Экзамен по теории дискретных функций

Лектор: Кочергин В. В. • Автор: Чепелев Дмитрий*, группа 105

1 курс • Весенний семестр 2024 г.

Аннотация

Обо всех ошибках и опечатках пишите мне, исправлю. Хочу выразить особую благодарность Никите Пшеничному, это его оболочка LaTeX и много хороших вещей я заимствовал из его файла по подготовке к коллоквиуму. Также хочу выразить благодарность за помощь в подготовке файла Егору Скроботову, за помощь в нахождении опечаток Ярославу Додонову.

Немного о файле: страницы в содержании кликабельны, теоремы носят обязательный характер, а предложения — наоборот.

Программа экзамена

1 Функции алгебры логики (булевы функции). Число булевых функций от n фиксированных переменных. Существенные и несущественные (фиктивные) переменные. Операции удаления и добавления несущественной переменной. Равенство булевых функций. Элементарные булевы функции и их свойства. 4

2 Способы задания булевых функций. Булева функция как подмножество вершин n-мерного единичного куба 5

3 Формулы над множеством булевых функций. Реализация булевых функций формулами. Операция суперпозиции. Эквивалентность формул. 5

4 Разложение булевой функции по одной и нескольким переменным. Совершенная дизъюнктивная нормальная форма (СДНФ). Полнота системы $\{x \vee y,\ x\&y,\ \overline{x}\}$. Совершенная конъюнктивная нормальная форма (СКНФ). 6

5 Лемма о сводимости полных систем булевых функций. Существование конечной полной подсистемы в полной системе булевых функций. Примеры полных систем. 7

6 Полином Жегалкина. Существование и единственность представления булевой функции в виде полинома Жегалкина. 8

7 Замыкание множества функций. Свойства замыкания. Замкнутые классы булевых функций. Классы T_0 и T_1 функций, сохраняющих константы. 8

8 Линейные функции. Замкнутость класса L. Лемма о нелинейной функции. 9

9 Двойственные и самодвойственные функции. Замкнутость класса S. Принцип двойственности. Лемма о несамодвойственной функции. 10

10 Монотонные функции. Замкнутость класса M. Лемма о немонотонной функции. 11

*Telegram: @Chepelka_v_chepchike. Последняя компиляция: 30 января 2026 г.
Актуальную версию этого файла можно найти на моём GitHub.

11 Критерий Поста полноты множества функций в P_2. Следствие о существовании в любом полном множестве полного подмножества из не более чем 4 функций. Пример базиса в P_2, состоящего из четырех функций. 12

12 Предполные классы. Теорема о предполных классах в P_2. 13

13 Функции k-значной логики ($k \geqslant 3$). Число функций k-значной логики от n фиксированных переменных. Существенные и фиктивные переменные для функций k-значной логики, отличие от случая булевых функций. Элементарные функции k-значной логики, их свойства. 13

14 Две универсальные формы представления произвольной функции k-значной логики. Полнота систем функций из этих универсальных форм. 15

15 Полнота системы $\{\max(x, y), \overline{x}\}$ в P_k. Функция Вебба. Полнота системы, состоящей только из функции Вебба 15

16 Алгоритм распознавания полноты системы функций k-значной логики. Исследование полноты систем функций k-значной логики на практике. 16

17 Классы сохранения множеств функций и их свойства. Теорема Кузнецова о функциональной полноте функций k-значной логики. 16

18 Представление функций k-значной логики полиномами. Малая теорема Ферма. Условие представления всех функций k-значной логики полиномами. 17

19 Пример Янова замкнутого класса k-значной логики, не имеющего базиса. 18

20 Пример Мучника замкнутого класса k-значной логики со счётным базисом. Континуальность семейства замкнутых классов функций k-значной логики. 18

21 Возведение в n-ю степень с использованием $\log_2 n + o(\log_2 n)$ операций умножения. 19

