, xy \in M,\ x+1, x \to y, x+y \notin M$.
3. $[\{0,1,x\vee y, xy\}] = M$.

Доказательство. Для любой функции из M справедливо представление

$$f(x_1,\ldots,x_n) = x_1 f(1,x_2,\ldots,x_n) \vee f(0,x_2,\ldots,x_n).$$

Чтобы доказать его проверим значения правой и левой частей на наборах $(0,x_2,\ldots,x_n)$ и $(1,x_2,\ldots,x_n)$. При $x_1 = 0$

$$0f(1,x_2,\ldots,x_n) \vee f(0,x_2,\ldots,x_n) = f(0,x_2,\ldots,x_n).$$

При $x_1 = 1$

$$1f(1,x_2,\ldots,x_n) \vee f(0,x_2,\ldots,x_n) = f(1,x_2,\ldots,x_n) \vee f(0,x_2,\ldots,x_n) = f(1,x_2,\ldots,x_n)$$

в силу монотонности f. Это представление и доказывает данное свойство M.

Лемма 2. *Пусть заданы функции $f_K, f_D \in M$. Тогда $x \vee y \in [\{1, f_K\}]$, $xy \in [\{0, f_D\}]$.*

Доказательство. Пусть у функции $f_K(x_1,\ldots,x_n) \in M$ все переменные существенные. Тогда существует набор, содержащий ровно один ноль(без ограничения общности будем считать, что это набор $(0,1,\ldots,1)$) такой, что значение функции на нем равно единице. Если это не так, тогда

$$f_K(0,1,\ldots,1) = f_K(1,0,\ldots,1) = \ldots = f_K(1,1,\ldots,0) = 0.$$

А, значит, в силу монотонности f_K, либо $f_K = x_1 \cdot \ldots \cdot x_n$, либо $f_K = 0$. В обоих случаях получаем противоречие с тем, что $f_K \notin K$. Далее, поскольку переменная x_1 существенная, то существует такой набор $\alpha_2,\ldots,\alpha_n \in \{0,1\}$, что

$$0 = f_K(0,\alpha_2,\ldots,\alpha_n) \neq f_K(1,\alpha_2,\ldots,\alpha_n) = 1.$$

Причем $(\alpha_2,\ldots,\alpha_n) \neq (1,1,\ldots,1)$. Без ограничения общности будем считать, что $(\alpha_2,\ldots,\alpha_n) = (\underbrace{0,\ldots,0}_{k\geqslant 1},1,\ldots,1)$. Отсюда, легко следует равенство

$$x \vee y = f_K(x,\underbrace{y,\ldots,y}_{k},1,\ldots,1).$$

Чтобы доказать его, нужно подставить всевозможные значения переменных x и y и убедиться, что равенство действительно выполняется.

Аналогичным образом доказывается утверждение о принадлежности конъюнкции замыканию системы $\{0, f_D\}$. Лемма доказана.

Теорема 1.1 *Пусть F — замкнутый класс Поста, $0, 1 \in F$. Тогда класс F является конечно порожденным.*

Доказательство. Доказательство представляет собой последовательное рассмотрения всевозможных случаев.

1. Любая функция $f \in F$ не имеет существенных переменных. Тогда $F = [\{0, 1\}]$. Будем обозначать этот класс C.

2. $F \nsubseteq C$, и любая функция из F имеет не более одной существенной переменной.

   а) $F \nsubseteq M$. Тогда $F = [\{0, 1, \overline{x}\}]$. Будем обозначать этот класс U.

   б) $F \subseteq M$. Тогда $F = [\{0, 1, x\}] = U \bigcap M = UM$.

3. $F \nsubseteq U$.

   а) $F \subseteq K$. Тогда $F = [\{0, 1, xy\}]$.

   б) $F \subseteq D$. Тогда $F = [\{0, 1, x \vee y\}]$.

   в) $F \subseteq L$. Тогда $F = [\{0, 1, x + y\}]$.

   Пункты а)-в) следуют из соответствующих свойств классов K, D, L.

4. $F \nsubseteq K \bigcup D \bigcup L, F \subseteq M$. Тогда существуют функции $f_K, f_D, f_L \in F$. Следовательно, $x \vee y, xy \in [\{0, 1, f_K, f_D\}]$. Значит, $F = [\{0, 1, x \vee y, xy\}] = M$.

5. $F \nsubseteq K \bigcup D \bigcup L \bigcup M$. Т.е. существует функция $f_M(x_1, \ldots, x_n)$. Пусть все её переменные существенные. Поскольку она не является монотонной, то существуют наборы $\alpha, \beta \in B^n$ такие, что $\alpha \neq \beta, \alpha \leqslant \beta$, и $f_M(\alpha) > f_M(\beta)$. При этом, так как $\alpha \neq \beta$, то существует такое i, что $\alpha_i < \beta_i$. Следовательно, если в качестве аргумента функции взять набор $(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_{i+1}, \ldots, \alpha_n)$, то получим функцию уже от одной переменной $g(x)$ равную $\overline{x}$. Тем самым мы получили, что $\overline{x} \in [\{0, 1, f_M\}]$. Пользуясь следствием 4 получаем, что $xy \in [\{0, 1, f_L, \overline{x}\}]$. Система $\{0, 1, \overline{x}, xy\}$ порождает P_2.

Теорема доказана.

Следствие 5. Классы Поста, содержащие 0 и 1, исчерпываются следующим списком

$$P_2,\ M,\ L,\ K,\ D,\ U,\ UM,\ C.$$

Лекция 11.

Напомним, что на прошлой лекции мы получили следующие выражение произвольной монотонной функции. $f \in M$, тогда

$$f(x_1, \ldots, x_n) = x_1 f(1, x_2, \ldots, x_n) \vee f(0, x_2, \ldots, x_n).$$

Следствие 1. *Если* $f \in M,\ f \not\equiv 0, 1$. *Тогда* $f \in [\{x \vee y, xy\}]$.

Кроме того, на прошлой лекции мы доказали следующую лемму.

Лемма 1. *Пусть функции* $f_K, f_D \in M$. *Тогда* $x \vee y \in [\{1, f_K\}],\ xy \in [\{0, f_D\}]$.

Теперь выясним в каких случаях можно говорить, что $f \in [\Im]$.

Лемма 2. *Пусть* $\Im \subseteq P_2,\ x \vee y \in [\Im]$. *Если* $f \in [\Im \cup \{0\}],\ g \in [\Im]$ *и* $g \leqslant f$, *то* $f \in [\Im]$.
Доказательство.
Пусть формула Φ задает функцию f над $\Im \cup \{0\}$. Заменим в формуле Φ ноль на переменную y, и обозначим ее Φ'. Формула Φ' задает некоторую функцию $h(y, x_1, \ldots, x_n)$ над $\Im$. При этом

$$h(0, x_1, \ldots, x_n) = f(x_1, \ldots, x_n). \tag{1}$$

Функция f будет выражаться следующим образом

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) \vee h(g(x_1, \ldots, x_n), x_1, \ldots, x_n) \tag{2}$$

Пусть α произвольный набор из B^n. Если $g(\alpha) = 0$, то равенство (2) выполнено в силу (1). Пусть $g(\alpha) = 1$, тогда, так как $g \leqslant f$, $f(\alpha) = 1$ и, следовательно, равенство (2) выполнено на всех наборов из B^n. Значит,

$$f \in [\{g, x \vee y, h\}] \subseteq [\Im].$$

Лемма доказана.

Определение. Функция $f(x_1, \ldots, x_n)$ удовлетворяет условию 0^∞, если найдется такое i, что $1 \leqslant i \leqslant n$ и $f(x_1, \ldots, x_n) \geqslant x_i$.

Обозначим через 0^∞ множество всех таких функций. Перечислим свойства множества 0^∞.
1. $[0^\infty] = 0^\infty$.
2. $1, x, x \vee y, x \vee yz, x \to y = \overline{x} \vee y \in 0^\infty$, $0, \overline{x}, xy \notin 0^\infty$.
3. $[\{x \to y\}] = 0^\infty$.
Докажем последнее свойство используя лемму 2.
$x \vee y \in [\{x \to y\}]$, т. к. $(y \to x) \to x = x \vee \overline{(x \vee \overline{y})} = x \vee y$.
Поскольку $x \to 0 = \overline{x}$, то $[\{x \to y, 0\}] = P_2$. (система $\{\overline{x}, x \vee y\}$ полна)
Если $f \in 0^\infty$,то по определению существует такое x_i, что $f \geqslant x_i$. Ясно, что $x_i \in [\{x \to y\}]$, а, значит, по лемме 2, $f \in 0^\infty$.

Введем функцию $\omega(x, y, z) = x \vee yz$. Ясно, что $\omega \in 0^\infty \bigcap M$.

Утверждение 1. *Если* $f(x_1, \ldots, x_n) \in 0^\infty \bigcap M$ *и* $f \not\equiv 1$, *то* $f \in [\{\omega\}]$.
Доказательство. Пусть f произвольная монотонная функция из 0^∞, $f \not\equiv 1$. Тогда в силу того, что любая монотонная функция отличная от константы ($0 \notin 0^\infty$) принадлежит $[\{x \vee y, xy\}]$, то $f \in [\{\omega, 0\}]$. Кроме того, $x_i \leqslant f$ при некотором i и $x_i \in [\{\omega\}]$, а также $x \vee y \in [\{\omega\}]$. Поэтому по лемме 2 $f \in [\{\omega\}]$. Что и требовалось доказать.

Утверждение 2. *Если функции* $f_K, f_D \in M$, *то* $\omega \in [\{1, f_K, f_D\}]$.
Доказательство. На прошлой лекции мы доказали, что если функции $f_D, f_K \in M$, то $x \vee y, xy \in [\{0, 1, f_K, f_D\}]$. Отсюда следует, что $\omega \in [\{0, 1, f_K, f_D\}]$, кроме того, $x, x \vee y \in [\{1, f_K, f_D\}], x \leqslant \omega$, а значит, в силу леммы 2 $\omega \in [\{1, f_K, f_D\}]$. Утверждение доказано.

Введем функцию $d_p(x_1, \ldots, x_p) = \bigvee\limits_{i<j} x_i x_j, p \geqslant 2$

Перечислим свойства функции d_p.

