

Лекция: Теорема Анселя о разбиении  
 $n$ -мерного куба на цепи. Теорема о числе  
монотонных функций алгебры логики. Теорема о  
расшифровке монотонных функций алгебры  
логики.

Лектор - доцент Селезнева Светлана Николаевна

Лекции по “Избранным вопросам дискретной математики”.  
3-й курс, группа 318,  
факультет ВМК МГУ имени М.В. Ломоносова

Лекции на сайте <http://mk.cs.msu.su>

# Разбиение $n$ -мерного куба на цепи

По теоремам Дилуорса и о ширине куба  $E_2^n$  куб  $E_2^n$  можно разбить на  $C_n^{\lfloor \frac{n}{2} \rfloor}$  цепей.

А как можно устроить такое разбиение?

Ответ на этот вопрос дает теорема Анселя.

# Теорема Анселя

**Теорема 1 (Анселя (Hansel)).** При  $n \geq 1$  куб  $E_2^n$  можно разбить на  $C_n^{\lfloor \frac{n}{2} \rfloor}$  цепей со следующими свойствами:

- 1) количество цепей длины  $n - 2p + 1$  в точности равно  $C_n^p - C_n^{p-1}$ ,  $p = 0, 1, \dots, \lfloor \frac{n}{2} \rfloor$ ;
- 2) в наименьшей вершине цепи длины  $n - 2p + 1$  содержится  $p$  единиц и  $(n - p)$  нулей, в наибольшей ее вершине содержится  $(n - p)$  единиц и  $p$  нулей;
- 3) для произвольных наборов  $\alpha_1 < \alpha_2 < \alpha_3$  цепи длины  $n - 2p + 1$  вида

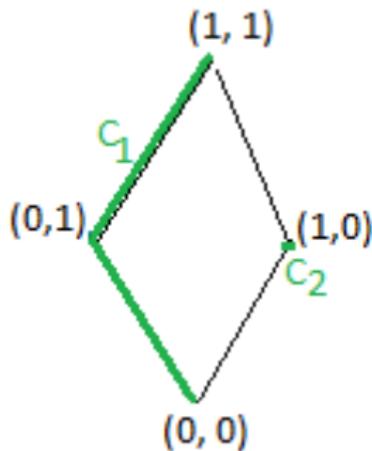
$$\begin{aligned}\alpha_1 &= (a_1, \dots, a_{i-1}, \textcolor{blue}{0}, a_{i+1}, \dots, a_{j-1}, \textcolor{green}{0}, a_{j+1}, \dots, a_n); \\ \alpha_2 &= (a_1, \dots, a_{i-1}, \textcolor{blue}{0}, a_{i+1}, \dots, a_{j-1}, \textcolor{green}{1}, a_{j+1}, \dots, a_n); \\ \alpha_3 &= (a_1, \dots, a_{i-1}, \textcolor{blue}{1}, a_{i+1}, \dots, a_{j-1}, \textcolor{green}{1}, a_{j+1}, \dots, a_n);\end{aligned}$$

набор  $\beta$  вида  $\beta = (a_1, \dots, a_{i-1}, \textcolor{blue}{1}, a_{i+1}, \dots, a_{j-1}, \textcolor{green}{0}, a_{j+1}, \dots, a_n)$  принадлежит цепи длины  $n - 2p - 1$  ( $i \neq j$ ).

# Теорема Анселя

**Доказательство** проведем индукцией по  $n$ .

*Базис индукции:*  $n = 2$ . Разобьем куб  $E_2^2$  на 2 цепи:  
 $C_1 = \{(0, 0) < (0, 1) < (1, 1)\}$ ;  $C_2 = \{(1, 0)\}$ .



# Теорема Анселя

**Доказательство** (продолжение).

*Индуктивный переход.* Рассмотрим куб  $E_2^{n+1}$ . Его можно построить из двух кубов  $E_2^n$ .