22 Граф (ориентированный и неориентированный). Основные понятия для графа. Геометрическая реализация графа. Изоморфизм графов. Подграф. Подграф, индуцированный множеством вершин. Пути, цепи, циклы на графе. Компоненты связности графа. Связные графы. 20

23 Деревья, характеристические свойства деревьев. 21

24 Ориентированные графы без ориентированных циклов. Лемма о правильной (монотонной) нумерации вершин в конечном ориентированном графе без циклов. 22

25 Схемы из функциональных элементов в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$. Определение функций, реализуемых в вершинах схемы. Независимость функций, реализуемых в вершинах схемы, от выбора монотонной нумерации вершин. Формулы как схемы. Схемы вычислений. 22

26 Сложность реализации функции (множества функций) схемами из функциональных элементов. Функция Шеннона. Простые верхняя и нижняя оценки функции Шеннона. 23

27 Асимптотически оптимальная по сложности реализация системы всех элементарных конъюнкций длины n. 24

28 Метод Шеннона получения верхней оценки функции Шеннона. 25

29 Метод каскадов получения верхней оценки функции Шеннона. 26

30 Точное значение сложности реализации системы всех функций от n переменных в произвольном полном базисе. 26

31 Реализация симметрических булевых функций. 27

32 Мощностной метод получения нижних оценок функции Шеннона. Эффект Шеннона. Усиленная мощностная нижняя оценка функции Шеннона в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$. 29

33 Порядок роста функции Шеннона в произвольном полном конечном базисе. 31

34 Асимптотически наилучший метод (метод Лупанова) построения схем в базисе $\{x \vee y, x\&y, \overline{x}\}$. Асимптотика роста функции Шеннона в этом базисе. 31

35 Асимптотика роста функции Шеннона в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$ для класса самодвойственных функций. 34

36 Минимальное число инверторов, достаточное для реализации системы функций $\{\overline{x},\ \overline{y},\ \overline{z}\}$ в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$. 34

37 Детерминированные функции. Информационное дерево. Вес детерминированной функции. Ограниченно-детерминированные функции. Состояния, диаграмма переходов (диаграмма Мура), таблица переходов и канонические уравнения ограниченно-детерминированной функции. 35

38 Автомат. Инициальный автомат. Задание автомата с помощью таблицы, канонических уравнений и диаграммы Мура. Автомат «счётчик чётности». Автомат задержки. Автоматные функции. Тождественность ограниченно-детерминированных и автоматных функций 37

39 Периодические последовательности. Лемма о преобразовании автоматом периодических последовательностей. 38

40 Автоматные функции от нескольких переменных. Операция суперпозиции на автоматных функциях. Отсутствие конечной полной системы автоматных функций относительно операции суперпозиции. 38

41 Канонические уравнения автомата в скалярном (булевом) виде. Операция обратной связи. Конечные полные системы автоматных функций относительно операций суперпозиции и обратной связи. Реализация автомата схемами из функциональных элементов и элементов задержки. 40

42 Изоморфизм автоматов. Отличимость состояний автомата на входном слове и множестве входных слов. Неотличимость состояний и автоматов. Приведённый автомат. Теорема о существовании и единственности приведённого автомата. 41

43 Отличимость состояний автомата на входных словах заданной длины. 1-я и 2-я теоремы Мура. Примеры автоматов, для которых утверждения теорем Мура не могут быть усилены. 43

1. Функции алгебры логики (булевы функции). Число булевых функций от n фиксированных переменных. Существенные и несущественные (фиктивные) переменные. Операции удаления и добавления несущественной переменной. Равенство булевых функций. Элементарные булевы функции и их свойства.

Положим $E = \{0, 1\}, B_n = E^n$ — *n-мерный булев куб.*

Предложение 1. $|B_n| = 2^n$.

Доказательство. Любой элемент B_n имеет вид $(a_1, \ldots, a_n)$, где $a_i = 0$ или $a_i = 1$ $\forall i = 1, \ldots, n$. Тогда для каждой из n координат имеет ровно 2 значения, значит, всего значений 2^n. ■

Определение 1. *Булева функция* $f(x_1, \ldots, x_n)$ от n переменных $f : E^n \to E$.
P_2 — множество булевых функций, $P_2(n)$ — от n переменных.