1) $d_p(1,0,\ldots,0) = \ldots = d_p(0,\ldots,0,1) = 0$,
$d_p(0,\ldots,0,\overset{i}{1},0,\ldots,0,\overset{j}{1},0,\ldots,0) = 1$ для любых $i,j,\ i \neq j$.

2) $d_p \notin 0^\infty$.

3) $d_p(x_1,\ldots,x_p) = x_1(x_2 \vee \ldots \vee x_p) \vee d_{p-1}(x_2,\ldots,x_p)$, при $p > 2$.

4) $d_{p+1}(x_1,\ldots,x_{p+1}) > d_p(x_1,\ldots,x_p)$ (следует из свойства 3).

5) $\omega \in [\{1,d_3\}]$; если $p > 3$, то $\omega \in [\{d_p\}]$ (т. к. $d_p(x,\ldots,x,y,z) = x \vee yz = \omega$).

6) $d_3(x_1,x_2,x_3) = x_1x_2 \vee x_1x_3 \vee x_2x_3$. $d_3 \notin K, D, d_3 \in M$.

Утверждение 3. *При всех $p \geqslant 2$ справедливо следующее соотношение*

$$[\{\omega\}] \subset [\{\omega, d_{p+1}\}] \subseteq [\{\omega, d_p\}].$$

Доказательство. Из свойства 3) следует, что при $p \geqslant 2 \quad d_{p+1} \in [\{\omega, d_p\}]$. Из свойства 2) следует, что $[\{\omega\}] \subset [\{\omega, d_{p+1}\}]$.

Упражнение. Доказать, что $[\{\omega, d_{p+1}\}] \subset [\{\omega, d_p\}]$.
(Указание. Говорят, что функция удовлетворяет условию 0^μ, если любые μ наборов ($\mu \geqslant 2$), на которых функция равна 0, имеют общую нулевую компоненту. Пусть 0^μ – множество всех функций, удовлетворяющих условию 0^μ, $\mu = 2,3,\ldots,\infty$. Классы 0^μ, $\mu = 2,3,\ldots,\infty$ являются замкнутыми, и выполнено соотношение $0^\infty \subset \ldots \subset 0^\mu \subset \ldots \subset 0^2$. И, наконец, $d_{p+1} \in 0^p$, но $d_p \notin 0^\infty$.)

Пусть задана функция $f(x_1,\ldots,x_n) \in M, n \geqslant 2$. Определим функции f^i_j.

$$f^i_j(x_1,\ldots,x_{j-1},x_{j+1},\ldots,x_n) = f(x_1,\ldots,x_{j-1},x_i,x_{j+1},\ldots,x_n),\ i,j = 1,\ldots,n, i \neq j.$$

Перечислим свойства этих функций.
1) $f^i_j \leqslant x_i \vee f$. Если $x_i = 1$, то равенство, очевидно, выполняется. Пусть $x_i = 0$. Неравенство

$$f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_{j-1},0,x_{j+1},\ldots,x_n) \leqslant$$

$$\leqslant f(x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_{j-1},x_j,x_{j+1},\ldots,x_n)$$

выполняется в силу монотонности функции f.
2) $x_j f^i_j \leqslant f$. Проверяется аналогично.

Введем несколько обозначений. Пусть $A_k(f)$ множество функций вида $g(x_{i_1},\ldots,x_{i_k})$, $x_{i_1},\ldots,x_{i_k} \subseteq \{x_1,\ldots,x_n\}$, $i_j \neq i_l$, при $j \neq l$, полученных из f отождествлением переменных.
В частности, $A_{n-1}(f) = \{f^i_j, i,j = \overline{1..n}\}$.
Пусть $\Im_f = \{\omega, d_n\} \cup A_{n-1}(f)$.

Лемма 3. *Если $f(x_1,\ldots,x_n)$ монотонная функция и $n \geqslant 2$. Тогда f принадлежит $[\{\Im_f\}]$.*
Доказательство. Если $f \equiv const$, то утверждение леммы очевидно. Если $f \not\equiv const$ и $f \in 0^\infty$, то по ранее доказанному утверждению $f \in [\{\omega\}]$.
Пусть теперь $f \notin 0^\infty, n \geqslant 2, f \not\equiv const$. Докажем по индукции. При $n = 2$ $d_2 = x_1x_2$,

$$f \in [\{x \vee y, xy\}] \subseteq [\{\omega, d_2\}].$$

Предположим, что утверждение леммы справедлива для всех $k < n$. Докажем, что она верна для любой монотонной функции f, зависящей от n переменных.

Введем функцию $g := f(0,x_2,\ldots,x_n)$. Если $g \in 0^\infty$, то т.к. $f \geqslant g$, $f \in 0^\infty$. Чего не может быть по предположению. Следовательно, $g \notin 0^\infty$. Значит $g \not\equiv 1$. Пусть $g \equiv 0$. Тогда справедливо выражение

$$f(x_1,x_2,\ldots,x_n) = x_1 f(1,x_2,\ldots,x_n).$$

И поэтому $f(x, y, \dots, y) = xy$, т.к. $f(1, 0, \dots, 0) = 0$ (если $f(1, 0, \dots, 0) = 1$, то в силу монотонности $f \in 0^\infty$).

Ясно, что $xy \in [\Im_f]$, и по следствию 1 выполнено утверждение леммы.

Поэтому осталось рассмотреть случай, когда $g \notin 0^\infty$, $g \not\equiv 0, 1$. Поскольку $g \in M$, то по предположению индукции справедливо соотношение

$$g \in [\Im_g] = [\{\omega, d_n - 1\} \cup A_{n-2}(g)].$$

Пусть Φ_g формула над $\Im_g$, задающая функцию g. Сделаем над ней следующее преобразование. Если в формулу Φ_g входит элемент $B = d_{n-1}(B_2, \dots, B_n)$, то заменяем его на новый элемент $B = d_n(y_1, B_2, \dots, B_n)$. Точно так же заменяем элемент $B = g^i_j(B_2, \dots, B_n)$ на новый элемент $B = f^i_j(y_1, B_2, \dots, B_n)$, $i, j = 2, \dots, n$, $i \neq j$. Тем самым получим формулу Φ над $[\Im_f]$, реализующую некоторую функцию $h(y_1, \dots, y_n)$. При этом $h(0, y_2, \dots, y_n) = g(y_2, \dots, y_n)$ и $h(1, 0, \dots, 0) = g(0, \dots, 0) = 0$ (последние равенство легко доказывается по индукции глубины формулы). Из этого следует следующее равенство

$$y_1(y_2 \vee \dots \vee y_n) \vee h(y_1, \dots, y_n) = y_1(y_2 \vee \dots \vee y_n) \vee g(y_2, \dots, y_n). \tag{3}$$

Введем функцию $\phi(y_1, \dots, y_n) := y_1(y_2 \vee \dots \vee y_n) \vee g(y_2, \dots, y_n)$. Из (3) следует, что $\phi \in [\Im_f]$. Покажем, что $\phi(x_1, f^2_1, \dots, f^n_1) \leqslant f$.

$$x_1(f^2_1, \dots, f^n_1) \vee g(f^2_1, \dots, f^n_1) \leqslant f \vee g(x_2 \vee f, \dots, x_n \vee f) \leqslant f.$$

Тем самым мы нашли некоторую функцию $\chi \in [\Im_f]$, т.ч. $\chi \leqslant f$. Очевидно, что $x \vee y \in [\Im_f]$ и $xy \in [\Im_f \cup \{0\}]$ Поэтому по следствия 1 $f \in [\Im_f \cup \{0\}]$. А значит, по лемме 1 $f \in [\Im_f]$.

Что и требовалось доказать.

Пусть $f(x)$ – монотонная функция, $f \in 0^\infty$, $f \not\equiv 0$. Обозначим через F_f множество всех таких функций, которые получаются из f отождествлением переменных (быть, может пустым) и не принадлежат 0^∞, а при всяком отождествлении двух переменных переходят в функции из 0^∞.

Пример. $f(x, y, z) = d_3(x, y, z) = xy \vee xz \vee yz$. Тогда $F_{d_3} = \{d_3\}$.

Если функция $g(x_1, \dots, x_p) \in F_f$, то $g \in M$, и $g \notin 0^\infty$. Следовательно,

$$g(1, 0, \dots, 0) = \dots = g(0, \dots, 0, 1) = 0.$$

Поскольку $g^i_j \in 0^\infty$, то

$$g(0, \dots, 0, \overset{i}{1}, 0, \dots, 0, \overset{j}{1}, 0, \dots, 0) = 1, \quad i, j = 1, \dots, n, \; i \neq j.$$

Значит имеет место следующее

Следствие. *Любая функция g из F_f, существенно зависящая от p переменных, имеет вид $g = d_p$.*

Замечание. Разными отождествлениями можно прийти к разным функциям d_p.

Пусть $p(f)$ минимальное число существенных переменных у функций из F_f. В силу следствия имеем $d_{p(f)} \in [\{f\}]$.

Лемма 4. *Для любой монотонной функции $f \notin 0^\infty$, $f \not\equiv 0$, выполняется соотношение $f \in [\omega, d_{p(f)}]$.*

Доказательство. Из леммы 3

$$f \in [\{\omega, d_n\} \cup A_{n-1}(f)] \subseteq [\{\omega, d_n, d_{n-2}\} \cup A_{n-2}(f)] \subseteq \dots$$
$$\dots \subseteq [\{\omega, d_n, d_{n-1}, \dots, d_{p(f)}\} \cup A_{p(f)-1}] \subseteq [\{\omega, d_n, \dots, d_{p(f)}\}]$$

Последние вложение справедливо в силу того, что $A_{p(f)-1} \subseteq 0^\infty \cap M$.

Ранее мы доказали, что при $p \geqslant 3$ верно соотношение $[\{\omega, d_p\}] \subseteq [\{\omega, d_{p-1}\}]$. Следовательно, $[\{\omega, d_n, \dots, d_{p(f)}\}] \subseteq [\{\omega, d_{p(f)}\}]$.

Лемма доказана.

Лекция 12.

Напомним некоторые обозначения замкнутых классов. $C = \{0, 1\}$, $U = \{0, 1, \overline{x}\}$, $K = \{0, 1, xy\}$, $D = \{0, 1, x \vee y\}$. Кроме того, если функция f не принадлежит системе $\Im$, для краткости мы будем обозначать ее $f_{\Im}$.