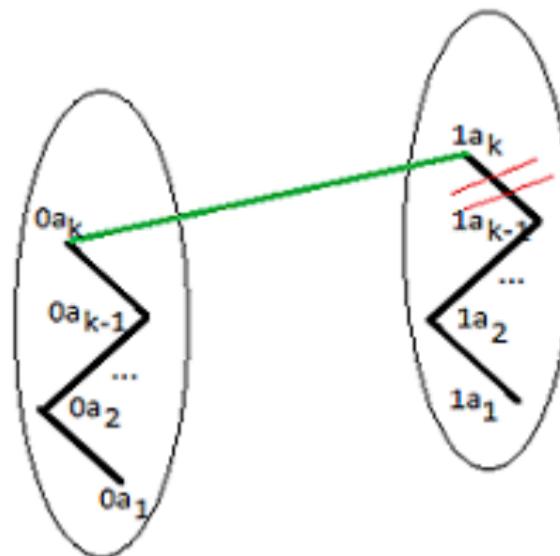
По индуктивному предположению разбиение на цепи в кубах  $E_2^n$  уже построено.

Разобьем куб  $E_2^{n+1}$  на цепи по следующим правилам:  
возьмем в двух кубах  $E_2^n$  **одинаковые** цепи и первую из них (с первой координатой 0) **дополним** наибольшим элементом второй цепи (с первой координатой 1);  
соответственно, из второй цепи **удалим** ее наибольший элемент.

# Теорема Анселя

**Доказательство** (продолжение). Из двух одинаковых цепей  $C$  в кубах  $E_2^n$  получаем цепи

$C_1 = \{(0, a_1) < (0, a_2) < \dots < (0, a_{k-1}) < (0, a_k) < (1, a_k)\}$  и  
 $C_2 = \{(1, a_1) < (1, a_2) < \dots < (1, a_{k-1})\}$  в кубе  $E_2^{n+1}$ .



# Теорема Анселя

**Доказательство** (продолжение). Докажем, что построенное разбиение на цепи удовлетворяет свойствам 1)-3).

1) Каким образом можно получить цепь длины  $(n + 1) - 2p + 1$  в кубе  $E_2^{n+1}$ ?

Надо либо цепь длины  $n - 2p + 1$  в кубе  $E_2^n$  увеличить на один элемент, либо цепь длины  $n - 2p + 3 = n - 2(p - 1) + 1$  в кубе  $E_2^n$  уменьшить на один элемент.

По предположению индукции первых цепей в кубе  $E_2^n$  в точности  $C_n^p - C_n^{p-1}$ , вторых цепей —  $C_n^{p-1} - C_n^{p-2}$ .

Поэтому цепей длины  $(n + 1) - 2p + 1$  в кубе  $E_2^{n+1}$  появится в точности

$$(C_n^p - C_n^{p-1}) + (C_n^{p-1} - C_n^{p-2}) = (C_n^p + C_n^{p-1}) - (C_n^{p-1} + C_n^{p-2}) = \\ = C_{n+1}^p - C_{n+1}^{p-1}.$$

Т.е. столько, сколько требуется в теореме.

# Теорема Анселя

**Доказательство** (продолжение). Докажем, что построенное разбиение на цепи удовлетворяет свойствам 1)-3).

2) Свойство 2) непосредственно проверяется.

## Теорема Анселя

**Доказательство** (продолжение). Докажем, что построенное разбиение на цепи удовлетворяет свойствам 1)-3).

3) Если наборы  $\alpha_1, \alpha_2, \alpha_3$  принадлежат и цепи в кубе  $E_2^n$ , то свойство 3) выполняется по предположению индукции.

Осталось рассмотреть случай, когда

$$\alpha_1 = (\mathbf{0}, a_{k-1}), \quad \alpha_2 = (\mathbf{0}, a_k), \quad \alpha_3 = (\mathbf{1}, a_k),$$

где  $C = \{a_1 < a_2 < \dots < a_{k-2} < a_{k-1} < a_k\}$  – цепь в кубе  $E_2^n$ . Тогда  $\beta = (\mathbf{1}, a_{k-1})$ , и по построению набор  $\beta$  лежит на цепи, меньшей на два элемента.