Теорема 1. Число булевых функций от n переменных равно 2^{2^n}.

Доказательство. В самом деле, наша функция определяется значениями, которые она принимает на 2^n наборах. Для каждого набора 2 значения, значит, всего значений 2^{2^n}. ■

Определение 2. Функцию алгебры логики $f(\widetilde{x}^n)$ назовём *существенно зависящей от переменной* x_i $(i = 1, \ldots, n)$, если существуют значения $\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n$ из E такие, что

$$f(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) \neq f(\alpha_1, \ldots, \alpha_{i-1}, 1, \alpha_{i+1}, \ldots, \alpha_n).$$

В этом случае x_i называется *существенной переменной функции* f. Переменная, не являющаяся существенной, называется *фиктивной.*

Определение 3. Пусть x_i — фиктивная переменная функции $f(\widetilde{x}^n)$. Тогда функция

$$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) := f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$$

называется *полученной из f удалением фиктивной переменной x_i*. Обратно, говорят, что *f получена из g добавлением i-ой фиктивной переменной.*

Определение 4. Две булевы функции f и g называются *одинаковыми*, если у них одинаковое множество переменных и на любом наборе этих переменных функции принимают одинаковые значения.

Определение 5. Две булевы функции f и g называются *равными*, если одну из другой можно получить за конечное число применений операций добавления и удаления фиктивных переменных.

Определение 6. *Элементарными* мы будем называть следующие функции:

1. *Константы* 0 и 1 (нуль-местные функции).
2. *Тождественная функция* x и *отрицание* $\overline{x} := 1 - x$ (одноместные функции).
3. *Конъюнкция* $x_1 \& x_2 := \min\{x_1, x_2\}$ (иногда обозначается как $x_1 \cdot x_2$ или $x_1 x_2$).
4. *Дизъюнкция* $x_1 \vee x_2 := \max\{x_1, x_2\}$.
5. *Импликация* $x_1 \to x_2$, $x_1 \to x_2 = 0 \overset{\text{def}}{\iff} x_1 = 1, x_2 = 0$.
6. *Сумма по* $\bmod 2$ $x_1 \oplus x_2$, $x_1 \oplus x_2 = 0 \overset{\text{def}}{\iff} x_1 = x_2$.
7. *Эквивалентность* $x_1 \sim x_2$, $x_1 \sim x_2 = 1 \overset{\text{def}}{\iff} x_1 = x_2$.
8. *Штрих Шеффера* $x_1 \mid x_2 := \overline{x_1 \cdot x_2}$.
9. *Стрелка Пирса* $x_1 \downarrow x_2 := \overline{x_1 \vee x_2}$.

Отметим некоторые **свойства** операций:

1. Коммутативность
   - $x\&y = y\&x$;
   - $x \vee y = y \vee x$;
   - $x \oplus y = y \oplus x$;
2. Ассоциативность
   - $(xy)z = x(yz)$;
   - $(x \vee y) \vee z = x \vee (y \vee z)$;
   - $(x \oplus y) \oplus z = x \oplus (y \oplus z)$;
3. Дистрибутивность
   - $x(y \vee z) = xy \vee xz$;
   - $x \vee (yz) = (x \vee y)(x \vee z)$;
   - $x(y \oplus z) = xy \oplus xz$;
4. Идентичность
   - $xx = x$;
   - $x \vee x = x$;
   - $x \oplus x = 0$;
5. Правила Де Моргана
   - $\overline{\overline{x}} = x$;
   - $\overline{x\&y} = \overline{x} \vee \overline{y}$;
   - $\overline{x \vee y} = \overline{x}\&\overline{y}$;
6. Законы поглощения
   - $x \vee xy = x$;
   - $x\&(x \vee y) = x$;

2. Способы задания булевых функций. Булева функция как подмножество вершин n-мерного единичного куба

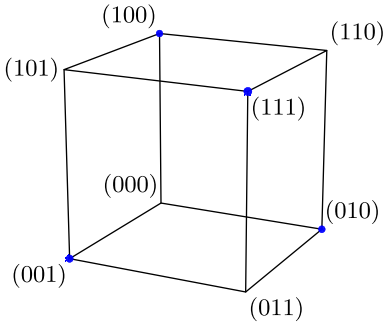
Способы задания БФ:

1. *Таблица значений.* Выписываем все наборы и значения, которые функция на них принимает.