Теорема 2.1. *Пусть система $\Im \subseteq M$, $1 \in [\Im]$, $0 \notin [\Im]$. Тогда $F = [\Im]$ является конечно порожденным классом.*

Доказательство проведем рассмотрев всевозможные случаи.

1) Пусть $\Im \subseteq C$, тогда $[\Im] = [\{1\}]$.

2) Пусть $\Im \subseteq U, \Im \nsubseteq C$, тогда $[\Im] = [\{1, x\}] = [\{1, f_C\}]$.

3а) Пусть $\Im \subseteq K, \Im \nsubseteq U \cup C$, тогда $[\Im] = [\{1, xy\}]$.

3б) Пусть $\Im \subseteq D, \Im \nsubseteq U \cup C$, тогда $[\Im] = [\{1, x \vee y\}]$.

4) Пусть $f_K, f_D \in \Im$ и $\Im \subseteq 0^\infty$. Тогда по утверждению 1 лекции 11 следует, что $\Im \subseteq [\{1, \omega\}]$, а из утверждения 2 — $[\{1, \omega\}] \subseteq [\{1, f_k, f_d\}] \subseteq [\Im]$. Тем самым мы получили, что в этом случае $[\Im] = M \cap 0^\infty = [\{1, \omega\}]$.

5) Пусть $f_K, f_D \in \Im$ и $\Im \nsubseteq 0^\infty$. Рассмотрим произвольную функцию f из $\Im$. Если $f \in 0^\infty$, то $f \in [\{1, \omega\}]$. Пусть $f \in 0^\infty$. Тогда по лемме 4 лекции 11 следует, что $f \in [\{1, \omega, d_{p(f)}\}]$. Значит,

$$\Im \subseteq [\{1, \omega\} \cup \{ \bigcup_{\substack{f \in \Im, \\ f \notin 0^\infty}} d_{p(f)}\}] \subseteq [\{1, \omega, d_{p(\Im)}],$$

где $p(\Im) = \min\limits_{\substack{f \in \Im, \\ f \notin 0^\infty}} p(f)$. Последние вложение справедливо в силу утверждения 3 лекции 11.

Возьмем ту функцию f, для которой $d_{p(f)} = d_{p(\Im)}$. Обозначим её $f^{p(\Im)}$. В предыдущем случае мы показали, что функция ω принадлежит системе $\Im$. Нам осталось показать, что функция $d_{p(\Im)}$ принадлежит системе $\Im$. Но это легко следует из того, что $d_{p(\Im)} \in [\{f^{p(\Im)}\}]$. Таким образом

$$[\{1, \omega, d_{p(\Im)}\}] \subseteq [\{1, f_K, f_D, f^{p(\Im)}\}] \subseteq [\Im].$$

Теорема полностью доказана.

Следствие 1. *Все классы монотонных функций, содержащие 1, и не содержащие 0, исчерпываются следующим списком*

$$[\{1\}], \quad [\{1, x\}], \quad [\{1, x \vee y\}], \quad [\{1, xy\}], \quad M \cap 0^\infty, \quad M \cap T_1 = [\{1, x \vee y, xy\}],$$

$$[\{1, \omega, d_p\}], \quad p = 3, 4, \ldots$$

Упражнение. Доказать, что все эти классы различны.

Принцип двойственности.

Пусть нам задана произвольная функция $f(x_1,\ldots,x_n)\in P_2$.

Определение. *Двойственной* функцией к функции f будем называть функцию

$$f^*(x_1,\ldots,x_n)=\overline{f}(\overline{x}_1,\ldots,\overline{x}_n).$$

Пример. $(x\vee y)^*=\overline{\overline{x}\vee\overline{y}}=xy, \quad (\overline{x})^*=\overline{(\overline{\overline{x}})}=\overline{x}.$

Определение. Если $f(x_1,\ldots,x_n)=f^*(x_1,\ldots,x_n)$, то функция f называется *самодвойственная.*

Обозначим через S множество всех самодвойственных функций.

Утверждение. (Принцип двойственности.) *Пусть* $\Phi(x_1,\ldots,x_n)=f(f_1(x_1,\ldots,x_n),\ldots$ $\ldots,f_m(x_1,\ldots,x_n))$. *Тогда справедливо равенство*

$$\Phi^*(x_1,\ldots,x_n)=f^*(f_1^*(x_1,\ldots,x_n),\ldots,f_m^*(x_1,\ldots,x_n)).$$

Доказательство.

$$\Phi^*(x_1,\ldots,x_n)=\overline{\Phi}(\overline{x}_1,\ldots,\overline{x}_n)=\overline{f}(f_1(\overline{x}_1,\ldots,\overline{x}_n),\ldots,f_m(\overline{x}_1,\ldots,\overline{x}_n))=$$

$$=\overline{f}(\overline{\overline{f}}_1(\overline{x}_1,\ldots,\overline{x}_n),\ldots,\overline{\overline{f}}_m(\overline{x}_1,\ldots,\overline{x}_n))=\overline{f}(\overline{f}_1^*,\ldots,\overline{f}_m^*)=f^*(f_1^*,\ldots,f_m^*).$$

Что и требовалось доказать.

Отметим следующие свойства самодвойственных функций.

1) S – замкнутый класс.
Для проверки замкнутости класса достаточно показать, что любая функция вида

$$f(x_1,\ldots,x_n)=f_0(f_1(x_1,\ldots,x_n),\ldots,f_m(x_1,\ldots,x_n))$$

принадлежит классу, с учетом того, что функции $f_0,f_1,\ldots,f_m$ принадлежат этому классу. Из принципа двойственности следует, что

$$f^*=f_0^*(f_1^*,\ldots,f_m^*)=f_0(f_1,\ldots,f_m)=f.$$

2) $x,\overline{x},d_3\in S,\ \ 1,0,x\vee y,xy,x\to y\notin S.$

3) Если $f(x_1,\ldots,x_n)\in S$, то $f(1,x_2,\ldots,x_n)=f^*(0,x_2,\ldots,x_n)$.

Пример. $f(x,y,z)=d_3(x,y,z)=x(y\vee z)\vee yz.$

$$f(1,y,z)=y\vee z,\quad f(0,y,z)=yz.$$

Пусть нам задан класс F. Класс функций двойственных к функциям из класса F будем обозначать F^*. $F^*=\{f\in P_2\mid f^*\in F\}$.
4) Если $[\Im]=F$, то $[\Im^*]=F^*$ (следует из принципа двойственности).

Множество функций сохраняющих 1 будем обозначать T_1. Множество функций сохраняющих $0-T_0$.
Перечислим свойства классов T_1 и T_0.
1) T_0,T_1 – замкнутые классы.
2) $1,x,x\vee y,xy,x\to y\in T_1,\ \ 0,\overline{x}\notin T_1.\ \ \ 0,x,x\vee y,xy,x+y\in T_0,\ \ 1,x\to y\notin T_0.$
3) $T_0=T_1^*$.
4) $[\{x\to y,xy\}]=T_1$.

Докажем последнее свойство используя лемму 2 из лекции 11. Пусть f произвольная функция из T_1. Ранее мы показали, что $[\{x \to y, 0\}] = P_2$, следовательно $f \in [\{0, x \to y, xy\}]$. Поскольку $(x \to y) \to y = x \vee y$, то $x \vee y \in [\{x \to y, xy\}]$.

Кроме того, легко видеть, что $x_1 x_2 \ldots x_n \leqslant f(x_1, \ldots, x_n)$ и $x_1 x_2 \ldots x_n \in [\{x \to y, xy\}]$. Поэтому применяя лемму 2 из лекции 11 получаем, что $f \in [\{x \to y, xy\}]$.

Из свойства 4) следует, что базис T_0 выражается следующим образом $\{(x \to y)^*, (xy)^*\}$. Следовательно, $[\{x\overline{y}, x \vee y\}] = T_0$.

Следствие 2. *Если функции $f_M, f_L \in T_1$, то $x \to y \in [\{1, f_M, f_L\}]$.*

Доказательство. Поскольку функция $f_M(x_1, \ldots, x_n)$ не является монотонной, то существуют два различных сравнимых набора $\alpha = (\alpha_1, \ldots, \alpha_n)$ и $\beta = (\beta_1, \ldots, \beta_n)$, т.ч. $\alpha > \beta$, и $0 = f(\alpha) < f(\beta) = 1$. Так как набор α строго больше набора β, то существуют такие числа $i_1, \ldots, i_k$, $k \geqslant 1$, что $1 = \alpha_{i_j} > \beta_{i_j} = 0$, $j = 1, \ldots, k$ и $\alpha_i = \beta_i$, если $i \notin \{i_1, \ldots, i_k\}$. Не ограничивая общности считаем, что это первые k чисел наборов α и β. Поэтому справедливо следующее равенство

$$f_M(\underbrace{x, \ldots, x}_{k}, 1, \ldots, 1, \underbrace{0, \ldots, 0}_{\geqslant 1}) = \overline{x}. \tag{1}$$

Количество нулей больше либо равно единицы в силу того, что $f_M \in T_1$. Рассмотрим функцию $g(x, y) = f_M(x, \ldots, x, 1, \ldots, 1, y, \ldots, y)$, полученную с помощью заменой нулей на переменную y в правой части равенства (1). Из определения функции g следует, что $g(1,1) = 1$, $g(1,0) = 0$, $g(0,0) = 1$. Если $g(0,1) = 1$, то $g(x,y) = x \to y = \overline{x} \vee y \in [\{1, f_M\}]$, и тем самым следствие доказано. Пусть $g(0,1) = 0$, тогда $g(x,y) = x + y + 1 \in [\{1, f_M\}]$.

Теперь рассмотрим функцию $f_L(x_1, \ldots, x_n) \in T_1$. Ясно, что $f_L^* \notin L$ и $f_L^* \in T_0$. По лемме 1 лекции 10 существует функция $g_L(x,y) \in [\{0, f_L^*\}]$, при этом $g_L(0,0) = 0$. Пусть $h(x,y) := g_L^*(x,y)$. По свойству 4) $h(x,y) \in [\{1, f_L\}]$, а, так как $g_L^*(x,y) \in T_1$, то $h(1,1) = 1$. Кроме того,

$$h(x,y) \notin L. \tag{2}$$

Далее, разберем случаи, когда функция $h(x,y)$ принимает все возможные значения на наборах $(0,0)$, $(0,1)$, $(1,0)$.