# Теорема Анселя

**Доказательство** (продолжение).

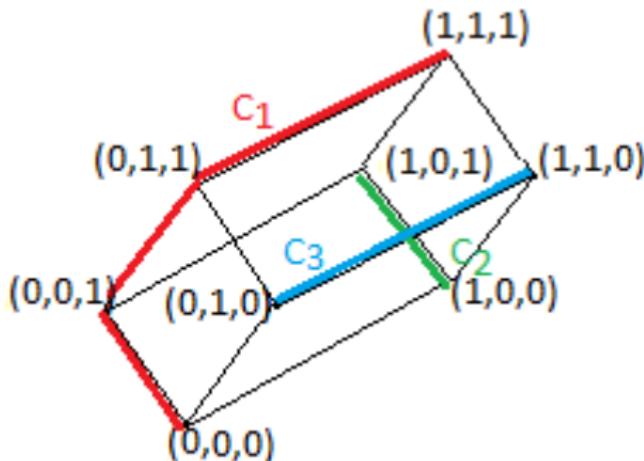
Кроме того, всего цепей в кубе  $E_2^{n+1}$  получено

$$\sum_{p=0}^{\lfloor \frac{n+1}{2} \rfloor} (C_{n+1}^p - C_{n+1}^{p-1}) = \textcolor{blue}{C_{n+1}^0} - C_{n+1}^{-1} + \textcolor{green}{C_{n+1}^1} - \textcolor{blue}{C_{n+1}^0} + \cdots + \\ + \cdots + C_{n+1}^{\lfloor \frac{n+1}{2} \rfloor} - \textcolor{brown}{C_{n+1}^{\lfloor \frac{n+1}{2} \rfloor - 1}} = C_{n+1}^{\lfloor \frac{n+1}{2} \rfloor}.$$

□

# Разбиение куба $E_2^3$ на цепи Анселя

Цепь  $C_1 = \{(0, 0, 0) < (0, 0, 1) < (0, 1, 1) < (1, 1, 1)\}$ ; цепь  
 $C_2 = \{(1, 0, 0) < (1, 0, 1)\}$ ; цепь  $C_3 = \{(0, 1, 0) < (1, 1, 0)\}$ .



## Применения разбиений ЧУМ на цепи

Разбиение куба  $E_2^n$  на цепи Анселя имеет множество применений при решении дискретных задач.

Мы рассмотрим два из них: в задаче подсчета числа монотонных функций и в задаче расшифровки монотонных функций.

## Подсчет числа объектов в классе

Знание количества объектов в некотором классе объектов (например, числа монотонных функций, зависящих от  $p$  переменных) является основой для применения **мощностного метода**.

Мощностной метод применяется, например, в логическом синтезе управляющих систем при получении нижних оценок **сложности** схемы для “самой сложной” функции в классе.

# Монотонные функции алгебры логики

Напомним, что **функцией алгебры логики от  $n$  переменных** называется отображение  $f : E_2^n \rightarrow E_2$ , где  $E_2 = \{0, 1\}$ .

Функция алгебры логики  $f(x_1, \dots, x_n)$  называется **монотонной**, если

$$\forall \alpha, \beta \in E_2^n (\alpha \leq \beta) \Rightarrow (f(\alpha) \leq f(\beta)).$$

Множество всех монотонных функций алгебры логики обозначается  $M$ . Обозначим как  $M^n$  множество всех монотонных функций алгебры логики, зависящих от переменных  $x_1, \dots, x_n$ .

Можно ли подсчитать количество монотонных функций алгебры логики, зависящих от  $n$  переменных, т.е. найти  $|M^n|$ ?

Оценку их числа дает следующая теорема Анселя. При этом существенно используются свойства разбиения куба  $E_2^n$  на цепи Анселя.

# Оценка числа монотонных функций алгебры логики

**Теорема 2 (Анселя).** При  $n \geq 1$  верно двойное неравенство

$$2^{C_n^{\lfloor \frac{n}{2} \rfloor}} \leq |M^n| \leq 3^{C_n^{\lfloor \frac{n}{2} \rfloor}}.$$

**Доказательство.** 1. Нижняя оценка. Возьмем куб  $E_2^n$ , и выделим в нем средний слой  $\lfloor \frac{n}{2} \rfloor$ .