   Например,

x	y	$x\&y$	$x \vee y$	$x \to y$
0	0	0	0	1
0	1	0	1	1
1	0	0	1	0
1	1	1	1	1

2. *Булев куб.* Для функции от n переменных рисуем n-мерный куб (каждая вершина соответствует набору из B_n) и выделяем те, на которых функция принимает значение 1.

   Например, функцию $f(x, y, z) = x \oplus y \oplus z$ можно задать так:

3. *Описательный способ.* Задаём правила, которые описывают функцию.

   Например, $m(x, y, z) = \begin{cases} 1, & x + y + z \geqslant 2 \\ 0, & x + y + z < 2 \end{cases}$.

   Функцией голосования называется булева функция, принимающая значение 1, когда в наборах значений переменных преобладают единицы, и принимающая значение 0, когда в наборах значений переменных преобладают нули.

4. *Формульный способ.* Задаём функцию формулой (см. билет 3). Например, $x \vee y = xy \oplus x \oplus y$.

Упражнение 1. Сколько вершин в серединном сечении n-мерного куба? Какова асимптотика роста этой функции?

3. Формулы над множеством булевых функций. Реализация булевых функций формулами. Операция суперпозиции. Эквивалентность формул.

Пусть дано множество переменных X, а также (конечное или счётное) множество функциональных символов $A = \{f_1^{(n_1)}, \ldots, f_k^{(n_k)}, \ldots\}$.

Определение 1. Определим *формулу над множеством переменных X и множеством функциональных символов A* индуктивно:

1. Любая переменная из X — формула;
2. Если $\Phi_1, \ldots, \Phi_{n_i}$ — формулы, то $f_i^{(n_i)}(\Phi_1, \ldots, \Phi_{n_i})$ — также формула.

Формула над множеством переменных X и множеством функциональных символов A — это последовательность из функциональных символов, символов переменных, скобок и запятых, которую можно получить по указанным правилам за конечное число шагов.

Формула — не функция, а последовательность символов. Однако каждая формула задает функцию: естественным образом определяется значение формулы на каждом наборе значений переменных, входящих в формулу. Или же более формально:

Определение 2. Определим *значение формулы* Φ *на наборе* $\widetilde{\alpha}$ переменных $\widetilde{x}$ индукцией по построению формулы Φ:

1. Если Φ есть однобуквенное слово x_i, то $\Phi[\widetilde{x}, \widetilde{\alpha}] := \alpha_i$.
2. Пусть Φ имеет вид $f(\Phi_1, \ldots, \Phi_m)$, причём $\Phi_1[\widetilde{x}, \widetilde{\alpha}] = \beta_1, \ldots, \Phi_m[\widetilde{x}, \widetilde{\alpha}] = \beta_m$.
   Тогда $\Phi[\widetilde{x}, \widetilde{\alpha}] := f(\beta_1, \ldots, \beta_m)$.

Определение 3. Формулы, реализующие равные функции, называются *эквивалентными.*

Определение 4. Если функция $f(x_1, \ldots, x_n)$ реализуется формулой над системой функций F, то говорят, что она получена операцией суперпозиции из функций системы F.

4. Разложение булевой функции по одной и нескольким переменным. Совершенная дизъюнктивная нормальная форма (СДНФ). Полнота системы $\{x \vee y,\ x\&y,\ \overline{x}\}$. Совершенная конъюнктивная нормальная форма (СКНФ).