1) Пусть $h(0,0) = 1$. Тогда, если

   а) $h(0,1) = h(1,0) = 0$, то $h = x + y + 1 \in L$. Противоречие с (2).

   б) $h(0,1) = h(1,0) = 1$, то $h \equiv 1 \in L$. Противоречие с (2).

   в) $h(0,1) \neq h(1,0)$, то, либо $h = x \to y$, либо $h = y \to x$,

   и в этом случае следствие доказано.

2) Пусть $h(0,0) = 0$. Тогда, если

   а) $h(0,1) = h(1,0) = 0$, то $h = xy$. И, поскольку $x + y + 1 \in [\{1, f_M\}]$, то $y \to x = xy + y + 1 \in [\{1, f_M, f_L\}]$.

   б) $h(0,1) = h(1,0) = 1$, то $h = x \vee y$. И $x \to y = x \vee y + y + 1 \in [\{1, f_M, f_L\}]$.

   в) $h(0,1) \neq h(1,0)$, то, либо $h = x$, либо $h = y$, и $h \in L$. Противоречие с (2).

Следствие доказано.

Лемма 1. *Для любой функции f из P_2 существует монотонная функция g такая, что $g \leqslant f$ и $g \in [\{1, x \vee y, f\}]$.*

Доказательство. Если функция f сама является монотонной, то утверждение леммы очевидно. Пусть $f \notin M$. Если $n = 1$, то $f(x_1) = \overline{x}_1$, и тогда в качестве функции g можно взять тождественный ноль. Итак, пусть $n \geqslant 2$. Пусть x_1 – переменная, по которой функция f немонотонна. Т.е. существует такой набор $\alpha = (\alpha_2, \ldots, \alpha_n)$, что $f(x_1, \alpha_2, \ldots, \alpha_n) = \overline{x}_1$. Введем множество $R = \{\alpha = (\alpha_2, \ldots, \alpha_n) \mid f(x_1, \alpha_2, \ldots, \alpha_n) = \overline{x}_1\}$. Множество R не пусто. Рассмотрим функцию

$$f_1(x_1, \ldots, x_n) = f(f \vee \chi_R, x_2, \ldots, x_n),$$

где функция $\chi_R(x_2, \ldots, x_n) = \begin{cases} 1, & (x_2, \ldots, x_n) \in R, \\ 0, & \text{иначе.} \end{cases}$

Покажем, что $f_1 \leqslant g$. Рассмотрим произвольный набор $(x_1, \alpha_2, \ldots, \alpha_n)$. Если $\alpha = (\alpha_2, \ldots, \alpha_n) \in R$, то

$$f_1(1, \alpha_2, \ldots, \alpha_n) = f_1(0, \alpha_2, \ldots, \alpha_n) = f(1, \alpha_2, \ldots, \alpha_n) = 0;$$

если же $\alpha \notin R$, то либо $f(0, \alpha) = f(1, \alpha)$, либо $f(x_1, \alpha) = x_1$. В любом случае имеем, что $g(x_1, \alpha) = f(x_1, \alpha)$.

Теперь покажем, что $f_1 \in [\{1, x \vee y, f\}]$. Для этого достаточно показать, что $f \vee \chi_R \in [\{1, x \vee y, f\}]$. В 5-ом пункте теоремы 1.1 из лекции 10 мы доказали, что $\overline{x} \in [\{0, 1, f_M\}]$. Поэтому $f \vee \chi_R \in [\{1, x \vee y, f, 0\}] = P_2$. Кроме того, $f \leqslant f \vee \chi_R$, а значит, в силу леммы 2 из лекции 11 $f \vee \chi_R \in [\{1, x \vee y, f\}]$. Если f_1 немонотонная функция, то применим к ней аналогичное преобразование и т.д. В конце концов получим искомую монотонную функцию $g \in [\{1, x \vee y, f\}],\ g \leqslant f$.

Следствие 3. *Если f принадлежит T_0, то $g \in [\{x \vee y, f\}]$.*

Доказательство. Пусть Φ – формула над $\{1, x \vee y, f\}$, реализующая функцию g и $g \leqslant f$. Заменим всякое вхождение константы 1 в Φ на $x_1 \vee \ldots \vee x_n$. Легко видеть, что полученная формула над $\{x \vee y, f\}$ реализует функцию g.

Теорема 2.2 *Если система $\Im \subseteq P_2$, $1 \in [\Im]$, $0 \notin [\Im]$. Тогда $F = [\Im]$ является конечно порожденным классом.*

Доказательство. Система $\Im \subseteq T_1$, т.к. если существует функция f из $\Im$, не принадлежащая T_1, то $f(1, 1, \ldots, 1) = 0$ и, следовательно, $0 \in [\Im]$, что противоречит условию теоремы. Если $\Im \subseteq M$, то см. теорему 2.1. Итак, существует немонотонная функция f_M из $\Im$.

Проведем доказательство рассмотрев все возможные случаи.

1) Пусть $\Im \subseteq L$, тогда $\Im \notin U$. Кроме того, функции из $\Im$ имеют следующий вид:

$$f(x_1, \ldots, x_n) = \begin{cases} x_1 + \ldots + x_{2k}, & n = 2k, \\ x_1 + \ldots + x_{2k+1}, & n = 2k+1, \end{cases} \qquad n \geqslant 2.$$

Тогда $\Im \subseteq [\{1, x + y + 1\}] \subseteq [\Im]$. В этом случае $[\Im] = [\{1, x + y + 1\}] = L \cap T_1$.

2) $f_M, f_L \in \Im$, $\Im \subseteq 0^\infty$. Тогда в силу того, что $[\{x \to y\}] = 0^\infty$ и следствия 2, справедливы соотношения

$$\Im \subseteq [\{x \to y\}] \subseteq [\{1, f_M, f_L\}] \subseteq [\Im].$$

Откуда следует, что $[\Im] = 0^\infty$.

3) $f_M, f_L \in \Im$, $\Im \nsubseteq 0^\infty$. Пусть f – произвольная функция из $\Im$. Тогда, если $f \in 0^\infty$, то $f \in [\{x \to y\}]$. Пусть $f \notin 0^\infty$, тогда по лемме 1 существует такая монотонная функция g_f, что $g_f \leqslant f$ и $g_f \in [\{1, x \vee y, f\}]$. По лемме 2 из лекции 11 $f \in [\{x \to y, g_f\}]$.

Пусть $\mathfrak{B} = \bigcup\limits_{\substack{f \in \Im, \\ f \notin 0^\infty}} g_f$. Ясно, что $\Im \subseteq [\{x \to y\} \cup \mathfrak{B}]$. Так как $\mathfrak{B}$ состоит только из монотонных функций, то по теореме 2.1 $\mathfrak{B} \subseteq [\{1, \omega, d_{p(\mathfrak{B})}\}] \subseteq [\{1, \omega, g^{p(\mathfrak{B})}\}]$. По определению функции g существует такая функция $\widehat{f}^{p(\mathfrak{B})} \in \Im$, что $g^{p(\mathfrak{B})} \in [\{1, x \vee y, \widehat{f}^{p(\mathfrak{B})}\}]$. А это означает, что $\mathfrak{B} \subseteq [\{1, \omega, x \vee y, \widehat{f}^{p(\mathfrak{B})}\}]$. Отсюда следует, что

$$\Im \subseteq [\{x \to y\} \cup \mathfrak{B}] \subseteq [\{x \to y, d_{p(\mathfrak{B})}\}] \subseteq [\{x \to y, \widehat{f}^{p(\mathfrak{B})}\}] \subseteq [\{1, f_M, f_L, \widehat{f}^{p(\mathfrak{B})}\}] \subseteq [\Im].$$

Таким образом $[\Im] = [\{x \to y, d_{p(\mathfrak{B})}\}]$. Теорема доказана.

Следствие 4. *Все замкнутые классы функций, содержащие немонотонную функцию и 1 и не содержащие 0, исчерпываются следующим списком*

$$L \cap T_1, 0^\infty, T_1 = [\{x \to y, xy\}], [\{x \to y, d_p\}],\ p = 3, 4, \ldots$$

Упражнение Доказать, что все классы различны.

Теорема 3. *Если система $\Im \subseteq P_2$, $0 \in [\Im]$, $1 \notin [\Im]$. Тогда $F = [\Im]$ является конечно порожденным классом.*

Доказательство. Пусть $\mathfrak{B} = \Im^*$. Тогда $1 \in [\mathfrak{B}],\ 0 \notin [\mathfrak{B}]$, и по теореме 2.2 существует такая система $\widehat{\mathfrak{B}}$, что $|\widehat{\mathfrak{B}}| < \infty$ и $[\widehat{\mathfrak{B}}] = F^* = [\Im^*]$. Если положить $\widehat{\Im} = \widehat{\mathfrak{B}}^*$, то система $\widehat{\Im}$ будет конечна и $[\widehat{\Im}] = F$. Теорема доказана.

Следствие 5. *Все замкнутые классы, содержащие 0 и не содержащие 1, будут двойственными к классам, перечисленным в следствиях 1 и 4.*

Теорема 4. *Если система $\Im \subseteq P_2$, $0, 1 \notin [\Im]$. Тогда $F = [\Im]$ является конечно порожденным классом.*

Доказательство. Случай **A**.

Пусть $\Im \subseteq S$ и $[\Im \cup \{1\}] = F_1$. Тогда по теореме 2.2 класс F_1 является конечно порожденным. Т.е. существует система $\mathfrak{B} \subseteq \Im$ такая, что $[\mathfrak{B} \cup \{1\}] = F_1$ и $|\mathfrak{B}| < \infty$.

Докажем, что $[\mathfrak{B}] = F = [\Im]$. Пусть $f(x_1, \ldots, x_n)$ – произвольная функция из $F \subseteq S$. Существует формула Φ над $\mathfrak{B} \cup \{1\}$, реализующая функцию f. Заменяем в ней все вхождения 1 переменной y. Получили формулу Φ' над $\mathfrak{B}$, реализующую функцию $g(y, x_1, \ldots, x_n)$. Ясно, что $g \in S$. Кроме того,

1) $g(0, x_1, \ldots, x_n) = g(1, x_1, \ldots, x_n)$.

2) $g(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$.