Рассмотрим все возможные функции алгебры логики, которые

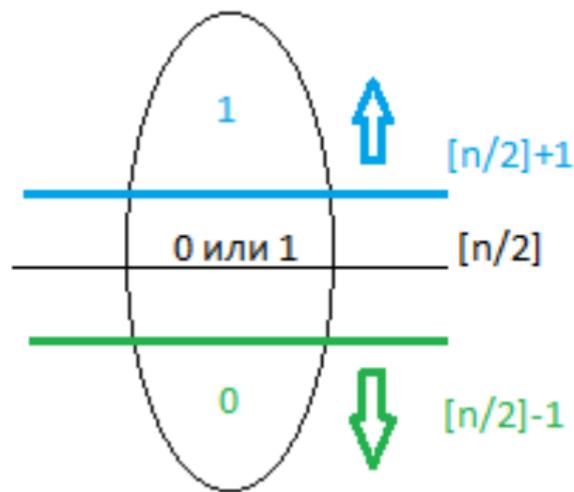
- 1) на всех слоях, выше среднего, принимают значение 1;
- 2) на всех слоях, ниже среднего, принимают значение 0;
- 3) на среднем слое  $\lfloor \frac{n}{2} \rfloor$  принимают произвольные значения (0 или 1).

Заметим, что все такие функции – монотонные. Поэтому число  $|M^n|$  не меньше количества таких функций.

А их в точности  $2^{C_n^{\lfloor \frac{n}{2} \rfloor}}$ . Т.е. нижняя оценка получена.

## Иллюстрация доказательства нижней оценки

Выше среднего слоя – значение 1; ниже среднего слоя – значение 0; на среднем слое – либо значение 0, либо значение 1.



# Оценка числа монотонных функций алгебры логики

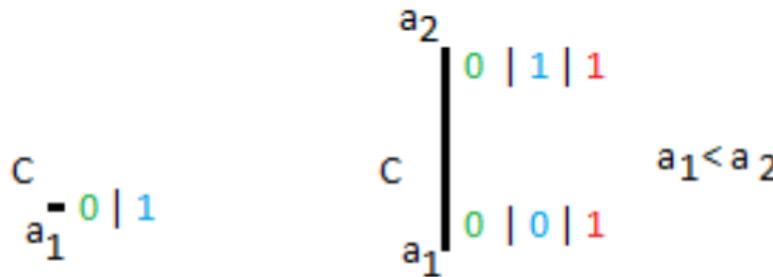
**Доказательство** (продолжение). 2. Верхняя оценка. Разобьем куб  $E_2^n$  на цепи Анселя.

Индукцией по длине цепи докажем, что на каждой из цепей Анселя монотонная функция алгебры логики может быть определена не более, чем тремя разными способами.

# Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение).

*Базис индукции.* В зависимости от четности  $n$  рассмотрим цепи длины 1 или 2. На цепи длины 1 монотонную функцию можно определить двумя способами. На цепи длины 2 монотонную функцию можно определить тремя способами. Базис индукции обоснован.



цепь длины 1

цепь длины 2

# Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение).

*Индуктивный переход.* Рассмотрим цепь длины  $n - 2p + 1$ .

Выберем в ней три меньших набора  $\alpha_1 < \alpha_2 < \alpha_3$ .

По индуктивному построению цепей Анселя, соседние элементы в них отличаются в одной координате.

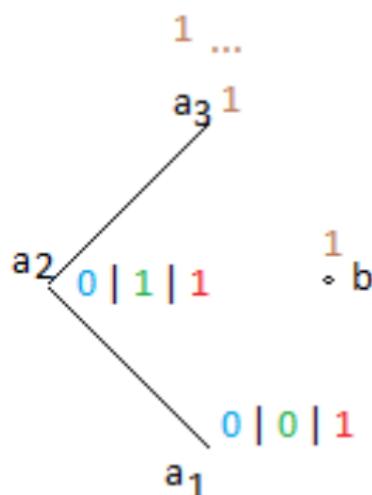
Значит, эти три набора удовлетворяют условию свойства 3) цепей Анселя.