Определение 1. Пусть x — переменная, $\sigma \in E$. Тогда $x^\sigma := \begin{cases} x, & \text{если } \sigma = 1, \\ \overline{x}, & \text{если } \sigma = 0. \end{cases}$

Примечание. $x^\sigma = 1 \Leftrightarrow x = \sigma$.

Определение 2. $\sum\limits_{i=1}^{n} a_i := a_1 \oplus a_2 \oplus \ldots \oplus a_n$, $\prod\limits_{i=1}^{n} a_i := a_1 \cdot a_2 \cdot \ldots \cdot a_n$, $\bigvee\limits_{i=1}^{n} a_i := a_1 \vee a_2 \vee \ldots \vee a_n$.

Теорема 1. $\forall f \in P_2(n)$, $\forall m = 1, \ldots, n$

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_m) \in E^m} \prod_{i=1}^{m} x_i^{\sigma_i} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n).$$

Доказательство. Рассмотрим произвольный двоичный набор $(\alpha_1, \ldots, \alpha_m)$. Если $(\sigma_1, \ldots, \sigma_m) \neq (\alpha_1, \ldots, \alpha_m)$, то найдётся $i \in \{1, \ldots, m\}$, для которого $\sigma_i \neq \alpha_i$. Тогда $\alpha_i^{\sigma_i} = 0$. Единственным членом дизъюнкции, влияющим на её значение является $(\sigma_1, \ldots, \sigma_m) = (\alpha_1, \ldots, \alpha_m)$. Он равен $\alpha_1^{\sigma_1} \ldots \alpha_m^{\sigma_m} f(\alpha_1, \ldots, \alpha_m, x_{m+1}, \ldots, x_n) = f(\alpha_1, \ldots, \alpha_m, x_{m+1}, \ldots, x_n)$. ■

Следствие 1. При $m = 1$ получаем, так называемое, *разложение функции f по переменной x_n*:

$$f(x_1, \ldots, x_n) = x_n \cdot f(x_1, \ldots, x_{n-1}, 1) \vee \overline{x_n} \cdot f(x_1, \ldots, x_{n-1}, 0).$$

Следствие 2. При $m = n$ получаем *совершенную дизъюнктивную нормальную форму*:

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) : f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \ldots x_n^{\sigma_n}.$$

Теорема 2. Каждая функция алгебры логики может быть получена суперпозициями из отрицания, конъюнкции и дизъюнкции.

Доказательство. Если функция не тождественно нулевая, то она реализуется с помощью СДНФ. Её можно рассматривать как формулу алгебры логики, построенную при помощи отрицаний, конъюнкций и дизъюнкций. Если функция тождественно нулевая, то её можно задать формулой $x_1 \cdot \overline{x_1}$, рассматриваемой относительно списка фиктивных переменных требуемой длины. ■

Теорема 3. $\forall f \in P_2(n)$, $f \neq 1$ справедлива формула (*совершенная конъюнктивная нормальная форма*).

$$f(x_1, \ldots, x_n) = \prod_{(\delta_1,\ldots,\delta_n): f(\delta_1,\ldots,\delta_n)=0} (x_1^{\overline{\delta_1}} \vee \ldots \vee x_n^{\overline{\delta_n}}).$$

Доказательство. Применяя разложение в виде СДНФ для $\overline{f(x_1, \ldots, x_n)}$, имеем

$$f(x_1, \ldots, x_n) = \overline{\overline{f(x_1, \ldots, x_n)}} = \overline{\bigvee_{(\delta_1,\ldots,\delta_n): \overline{f(\delta_1,\ldots,\delta_n)}=1} x_1^{\delta_1} \ldots x_n^{\delta_n}} = \prod_{(\delta_1,\ldots,\delta_n): f(\delta_1,\ldots,\delta_n)=0} \overline{(x_1^{\delta_1} \ldots x_n^{\delta_n})} =$$

$$= \prod_{(\delta_1,\ldots,\delta_n): f(\delta_1,\ldots,\delta_n)=0} (\overline{x_1^{\delta_1}} \vee \ldots \vee \overline{x_n^{\delta_n}}) = \prod_{(\delta_1,\ldots,\delta_n): f(\delta_1,\ldots,\delta_n)=0} (x_1^{\overline{\delta_1}} \vee \ldots \vee x_n^{\overline{\delta_n}}).$$

■

5. Лемма о сводимости полных систем булевых функций. Существование конечной полной подсистемы в полной системе булевых функций. Примеры полных систем.