А, значит, $g(y, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Т.е. переменная y – несущественная. Тем самым класс $F = [\Im]$ является конечно порожденным.

Случай **B**.

$\Im \nsubseteq S$. Следовательно, существует функция $f_S \in \Im$.

I. Покажем, что $\Im \subseteq T_0 \cap T_1$. Предположим, что это не так. Т.е. существует функция f из $\Im$ такая, что $f(x_1, \ldots, x_n) \notin T_0 \cap T_1$. Рассмотрим функцию $g(x) = f(x, \ldots, x)$. Если $g(x) \equiv 0, g(x) \equiv 1$ или $g(x) = x$, то это противоречит нашему предположению. Значит, $g(x) = \overline{x}$. Далее, существует набор α такой, что $f_S(\alpha_1, \ldots, \alpha_n) = f_S(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = c,\ c \in \{0, 1\}$. Без ограничения общности считаем, что $\alpha = (\underbrace{0, \ldots, 0}_{k}, \underbrace{1, \ldots, 1}_{n-k}),\ k \geqslant 0$.

Тогда $f(\underbrace{x, \ldots, x}_{k}, \underbrace{\overline{x}, \ldots, \overline{x}}_{n-k}) \equiv c \in \Im$. Что противоречит условию теоремы.

Итак, $\Im \subseteq T_0 \cap T_1$.

II. Либо $x \vee y \in [\{f_S\}]$, либо $xy \in [\{f_S\}]$. Поскольку $f_S \notin S$, то существует набор α такой, что $f_S(\alpha_1, \ldots, \alpha_n) = f_S(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = c,\ c \in \{0, 1\}$. Без ограничения общности считаем, что $\alpha = (\underbrace{0, \ldots, 0}_{k}, \underbrace{1, \ldots, 1}_{n-k})$. Но теперь в силу пункта 1 справедливы неравенства $1 \leqslant k \leqslant n - 1$. Рассмотрим функцию $h(x, y) = f_S(\underbrace{x, \ldots, x}_{k}, \underbrace{y, \ldots, y}_{n-k})$. $h(x, y) \in T_0 \cap T_1$, следовательно, $h(0, 0) = 0,\ h(1, 1) = 1$. Кроме того, из определения функции h следует, что $h(1, 0) =$ c, $h(0, 1) =$ c. Если $c = 1$, то $h(x, y) = x \vee y$, если $c = 0$, то $h(x, y) = xy$.

III. 1) $x \vee y \in [\Im]$. По теореме 2.2 класс $F_1 = [\Im \cup \{1\}]$ является конечно порожденным. Т.е. существует система $\mathfrak{B} \subseteq \Im$ такая, что $[\mathfrak{B} \cup \{1\}] = F_1$, и $|\mathfrak{B}| < \infty$. Докажем, что $[\mathfrak{B} \cup \{x \vee y\}] = F = [\Im]$. Пусть $f(x_1, \ldots, x_n)$ произвольная функция из $F \subseteq F_1$. Тогда существует формула Φ над $\mathfrak{B} \cup \{1\}$, реализующая функцию f. Все вхождения 1 в формулу Φ заменяем переменной y. Получили новую формулу Φ' над $\mathfrak{B}$, реализующую функцию $g(y, x_1, \ldots, x_n)$. $g \in [\mathfrak{B}] \subseteq [\Im] \subseteq$

$T_0 \cap T_1$. Следовательно, функция $h(x_1, \ldots, x_n) := g(x_1 \vee \ldots \vee x_n, x_1, \ldots, x_n) \in T_0 \cap T_1$. Кроме того $g(1, x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$. Отсюда, легко следует, что $h \equiv f$. Таким образом, класс F является конечно порожденным.

III. 2) $xy \in [\Im]$. Этот случай можно доказать аналогичным образом или используя принцип двойственности. Докажем, с помощью принципа двойственности. Пусть $\mathfrak{B} = \Im^*$. Тогда $\mathfrak{B} \subseteq T_0 \cap T_1$ и $x \vee y \in [\mathfrak{B}]$. Из предыдущего пункта следует, что существует конечная система $\widehat{\mathfrak{B}}$ такая, что $[\widehat{\mathfrak{B}}] = [\mathfrak{B}]$. Пусть система $\widehat{\Im} = \widehat{\mathfrak{B}}^*$. Тогда $|\widehat{\Im}| < \infty$. Из принципа двойственности следует, что $[\widehat{\Im}] = [\widehat{\mathfrak{B}}^*] = [\mathfrak{B}^*] = [\Im]$.

Теорема полностью доказана.

Завершающей теоремой этой части является

Теорема Поста. *Каждый класс булевых функций является конечно порожденным.*

Часть IV

Конечные автоматы.

Лекция 13.

Детерминированные функции.

Как и при изучении кодов, считаем что имеется два конечных алфавита: $A = \{a_1, ..., a_m\}$ и $B = \{b_1, ..., b_p\}$, причём имеется специальный символ Λ не входящий ни в один из алфавитов – пустое слово. Множеством слов конечной длины над алфавитом $E = \{e_1, ..., e_s\}$ называется

$$E^* = \bigcup_{k \geqslant 1} E^k \cup \{\Lambda\},$$

где

$$E^k = \{e_{i_1}...e_{i_k} | \forall j \ e_{i_j} \in E\}$$

Пусть имеется функция:

$$f : A^* \to B^*$$

Говорим, что f – д.-функция (детерминированная функция), если выполняются свойства

1) f сохраняет длину, т.е. для любого $\alpha \in A^*$ $\lambda(\alpha) = \lambda(f(\alpha))$;

2) для любых слов $\alpha, \beta \in A^*$:

$$\alpha = \alpha(1)...\alpha(k)$$

$$\beta = \beta(1)...\beta(k')$$

$$(\alpha(i), \beta(j) \in A, \forall i = 1, ..., k, \forall j = 1, ..., k'),$$

условие

$$\alpha(1) = \beta(1), ..., \alpha(m) = \beta(m)$$

для некоторого $1 \leqslant m \leqslant \min(k, k')$, влечёт

$$\delta(1) = \gamma(1), ..., \delta(m) = \gamma(m),$$

где $\delta = f(\alpha), \ \gamma = f(\beta)$.

Примеры недетерминированных отображений:

$$A = \{0, 1\}, B = \{0, 1\}$$

1. Не выполняется свойство 1): f – произвольное, такое что $0 \xrightarrow{f} 00$.
2. Не выполняется свойство 2): f – произвольное, такое что

$$00 \xrightarrow{f} 00$$

$$01 \xrightarrow{f} 10$$

Пусть f – д.-функция. Рассмотрим её действие на слове длины k. В силу пункта 1) определения

$$x = x(1)...x(k) \xrightarrow{f} y = y(1)...y(k)$$

При этом, в силу пункта 2)

$$\begin{array}{lll} y(1) & = & f_1(x(1)) \\ y(2) & = & f_2(x(1), x(2)) \\ \vdots & & \\ y(i) & = & f_i(x(1), ..., x(i)) \\ \vdots & & \\ y(k) & = & f_k(x(1), ..., x(k)), \end{array}$$

где f_i – некоторые функции (если $A = B = \{0,1\}$, то $f_i \in P_2$ – булевы функции). Везде далее считаем, что $A = B = \{0,1\}$.

Таким образом функции f однозначно соответствует набор функций $f_i \in P_2, i = 1, 2, ...$ На этом соображении основано представление д.-функции в виде бесконечного двоичного дерева с пометками на рёбрах, это представление называется информационным деревом: см. Рис. 1 (звёздочка отмечает корень дерева).

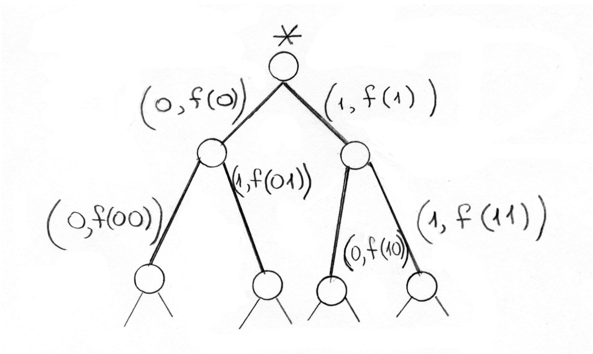

Рис. 1: Информационное дерево.

Пример 1. Рассмотрим пример детерминированной функции, являющийся для нас модельным:

$$f_i(x(1), ..., x(i)) = x(1) + ... + x(i) \pmod 2, \quad i = 1, 2, ...$$

Для неё информационное дерево выглядит следующим образом:

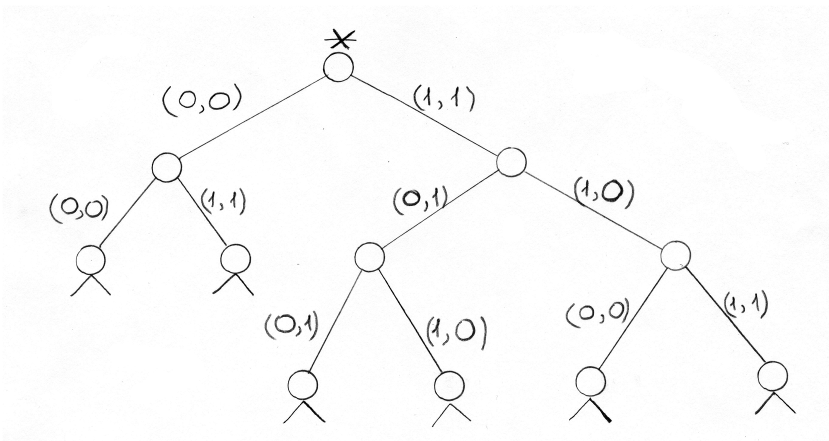

Рис. 2: Информационное дерево к Примеру 1.

Рассмотрим информационное дерево для функции f. Пусть μ_1, μ_2 – две некоторые его вершины, говорим что поддеревья с корнем в этих вершинах T_{μ_1} и T_{μ_1} изоморфны (T_{μ_1} T_{μ_2}), если на соответствующих рёбрах пометки у них одинаковы. Назовём *весом* r д.-функции число попарно неэквивалентных поддеревьев (r может быть равным ∞). Если $r < \infty$ функцию назовём *ограничено детерминированной.*

Пример 2. Построим пример неограничено детерминированной функции ($r = \infty$): пусть $c = c(1)c(2)...c(k)...$ – бесконечная непериодическая последовательность (например 01001000100001...). Определим функцию f:

$$\alpha = \alpha(1)...\alpha(k) \in A^*,\ k \geqslant 1$$

$$f(\alpha) = c(1)...c(k)$$

Очевидно, что f не является ограничено детерминированной.