Т.е. набор  $\beta$ , дополняющий эти три набора до квадрата, лежит на цепи длины  $n - 2(p + 1) + 1$ .

По индуктивному предположению, значение функции на наборе  $\beta$  уже определено.

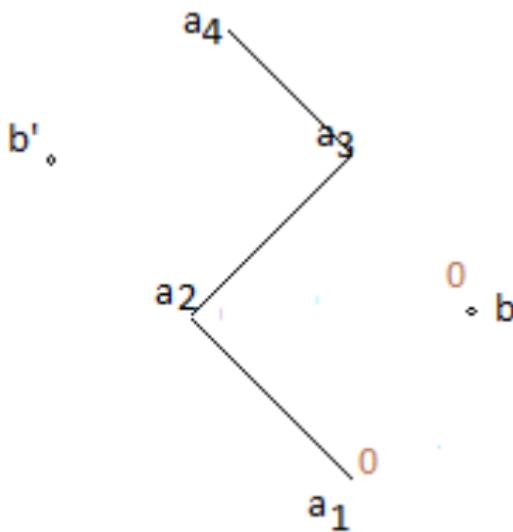
## Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение). 1) Пусть значение функции на наборе  $\beta$  равно 1. Тогда всех наборах этой цепи, больших или равных набору  $\alpha_3$ , функция тоже равна 1. На оставшихся двух наборах  $\alpha_1$  и  $\alpha_2$  функцию можно определить тремя способами.



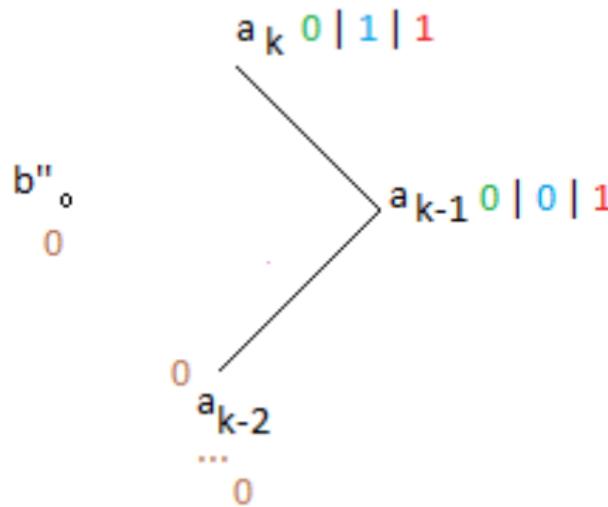
## Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение). 2) Пусть значение функции на наборе  $\beta$  равно 0. Тогда на наборе  $\alpha_1$  функция тоже равна 0. В этом случае рассмотрим следующие три набора этой цепи  $\alpha_2, \alpha_3, \alpha_4$ , и повторим для них рассуждения.



# Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение). В предельном случае мы придем к трем большим наборам этой цепи  $\alpha_{k-2}, \alpha_{k-1}, \alpha_k$  в ситуации, когда на наборе  $\alpha_{k-2}$  функция тоже равна 0. Тогда на двух наборах  $\alpha_{k-1}$  и  $\alpha_k$  функцию можно определить тремя способами.



# Оценка числа монотонных функций алгебры логики

**Доказательство** (продолжение).

Следовательно, на каждой из цепей Анселя мы можем определить монотонную функцию не более, чем тремя способами.

Всего цепей Анселя в точности  $C_n^{\lfloor \frac{n}{2} \rfloor}$ .

Значит,  $|M^n| \leq 3^{C_n^{\lfloor \frac{n}{2} \rfloor}}$ .



# Порядок логарифма числа монотонных функций алгебры логики

**Следствие 2.1.** При  $n \rightarrow \infty$  верно

$$\log_2 |M^n| \asymp C_n^{\lfloor \frac{n}{2} \rfloor} \left( \text{или } \log_2 |M^n| \asymp \frac{2^n}{\sqrt{n}} \right).$$

**Доказательство.** По теореме 2 получаем

$$C_n^{\lfloor \frac{n}{2} \rfloor} \leq \log_2 |M^n| \leq (\log_2 3) \cdot C_n^{\lfloor \frac{n}{2} \rfloor}.$$

Применяя свойство  $C_n^{\lfloor \frac{n}{2} \rfloor} \asymp \frac{2^n}{\sqrt{n}}$ , получаем вторую часть утверждения.