Определение 1. Система F булевых функций называется *полной*, если любая функция алгебры логики выражается формулой над F.

Примечание. Очевидно, что множество P_2 полно. Кроме того, согласно доказанной выше теореме, множество $\{\overline{x}, xy, x \vee y\}$ тоже полно.

Лемма 1 (О сводимости полных систем)**.** Пусть F — полная система булевых функций и любая функция из множества F выражается формулой над системой G. Тогда G — полная система.

Доказательство. В самом деле, рассматривая формулу для функции f над системой F, заменим каждую функцию на её выражение из G, получим формулу для произвольной функции f над системой G. ■

Теорема 1. В любой полной системе булевых функций можно выделить конечную полную подсистему.

Доказательство. Пусть есть бесконечная полная система F. Раз она полна, то существуют конечные формулы для $\{\overline{x}, xy, x \vee y\}$. Тогда по лемме о сводимости полных систем функции в этих формулах будут образовывать конечную полную подсистему. ■

С помощью данной леммы можем привести ещё ряд примеров полных систем:

1. $\{\overline{x}, xy\}$ полно, т. к. $\{\overline{x}, xy, x \vee y\}$ полно и $x \vee y = \overline{\overline{x}\,\overline{y}}$;
2. $\{\overline{x}, x \vee y\}$ полно — аналогично;
3. $\{x \mid y\}$ полно, т. к. $x \mid x = \overline{x}$, а $(x \mid y) \mid (x \mid y) = \overline{x \mid y} = xy$;
4. $\{x \downarrow y\}$ полно — аналогично;
5. $\{0, 1, xy, x \oplus y\}$ полно, т. к. $\overline{x} = x \oplus 1$.

6. Полином Жегалкина. Существование и единственность представления булевой функции в виде полинома Жегалкина.

Определение 1. *Элементарная конъюнкция* — выражение вида $x_{i_1}^{\sigma_1} x_{i_2}^{\sigma_2} \dots x_{i_k}^{\sigma_k}$, $k \geqslant 1$.

Определение 2. *Полином Жегалкина* — выражение вида $\sum\limits_{\{i_1,\dots,i_s\}\subseteq\{1,\dots,n\}} a_{i_1\dots i_s} x_{i_1} \cdot \dots \cdot x_{i_s}$.

Примечание. Можно рассматривать полином Жегалкина, как сумму по модулю 2 произвольного подмножества множества K_n^* конъюнкций вида $x_{i_1} x_{i_2} \dots x_{i_k}$, к которому добавлена константа 1, которую будем называть конъюнкцией длины 0 от пустого множества переменных.

Теорема 1 (Жегалкин)**.** Каждая функция алгебры логики представима в виде полинома Жегалкина, причём единственным образом.

Доказательство. Существование следует из полноты системы $\{0, 1, xy, x \oplus y\}$. Единственность следует из количества полиномов. В самом деле, возможных слагаемых в сумме ровно $2^n = |K_n^*|$. И каждое либо есть в нашей сумме, либо нет. Получаем $2^{2^n} = |P_2(n)|$. ■

7. Замыкание множества функций. Свойства замыкания. Замкнутые классы булевых функций. Классы T_0 и T_1 функций, сохраняющих константы.

Определение 1. *Замыканием* $[M]$ множества M функций алгебры логики называется множество всех функций, которые можно получить при помощи операций суперпозиции и введения фиктивных переменных над M.

Определение 2. Множество M называется *замкнутым*, если $[M] = M$.

Определение 3. Если для множеств A и F булевых функций выполняется равенство $[A] = F$, то говорят, что система A *полна* в F.