Из анализа информационного дерева для примера 1 видно, что $r = 2$.

Рассмотрим различные **способы задания ограниченно детерминированной функции:**

1. **Информационное дерево** (подходит и для неограничено детерминированных функций).

2. **Усечённое дерево.** Пусть $\{T_0, T_1, ..., T_{r-1}\}$ – множество попарно неэквивалентных поддеревьев. Пометим все вершины метками $\{\mu_0, \mu_1, ..., \mu_{r-1}\}$, так что μ_i – корень T_i. Далее, начиная двигаться от корня, идём по каждой ветке до первого повторения метки вершины и отбрасываем всё нижележащее дерево. Для примера 1 (вместо меток μ_0, μ_1 используются просто цифры 0 и 1):

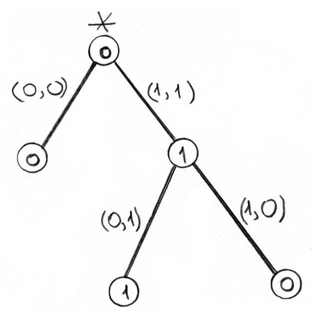

Рис. 3: Усечённое дерево.

3. **Диаграмма перехода (диаграмма Мура).** Превратим усечённое дерево в ориентированный граф "естественным"образом, т.е. поставив стрелки на рёбрах в направлении удаления от корня:

   Затем отождествим вершины с одинаковыми метками: см. Рис. 5.

   Получаем ориентированный граф (с "петлями"и кратными рёбрами) $G = (W, E)$, $|W| = r$, $|E| = mr$, где $|A| = m$, у которого одна из вершин помечена. Такой граф и называется диаграммой Мура.

4. **При помощи таблицы.** В диаграмме Мура пусть $Q = \{q_0, ..., q_{r-1}\}$ – различные вершины, назовём x – переменную, пробегающую алфавит A. Определим функции F и G:

$$F : A \times Q \to B$$

$$G : A \times Q \to Q$$

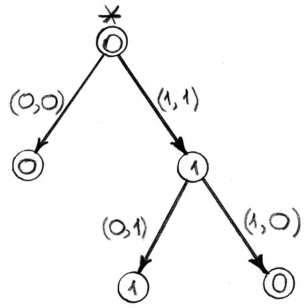

Рис. 4: Переход к диаграмме Мура.

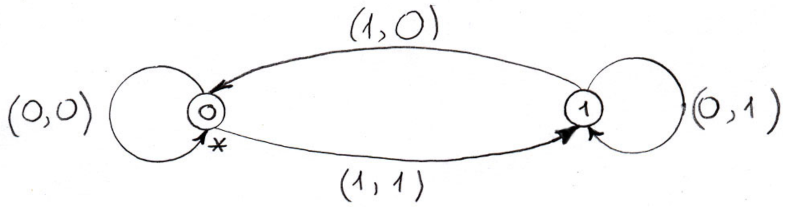

Рис. 5: Пример диаграммы Мура.

по следующему правилу: $F(x, q)$ есть выходной символ, соответствующий вершине q и входному символу x, $G(x, q)$ есть вершина, в которую осуществляется переход из вершины q по входному символу x. Задание этих функций вместе с указанием начальной (помеченной) вершины эквивалентно заданию диагрммы Мура. Для примера 1:

x	q	F	G
0	0	0	0
1	0	1	1
0	1	1	1
1	1	0	0

5. **Каноническое уравнение.** Введём дискретный параметр времени t пробегающий $\mathbb{N}$ – множество натуральных чисел. Считаем, что в момент времени t текущее состояние есть $q(t)$ и на вход подаётся $x(t)$. Тогда на выходе получаем символ $y(t) = F(x(t), q(t))$ и переходим в состояние $q(t+1) = G(x(t), q(t))$. Задание уравнений перехода вместе с начальным состоянием $q(1)$ и называется заданием канонических уравнений. Для примера 1:

$$\begin{cases} y(t) & = & x(t) + q(t) \\ q(t+1) & = & x(t) + q(t) \\ q(1) & = & 0 \end{cases}$$

В заключение обозначим $P_{A,B}^{\text{о.д.}}$ – множество всех ограниченно детерминированных функций $A^* \to B^*$.

Лекция 14.

Конечные автоматы.

Пусть A – входящий алфавит, $|A| = m$, B – выходящий алфавит, $|B| = p$, Q – алфавит состояний, $|Q| = r$, $F : A \times Q \to B$, $G : A \times Q \to Q$. Множество $V = (A, B, Q, F, G)$ называется конечным автоматом. Если в множестве Q выделено начальное состояние q_0, то такой автомат V_{q_0} называется инициальным конечным автоматом. V_{q_0} задаёт ограниченно детерминированную (или *автоматную*) функцию $f_{V_{q_0}}$.

Если задан инициальный автомат $V_{q_0} = (A, B, Q, F, G)$, то функции F и G можно считать продолженными на $A^* \times Q \to$ по следующему правилу:

$$F(\Lambda, q_0) = \Lambda$$

$$G(\Lambda, q_0) = q_0$$

$$F(\alpha a, q) = F(a, G(\alpha, q))$$

$$G(\alpha a, q) = G(a, G(\alpha, q))$$

где $\alpha \in A^*,\ a \in A$.

Определим: *множество слов представимых* V_{q_0} *посредством* $B' \subseteq B$ есть

$$M = \{\alpha \in A^* | F(\alpha, q_0) \in B'\}$$

Всякое $M \subseteq A^* \backslash \{\Lambda\}$ назовём событием. Событие M назовём представимым, если найдётся такой инициальный автомат V_{q_0} и такое множество $B' \subseteq B$, что M есть множество слов представимых V_{q_0} посредством B'.

На классе событий введём следующие три операции: $\cup, \cdot, <>$ (ниже E, K, L – события):

1. $E \cup K$ – теоретико множественное объединение.
2. $E \cdot K = EK = \{\alpha | \alpha = \alpha_1 \alpha_2,\ \alpha_1 \in E,\ \alpha_2 \in K\}$ – конкатенация.
3. $< E >= \{\alpha | \exists k \geqslant 1 : \alpha = \alpha_1 ... \alpha_k,\ \alpha_i \in E,\ i = 1, ..., k\}$.

Отметим очевидные **свойства** этих операций:

1. $E \cup K = K \cup E$
2. $E \cup (K \cup L) = (E \cup K) \cup L$
3. $E(K \cup L) = EK \cup EL$
4. $(E \cup K)L = EL \cup KL$
5. $(EK)L = E(KL)$
6. $\varnothing E = E \varnothing = \varnothing$
7. $< \varnothing >= \varnothing$
8. $<< E >>=< E >$
9. $< E >= E \cup E < E >$
10. $E < E >=< E > E$

События, которые можно получить за конечное число операций $\cup, \cdot, <>$ из элементарных событий $\varnothing, \{a_1\}, ..., \{a_m\}$, назовём *регулярными.*

Пусть задан ориентированный граф $I = (W, E)$, у которого выделены две вершины v_1, v_k – начальная и конечная соответственно. На каждом ребре этого графа написана либо буква алфавита $A = \{a_1, ..., a_m\}$, либо символ пустого слова Λ. Такой граф называется *обобщённым источником.*

Будем обозначать $p : v_i \to v_j$ – некоторый путь в заданном ориентированном графе с началом в v_i и концом в v_j, α_p – слово в обобщённом источнике, выписываемое при прохождении пути p (т.е. каждый раз при прохождении ребра выписывается буква, написанная на нём). С обобщённым источником I свяжем событие $[I]$:

$$[I] = \{\alpha \in A^* \setminus \{\Lambda\} \mid \exists p : v_1 \to v_k : \alpha_p = \alpha\}$$

называемое событием, *представляемым обобщённым источником* I.

Пример 1. Обобщённый источник:

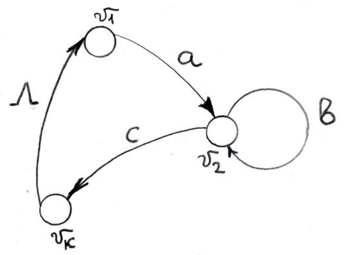

Рис. 6: Пример обобщённого источника.

Этот источник представляет слова $ac, acac, abbbc, abc, abbcac$ и др.

Пример 2. Источник

$$v_1 \cdot \qquad\qquad \cdot v_k$$

представляет событие $\varnothing$.

Лемма. *Если событие регулярно, то найдётся обобщенный источник, его представляющий.*

Доказательство. Доказательство будем вести индукцией по числу элементарных операций $\cup, \cdot$ и $<>$ используемых для получения события E.

В качестве базы индукции приведём обобщённые источники порождающие элементарные события:

$$\varnothing : v_1 \cdot \qquad \cdot v_k$$

$$\{a_1\} : v_1 \cdot \xrightarrow{a_1} \cdot v_k$$

$$\dots$$

$$\{a_m\} : v_1 \cdot \xrightarrow{a_m} \cdot v_k$$

Итак, пусть мы умеем представлять события, полученные с использованием не более n элементарных операций. Пусть для получения события E использована $n+1$ операция. Тогда E получено одним из трёх нижеследующих способов, где E_1, E_2 используют не более n элементарных операций, следовательно для них обобщённые источники могут быть построены:

1) $E = E_1 \cup E_2$ (см. Рис. 7).

2) $E = E_1 E_2$ (см. Рис. 8).

3) $E =< E_1 >$ (см. Рис. 9).

Лемма доказана.

Теорема. *Пусть E – регулярное событие, тогда E – представимо (с помощью конечного автомата).*

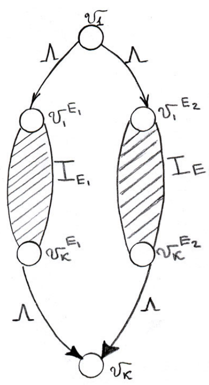

Рис. 7: Доказательство пункта 1.