## Задача расшифровки объекта

Задача **расшифровки** состоит в следующем.

Нам дан черный ящик, в котором находится некоторый объект из известного множества  $A$ .

Мы можем задавать вопросы о свойствах этого объекта и получать ответы на них.

Задача состоит в том, чтобы найти, за какое **наименьшее число** вопросов мы можем **расшифровать** (т.е. однозначно определить) любой объект из множества  $A$ .

## Задача расшифровки монотонных функций

В случае задачи **расшифровки монотонной функции** в черном ящике – **монотонная функция** из множества  $M^n$ .

Мы можем узнавать ее значения на произвольных наборах  $\alpha \in E_2^n$ .

Причем вопросы задаем **последовательно**, т.е. при каждом следующем вопросе можем применять знание ответов на предыдущие вопросы (**условная расшифровка**).

Задача состоит в том, чтобы определить, за какое **наименьшее число** вопросов  $\psi_m(n)$  о значении функции на наборе мы можем **расшифровать** любую монотонную функцию алгебры логики, зависящую от  $n$  переменных.

# Задача расшифровки монотонных функций одной и двух переменных

## Пример 1.

1. Понятно, что если  $n = 1$ , то  $\psi_m(1) = 2$ , т.к. надо задать два вопроса о значениях функции на наборах  $(0)$  и  $(1)$ .
2. Если  $n = 2$ , то  $\psi_m(2) = 3$ . В самом деле, узнаем значения на наборах  $(0, 1)$  и  $(1, 0)$ . Если
  - 1) на них есть хотя бы один ноль, то расшифровывает функцию вопрос об ее значении на наборе  $(1, 1)$ ;
  - 2) на них две единицы, то расшифровывает функцию вопрос об ее значении на наборе  $(0, 0)$ .

Докажите самостоятельно, что в общем случае меньшим числом вопросов не обойтись.

# Расшифровка монотонных функций алгебры логики

**Теорема 3.** При  $n \geq 1$  наименьшее число вопросов  $\psi_m(n)$  о значении функции на наборе, которое нужно задать, чтобы расшифровать произвольную монотонную функцию алгебры логики, зависящую от  $n$  переменных, равно  $C_n^{\lfloor \frac{n}{2} \rfloor} + C_n^{\lfloor \frac{n}{2} \rfloor + 1}$ .

# Расшифровка монотонных функций алгебры логики

**Доказательство.** 1. Нижняя оценка. Определим два множества монотонных функций  $M_1$  и  $M_2$ .

Множество  $M_1$  мы рассматривали при доказательстве нижней оценки числа монотонных функций.

Это функции, которые на всех слоях куба  $E_2^n$ , выше среднего слоя, принимают значение 1; на всех слоях, ниже среднего, принимают значение 0; на среднем слое  $\lfloor \frac{n}{2} \rfloor$  принимают произвольные значения (0 или 1).

Множество  $M_2$  строится аналогично, только базовым является слой  $\lfloor \frac{n}{2} \rfloor + 1$ .

Оно содержит все функции, которые на всех слоях куба  $E_2^n$ , выше слоя  $\lfloor \frac{n}{2} \rfloor + 1$ , принимают значение 1; на всех слоях, ниже этого слоя, принимают значение 0; на самом слое  $\lfloor \frac{n}{2} \rfloor + 1$  принимают произвольные значения (0 или 1).

# Расшифровка монотонных функций алгебры логики

**Доказательство** (продолжение).

Заметим, что для произвольного набора  $\alpha$  из объединения слоев  $\lfloor \frac{n}{2} \rfloor$ ,  $\lfloor \frac{n}{2} \rfloor + 1$  найдется пара функций  $f_1, f_2 \in M_1 \cup M_2$ , **различающихся только на этом наборе**, т. е.  $f_1(\alpha) \neq f_2(\alpha)$ , но  $f_1(\beta) = f_2(\beta)$  при  $\beta \neq \alpha$  (Проверьте!).