Теорема 1 (Простейшие свойства замыкания)**.**

1. $[M] \supseteq M$ (экстенсивность);
2. $[[M]] = [M]$ (идемпотентность);
3. $M_1 \subseteq M_2 \Rightarrow [M_1] \subseteq [M_2]$ (монотонность);
4. $[M_1 \cup M_2] \supseteq [M_1] \cup [M_2]$;
5. $[M_1 \cap M_2] \subseteq [M_1] \cap [M_2]$.

Определение 4. $T_0 := \{f \in P_2 : f(0, \dots, 0) = 0\}$ («сохраняют 0»), $T_1 := \{f \in P_2 : f(1, \dots, 1) = 1\}$ («сохраняют 1»).

Теорема 2. Классы T_0 и T_1 замкнуты.

Доказательство. Добавление/изъятие фиктивной переменной не выводит за пределы класса. Доказательство проведём индукцией для формулы Φ, которая реализует функцию g. База $\Phi = x_i$ — верно. Предположим, что Φ_i лежит в T_0 как функция $f_i(x_1, \dots, x_m)$ (при необходимости добавим фиктивные переменные). Рассмотрим произвольную формулу над T_0, $\Phi = f(\Phi_1, \dots, \Phi_n)$, которая реализует функцию

$$g(x_1, \dots, x_m) = f(f_1(x_1, \dots, x_m), \dots, f_n(x_1, \dots, x_m)).$$

Тогда, поскольку $f, f_i \in T_0$,

$$g(0, \dots, 0) = f(f_1(0, \dots, 0), \dots, f_n(0, \dots, 0)) = f(0, \dots, 0) = 0 \Rightarrow g \in T_0.$$

А значит, любая суперпозиция функций из T_0 также является функцией из T_0. Доказательство для T_1 аналогично. ■

Предложение 1. $|T_0 \cap P_2(n)| = |T_1 \cap P_2(n)| = 2^{2^n-1}$.

Доказательство. Значение для одного набора уже задано, для остальных выбираются так же, как и раньше. ■

Предложение 2. $T_0 = [\{xy, x \oplus y\}]$, $T_1 = [\{x \vee y, x \sim y\}]$.

Доказательство. Для начала покажем, что $T_0 \subseteq [\{xy, x \oplus y\}]$. Рассмотрим полином Жегалкина для произвольной функции $f \in T_0$. На нулевом наборе, он должен принимать значение 0, а значит, свободный коэффициент в полиноме равен 0. Следовательно, полином получается суперпозициями над $\{xy, x \oplus y\}$. Обратное включение следует из монотонности замыкания: $\{xy, x \oplus y\} \subseteq T_0 \Rightarrow [\{xy, x \oplus y\}] \subseteq [T_0] = T_0$.

Доказательство для T_1 следует из принципа двойственности (см. билет 9). ■

8. Линейные функции. Замкнутость класса L. Лемма о нелинейной функции.

Определение 1. $L := \{f \in P_2(n) \mid f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus a_0, n \in \mathbb{Z}^+, a_i \in E\}$ — множество *линейных* функций.

Теорема 1. Класс L замкнут.

Доказательство. Добавление/изъятие фиктивной переменной не выводит за пределы класса. Доказательство проведём индукцией для формулы Φ, которая реализует функцию g. База $\Phi = x_i$ — верно. Предположим, что Φ_i лежит в L как функция $f_i(x_1, \ldots, x_m) = a_1^i x_1 \oplus \ldots \oplus a_m^i x_m \oplus a_0^i$ (при необходимости добавим фиктивные переменные). Рассмотрим произвольную формулу над L, $\Phi = f(\Phi_1, \ldots, \Phi_n)$, которая реализует функцию

$$g(x_1, \ldots, x_m) = f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)).$$