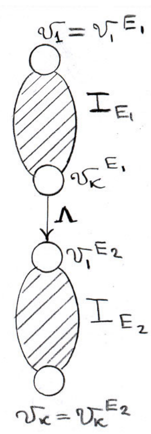

Рис. 8: Доказательство пункта 2.

Доказатальство. Возьмём $B = \{0, 1\}$, $B' = \{1\}$. По предыдущей лемме существует обобщённый источник $I = (W, E)$, такой что $[I] = E$. Пусть $W = \{v_1, ..., v_n\}$, где v_1 – начальная, v_n – конечная вершины. Для $\alpha \in A^*$ и $v \in W$ определим множества:

$$\Theta(\alpha, v) = \{\hat{v} \in W \mid \exists p : v \to \hat{v} : \alpha_p = \alpha\}$$

Определим множество состояний, как

$$Q = \{q_1, ..., q_{2^n}\}$$

– множество всевозможных подмножеств W. В качестве начального состояния возьмём $q_1 = \{v_1\}$. Определим функцию перехода:

$$G(a, q) = \bigcup_{v \in q} \Theta(a, v)$$

– множество вершин, в которые можно попасть из данного множества вершин q по букве a. Функцию F определим так:

$$F(a, q) = \begin{cases} 1, \ v_n \in G(a, q) \\ 0, \ \text{иначе} \end{cases}$$

– можно ли попасть в конечную вершину из данного множества по букве a.

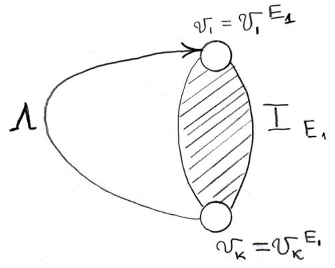

Рис. 9: Доказательство пункта 3.

Полученный автомат $V_{q_1}(A, B, Q, F, G)$ посредством B' представляет в точности $[I]$. Действительно, α представимо с помощью V_{q_1} посредством $B' \Leftrightarrow F(\alpha, q_1) = 1 \Leftrightarrow v_n \in G(\alpha, q_1) \Leftrightarrow v_n \in \Theta(\alpha, v_1) \Leftrightarrow \alpha \in [I]$. Предпоследний переход, если и не является очевидным, то очень легко доказывается. Поскольку $\alpha \in [I] \Leftrightarrow \alpha \in E$, то теорема доказана.

Лемма 1. *Пусть X, C, D – события. Тогда*

$$X = D \cup XC \Leftrightarrow$$

$$X = D \cup D < C >$$

Доказательство. Пусть $X = D \cup D < C >$. Тогда

$$D \cup XC = D \cup (D \cup D < C >)C = D \cup (DC \cup D < C > C) =$$

$$= D \cup D(C \cup < C > C) = D \cup D < C >= X$$

Обратно: пусть $X = D \cup XC$. Доказательство $X = D \cup D < C >$ разобьём на доказательства двух включени.

а) Покажем, что $X \subseteq D \cup D < C >$. Предположим противное: пусть существует такое $\alpha \in X$, что $\alpha \notin D \cup D < C >$. Среди всех таких α выберем слово наименьшей длины. $\alpha \notin D \Rightarrow \alpha \in XC \Rightarrow \alpha = \alpha_1\alpha_2$, где $\alpha_1 \in X$, $\alpha_2 \in C$. Причём $\lambda(\alpha_1) < \lambda(\alpha) \Rightarrow \alpha_1 \in D \cup D < C > \Rightarrow \alpha = \alpha_1\alpha_2 \in (D \cup D < C >)C = DC \cup D < C > C = D(C \cup < C > C) = = D < C > \subseteq D \cup D < C >$ – противоречие.

б) Покажем, что $X \supseteq D \cup D < C >$. Опять предполагаем противное: существует $\alpha \in D \cup D < C >$, такое что $\alpha \notin X$. Опять среди всех таких α выберем наименьшее по длине: $\alpha \notin X \Rightarrow \alpha \notin D \Rightarrow \alpha \in D < C > \overset{\text{см. а)}}{=} = (D \cup D < C >)C \Rightarrow \alpha = \alpha_1\alpha_2$, где $\alpha_1 \in D \cup D < C >$, $\alpha_2 \in C$. Т.к. $\lambda(\alpha_1) < \lambda(\alpha)$, то $\alpha_1 \in X \Rightarrow \alpha = \alpha_1\alpha_2 \in XC \subseteq X$ – противоречие. Лемма доказана.

Замечание. *Если события C и D регулярны и для события X выполняется равенство*

$$X = D \cup XC,$$

то по доказанной только что лемме следует, что X – регулярно.

Пример нерегулярного события. Обозначим:

$$0^k = \underbrace{0...0}_{k}$$

$$1^k = \underbrace{1...1}_{k}$$

Рассмотрим множество слов:
$$E = \{0^k 1^k, k = 1, 2, 3, ...\}$$
Это событие не является регулярным.

Доказательство. Предположим противное: пусть E – регулярно. Тогда по доказанному выше существует конечный автомат
$$V_{q_1} = (\{0,1\}, \{0,1\}, Q, F, G),$$
где $Q = \{q_1, ..., q_n\}$, такой что $\alpha \in E \Leftrightarrow F(\alpha, q_1) = 1$. Рассмотрим $n+1$ значение функции $G:$
$$G(0, q_1), G(0^2, q_1), ..., G(0^{n+1}, q_1)$$
Найдутся такие i и j, что $i \neq j$ и $G(0^i, q_1) = G(0^j, q_1)$. Для них:
$$1 = F(0^i 1^i, q_1) = F(1^i, G(0^i, q_1)) = F(1^i, G(0^j, q_1)) = F(0^j 1^i, q_1)$$
– противоречие.

Лемма 2. *Пусть выполняется n равенств:*
$$X_i = R_{0i} \cup X_1 R_{1i} \cup ... \cup X_n R_{ni},\ i = 1, ..., n, \qquad (*)$$
где X_i – события, R_{ji} – регулярные события $i = 1, ..., n,\ j = 0, 1, ..., n$. Тогда X_i – регулярные события $i = 1, ..., n$.

Доказательство. Доказательство проведём индукцией по n. Базой ($n = 1$) является Замечание к Лемме 1. Пусть утверждение доказано при всех $n = 1, ..., k-1$, покажем, что оно справедливо и при $n = k$. В первом уравнении обозначим $D = R_{01} \cup X_2 R_{21} \cup ... \cup X_k R_{n1},\ C = R_{11}$. Тогда
$$X_1 = D \cup C X_1 \overset{\text{по Лемме1}}{\Longrightarrow}$$
$$X_1 = D \cup D < C >$$
Подставим это выражение для X_1 в остальные уравнения и раскроем выражения для D и C. Получим систему вида $(*)$ для $X_2, ..., X_k$ с регулярными коэффициентами. По предположению индукции её решение есть регулярные события. Поэтому и X_1 регулярно. Лемма доказана.

Теорема (Клини.) *Событие E является регулярным тогда и только тогда, когда E – представимо.*

Доказательство. В одну сторону теорема доказана выше. Докажем теперь, что всякое представимое событие регулярно. Пусть дан инициальный конечный автомат:
$$V_{q_0} = (A, B, Q, F, G)$$
$|Q| = n,\ Q = \{q_1, ..., q_n\},\ B' \subseteq B,\ E = \{\alpha | F(\alpha, q_1) \in B'\}$.

Определим события:
$$E_i = \{\alpha \in A^* \setminus \{\Lambda\} | G(\alpha, q_1) = q_i\},\ i = 1, ..., n$$
$$\hat{E}_i = \{a \in A | F(a, q_i) \in B'\},\ i = 1, ..., n$$
Очевидно, что в силу конечности $\hat{E}_i$ регулярны. Покажем, что E_i регулярны. Определим события
$$R_{ji} = \{a \in A | G(a, q_j) = q_i\},\ i = 1, ..., n,\ j = 1, ..., n$$
Ясно, что в силу их конечности R_{ji} регулярны. Покажем, что
$$E_i = R_{1i} \cup E_1 R_{1i} \cup ... \cup E_n R_{ni} \qquad (**)$$
а) $\alpha \in E_i, \alpha = a \in A\ \Leftrightarrow G(a, q_1) = q_i \Leftrightarrow \alpha = a \in R_{1i}$

б) $\alpha = \alpha' a \in E_i, \alpha' \neq \Lambda, a \in A \Leftrightarrow q_i = G(\alpha' a, q_1) = G(a, G(\alpha', q_1)) = = G(a, q_j) \Leftrightarrow \alpha' \in E_j, a \in R_{ji}$

Из $(**)$ по лемме 2 следует, что E_i регулярны. Для завершения доказательства теоремы покажем, что

$$E = \hat{E}_1 \cup E_1\hat{E}_1 \cup ... \cup E_n\hat{E}_n$$

а) Покажем включение:

$$E \subseteq \hat{E}_1 \cup E_1\hat{E}_1 \cup ... \cup E_n\hat{E}_n$$

Пусть $\alpha \in E$. Если $\alpha = a \in A$, то, очевидно, $\alpha \in \hat{E}_1$. Если $\alpha = \alpha' a,\ \alpha' \neq \Lambda$, то $F(\alpha' a, q_1) \in B' \Rightarrow F(a, G(\alpha', q_1)) = F(a, q_i) \in B' \Rightarrow \alpha' \in E_i, a \in \hat{E}_i$.

б) Обратное включение:

$$E \supseteq \hat{E}_1 \cup E_1\hat{E}_1 \cup ... \cup E_n\hat{E}_n$$

Пусть $\alpha \in \hat{E}_1 \cup E_1\hat{E}_1 \cup ... \cup E_n\hat{E}_n$. Если $\alpha = a \in A \Rightarrow a \in \hat{E}_1 \Rightarrow a = \alpha \in E$. Если $\alpha = \alpha' a \Rightarrow \alpha' a \in E_i\hat{E}_i \Rightarrow \alpha' \in E_i, a \in \hat{E}_i \Rightarrow F(\alpha, q_1) = F(\alpha' a, q_1) = = F(a, G(\alpha', q_1)) = F(a, q_i) \in B'$.

Теорема доказана.

Лекция 15.

Конечные автоматы (продолжение).