Значит, при расшифровке надо задать вопросы о значениях функции на всех наборах из слоев  $\lfloor \frac{n}{2} \rfloor$ ,  $\lfloor \frac{n}{2} \rfloor + 1$ .

Т.е.  $\psi_m(n) \geq C_n^{\lfloor \frac{n}{2} \rfloor} + C_n^{\lfloor \frac{n}{2} \rfloor + 1}$ .

# Расшифровка монотонных функций алгебры логики

**Доказательство** (продолжение). 2. Верхняя оценка. Разобьем куб  $E_2^n$  на цепи Анселя.

Будем рассматривать последовательно все цепи по возрастанию их длины.

При этом, узнавая значение функции на некотором наборе  $\alpha$ , будем находить значения функции на всех больших либо меньших наборах (в зависимости от значения функции на наборе  $\alpha$ ).

В соответствии с доказательством теоремы 2 Анселя при увеличении длины цепи на 2 есть **только два набора**, на которых монотонная функция может определяться **произвольно**.

Будем задавать вопросы о значениях функции на этих двух наборах.

В итоге, расшифруем монотонную функцию.

# Расшифровка монотонных функций алгебры логики

**Доказательство** (продолжение). Посчитаем количество вопросов, которые мы при этом зададим.

1) Если  $n$  – четно, то наименьшая длина цепей Анселя равна 1, и таких цепей ровно  $C_n^{\frac{n}{2}} - C_n^{\frac{n}{2}-1}$ . Для каждой цепи будет задано по одному вопросу.

Цепей большей длины ровно  $C_n^{\frac{n}{2}} - \left(C_n^{\frac{n}{2}} - C_n^{\frac{n}{2}-1}\right) = C_n^{\frac{n}{2}-1}$ . Для каждой из них будет задано по два вопроса.

Поэтому всего будет задано вопросов

$$\left(C_n^{\frac{n}{2}} - C_n^{\frac{n}{2}-1}\right) + 2 \cdot C_n^{\frac{n}{2}-1} = C_n^{\frac{n}{2}} + C_n^{\frac{n}{2}+1}.$$

(Мы воспользовались свойством биномиальных коэффициентов  $C_n^k = C_n^{n-k}$ ).

# Расшифровка монотонных функций алгебры логики

**Доказательство** (продолжение).

2) Если же  $n$  – нечетно, то наименьшая длина цепей Анселя равна 2.

Поэтому на каждой из  $C_n^{\lfloor \frac{n}{2} \rfloor}$  цепей Анселя будет задано по два вопроса.

Поэтому всего будет задано вопросов

$$2 \cdot C_n^{\lfloor \frac{n}{2} \rfloor} = C_n^{\lfloor \frac{n}{2} \rfloor} + C_n^{\lfloor \frac{n}{2} \rfloor + 1}.$$

(Здесь мы воспользовались тем, что при нечетных  $n$  верно  $C_n^{\lfloor \frac{n}{2} \rfloor} = C_n^{\frac{n-1}{2}} = C_n^{\frac{n+1}{2}} = C_n^{\lfloor \frac{n}{2} \rfloor + 1}$ ).



## Задачи для самостоятельного решения

1. Построить разбиение на цепи Анселя куба  $E_2^4$ .
2. Подсчитать число монотонных функций алгебры логики, зависящих от  $n$  переменных при  $n = 0, 1, 2, 3$ .
3. [2] Гл. II 5.21–5.25.
4. Доказать, для произвольного набора  $\alpha$  из объединения слоев  $\lfloor \frac{n}{2} \rfloor$ ,  $\lfloor \frac{n}{2} \rfloor + 1$  найдется пара функций  $f_1, f_2 \in M_1 \cup M_2$ , отличающихся только на этом наборе.
5. По доказательству теоремы 3 построить алгоритм расшифровки за 6 вопросов монотонной функции алгебры логики, зависящей от 3-х переменных.

## Литература к лекции

1. Сапоженко А.А. Метод граничных функционалов. М.: Физматлит, 2009.
2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по дискретной математике. М.: Физматлит, 2004.

Конец лекции