Введём понятие *источника. Источником* называется ориентированный граф $J = (W, E)$ с выделенной начальной вершиной $v_1 \in W$ и конечными вершинами $v_{i_1}, ..., v_{i_k} \in W$ $(1 \leqslant k \leqslant |W|)$, каждое ребро которого помечено буквой алфавита $A : e \in E \Rightarrow \mu(e) \in A$ (пустое слово не может выступать в качестве метки ребра). Как и для обобщённого источника, для источника вводится множество слов, представимых им:

$$[J] = \{\alpha \in A^* \setminus \{\Lambda\} | \exists v' \text{– конечная вершина}, \exists p : v_1 \to v' : \alpha_p = \alpha\}$$

Утверждение 1. *Пусть* $J = (W, E)$ *– источник. Тогда существует обобщённый источник* $I = (W', E')$, *такой что* $[J] = [I]$.

Доказательство. Доказательство проведём в древнегреческой манере: СМОТРИ:

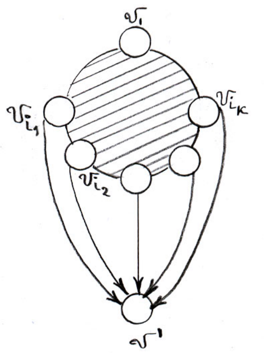

Рис. 10: Переход от источника к обобщенному источнику.

Пояснение: добавили ещё одну вершину v' и конечной теперь называем только её.

Утверждение 2. *Пусть* M *– представимо (с помощью инициального автомата). Тогда существует источник* $J = (W, E)$, *такой что* $M = [J]$.

Доказательство. Пусть V_{q_1} – инициальный автомат, представляющий M с помощью B' :

$$V = (A, B, Q, F, G)$$

$$Q = \{q_1, ..., q_n\}$$

$$|A| = m, \ |B| = p, \ B' \subseteq B$$

Определим множество вершин источника:

$$W = \{v_1 = (\Lambda, q_1), v_{li} = (b_l, q_i), 1 \leqslant l \leqslant p, \ 1 \leqslant i \leqslant n\}$$

при этом вершина $v_{li} = (b_l, q_i)$ – конечная, если, и только если $b_l \in B'$. Вершины (b_{l_1}, q_i) и (b_{l_2}, q_j) соединены ребром e от первой ко второй вершине, если, и только если существует $a \in A$, такое что $G(a, q_i) = q_j$ и $F(a, q_i) = = b_{l_2}$. При этом $\mu(e) = a$. Легко понять, что $M = [J]$.

Подытоживая установленную в нескольких предыдущих утверждениях связь между различными способами задания событий, составим диаграмму вложенности, показывающую, что на самом деле все способы задания событий эквивалентны: см. Рис. 11.

Поставим вопрос о равенстве двух событий, задаваемых инициальными конечными автоматами. Введём некоторые определения. Говорим, что для конечных автоматов $V = (A, B, Q, F, G)$, $V' =$

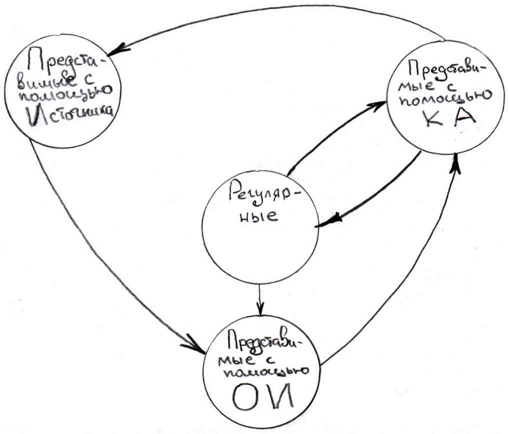

Рис. 11: Диаграмма установленной вложенности классов событий.

(A, B, Q', F', G') два начальных состояния $q_1 \in Q, q_2 \in Q'$ *эквивалентны*, и пишем $q_1 \sim q_2$, если для любого $\alpha \in A^*$ $f_{V_{q_1}}(\alpha) = f_{V'_{q_2}}(\alpha)$. Говорим, что они к-эквивалентны, и пишем $q_1 \overset{k}{\sim} q_2$, если для любого $\alpha \in A^k = \{a_1...a_k | a_i \in A\}$ $f_{V_{q_1}}(\alpha) = f_{V'_{q_2}}(\alpha)$. Говорим также, что сами конечные автоматы *эквивалентны* $V \sim V'$, если для любого $q \in Q$ существует $q' \in Q'$, такой что $q \sim q'$, и для любого $q' \in Q'$ существует $q \in Q$, такой что $q' \sim q$.

Вопросы эквивалентности состояний и автоматов помогают решить несколько следующих утверждений.

Лемма. *Пусть для некоторого автомата* $V = (A, B, Q, F, G)$ *существует два не эквивалентных, но к-эквивалентных состояния:* $q_1 \overset{k}{\sim} q_2$, $q_1 \not\sim q_2$. *Тогда для него найдутся два к-эквивалентных, но не к+1-эквивалентных состояния:* $q'_1 \overset{k}{\sim} q'_2$, $q'_1 \overset{k+1}{\not\sim} q'_2$.

Доказательство. Пусть $\alpha = \alpha(1)...\alpha(l)$ – наименьшее по длине слово, такое что $f_{V_{q_0}}(\alpha) \neq f_{V_{q_1}}(\alpha)$. Положим $\alpha' = \alpha(1)...\alpha(l-k-1)$. Тогда нетрудно проверить, что в качестве q'_1, q'_2 можно взять $q'_1 = G(\alpha', q_1)$, $q'_2 = = G(\alpha', q_2)$.

Теорема (Мур). *Пусть* $V = (A, B, Q, F, G)$, $q_1, q_2 \in Q$, $|Q| = n$. *Тогда*

$$q_1 \sim q_2 \Leftrightarrow q_1 \overset{n-1}{\sim} q_2$$

Доказательство. В одну сторону теорема очевидна. Докажем в другую. Пусть $q_1 \overset{n-1}{\sim} q_2$. Определим разбиение множества состояний Q на классы:

$$R_k = \{Q_1^k, ..., Q_{r_k}^k\}$$

по следующему правилу:

1. $Q_i^k \subseteq Q,\ Q_i^k \neq \varnothing$
2. $\bigcup\limits_{i=1}^{r_k} = Q$
3. $Q_i^k \cap Q_j^k = \varnothing,\ i \neq j$
4. $\forall q, q' \in Q_i^k\ q \overset{k}{\sim} q'$
5. $\forall q \in Q_i^k,\ \forall q' \in Q_j^k, i \neq j\ q \overset{k}{\not\sim} q'$

Т.е. $\{Q_i^k\}$ – разбиение множества состояний на к-эквивалентные (нетрудно проверить, что к-эквивалентность – отношение эквивалентности). Отметим очевидное свойство:

$$1 \leqslant |R_1| \leqslant ... \leqslant |R_n| \leqslant n$$

(каждое следующее разбиение является подразбиением предыдущего). Априори возможны две ситуации:

1) Существует $1 \leqslant k \leqslant n-1$ такое, что $|R_k| = |R_{k+1}|$. Но тогда, т.к. R_{k+1} является подразбиением R_k, то $R_{k+1} = R_k$. Это значит, что для любых $q, q' \in Q$, таких что $q \overset{k}{\sim} q'$ выполняется $q \overset{k+1}{\sim} q'$. Но это означает, что $q \sim q'$ – предполагая противное приходим к противоречию с леммой.

2) Такого k не существует. Покажем, что при $n \geqslant 2$ эта ситуация невозможна. Действительно, в этом случае $|R_i| = i$. В частности $R_1 = \{Q\}$, $R_2 \neq \{Q\}$. Т.е. любые два состояния 1-эквивалентны, но существуют 2 состояния не 2-эквивалентных. 1-эквивалентность любых двух состояний означает, что работа автомата не зависит от того, в каком состоянии он находится ($F(a, q_i) = F(a, q_j)$ для любых $q_i, q_j \in Q, \ a \in A$). Но это означает, что любые два состояния просто эквивалентны – противоречие с существованием 2-неэквивалентных состояний.

Теорема доказана.

Извлечём из предыдущей теоремы критерий эквивалентности двух автоматов.

Теорема. *Пусть даны два конечных автомата:*

$$V = (A, B, Q, F, G)$$

$$V' = (A, B, Q', F', G')$$

$$|Q| = n, \ |Q'| = n'$$

Тогда для любых $q \in Q, \ q' \in Q'$ справедливо следующее утверждение:

$$q \sim q' \Leftrightarrow q \overset{n+n'-1}{\sim} q'$$

Доказательство. Построим "объединённый" конечный автомат:

$$\hat{V} = (A, B, \hat{Q}, \hat{F}, \hat{G})$$

где

$$\hat{Q} = Q \cup Q'$$

$$\hat{F}(a, \hat{q}) = \begin{cases} F(a, \hat{q}), \ \hat{q} \in Q \\ F'(a, \hat{q}), \ \hat{q} \in Q' \end{cases}$$

$$\hat{G}(a, \hat{q}) = \begin{cases} G(a, \hat{q}), \ \hat{q} \in Q \\ G'(a, \hat{q}), \ \hat{q} \in Q' \end{cases}$$

Для автомата $\hat{V}$ утверждение теоремы совпадает с утверждением теоремы Мура.

Сокращённым автоматом для данного автомата $V = (A, B, Q, F, G)$ называется такой автомат $\hat{V} = (A, B, \hat{Q}, \hat{F}, \hat{G})$, что $\hat{V} \sim V$ и среди всех автоматов эквивалентных V $\hat{V}$ имеет наименьшее количество состояний, т.е. для любых $q, q' \in \hat{Q}$ выполнено $q \not\sim q'$.

Для построения сокращённого автомата необходимо построить последовательность множеств $R_k = \{Q_1^k, ..., Q_{r_k}^k\}$ (см. доказательство теоремы Мура) и найти наименьшее k, такое что $R_k = R_{k+1}$. В доказательстве теоремы Мура отмечалось, что для такого k $q, q' \in Q_i^k$ влечёт $q \sim q'$. Затем выбираем

$$\hat{Q} = \{q_1, ..., q_{r_k}\}$$

где q_i – произвольное из Q_i^k. Положим

$$\hat{F}(a, q_i) = F(a, q_i)$$

$$\hat{G}(a, q_i) = q_j$$

где $q_j \in \hat{Q}$ и $q_j \sim G(a, q_i)$.