Тогда, поскольку $f = a_1x_1 \oplus \ldots \oplus a_nx_n \oplus a_0$, $f_i \in L$,

$$\begin{aligned} g(x_1, \ldots, x_m) &= f(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)) = \\ &= f(a_1^1x_1 \oplus \ldots \oplus a_m^1x_m \oplus a_0^1, \ \ldots, \ a_1^nx_1 \oplus \ldots \oplus a_m^nx_m \oplus a_0^n) = \\ &= a_1(a_1^1x_1 \oplus \ldots \oplus a_m^1x_m \oplus a_0^1) \oplus \ldots \oplus a_n(a_1^nx_1 \oplus \ldots \oplus a_m^nx_m \oplus a_0^n) \oplus a_0 = \\ &= \left(\sum_{i_1=1}^{n} a_{i_1}a_1^{i_1}\right)x_1 \oplus \ldots \oplus \left(\sum_{i_m=1}^{n} a_{i_m}a_m^{i_m}\right)x_m \oplus \left(\sum_{i_0=1}^{n} a_{i_0}a_0^{i_0} \oplus a_0\right) \Rightarrow g \in L. \end{aligned}$$

А значит, любая суперпозиция функций из L также является функцией из L. ■

Предложение 1. $|L \cap P_2(n)| = 2^{n+1}$.

Доказательство. Любая n-местная линейная функция имеет вид $a_1x_1 \oplus \ldots \oplus a_nx_n \oplus a_0$. Таким образом, у нас $n+1$ неизвестных коэффициентов из E, число способов их выбрать равно 2^{n+1}. ■

Предложение 2. $L = [\{1, x \oplus y\}]$.

Лемма 1 (Лемма о нелинейной функции)**.** Если $f_L \in P_2 \setminus L$, то из f_L, 0, 1 и $\overline{x}$ суперпозициями можно получить функцию $x_1 \cdot x_2$.

Доказательство. Рассмотрим многочлен Жегалкина функции f_L:

$$f_L(x_1, \ldots, x_n) = \sum_{\{i_1,\ldots,i_s\} \subseteq \{1,\ldots,n\}} a_{i_1\ldots i_s}x_{i_1} \ldots x_{i_s}.$$

Т. к. $f_L \notin L$, то без ограничения общности можно считать, что в мономе степени больше 1 есть переменные x_1 и x_2. Перегруппируем члены полинома:

$$f_L(x_1,\dots,x_n) = x_1x_2f_1(x_3,\dots,x_n) \oplus x_1f_2(x_3,\dots,x_n) \oplus x_2f_3(x_3,\dots,x_n) \oplus f_4(x_3,\dots,x_n).$$

Т. к. полином Жегалкина единственный, то $f_1 \neq 0$. Значит, найдутся такие $\alpha_3,\dots,\alpha_n \in E$, что $f_1(\alpha_3,\dots,\alpha_n) = 1$. Рассмотрим функцию $\varphi(x_1,x_2) := f_L(x_1,x_2,\alpha_3,\dots,\alpha_n)$. Имеем $\varphi(x_1,x_2) = x_1x_2 \oplus \alpha x_1 \oplus \beta x_2 \oplus \gamma$ для каких-то $\alpha,\beta,\gamma \in E$. Избавимся от линейных членов (при необходимости заменяя $x_i \oplus 1$ на $\overline{x}_i$, в противном случае оставляя x_i):

$$\varphi(x_1 \oplus \beta, x_2 \oplus \alpha) = (x_1 \oplus \beta)(x_2 \oplus \alpha) \oplus \alpha(x_1 \oplus \beta) \oplus \beta(x_2 \oplus \alpha) \oplus \gamma = x_1x_2 \oplus (\alpha\beta \oplus \gamma).$$

Отсюда $x_1x_2 = \varphi(x_1 \oplus \beta, x_2 \oplus \alpha) \oplus (\alpha\beta \oplus \gamma)$. Теперь вспомним, что $x \oplus 1 = \overline{x}$, поэтому если $\alpha\beta \oplus \gamma = 1$, то получаем $x_1x_2 = \overline{\varphi(\dots)}$. Итак, мы получили $x_1 \cdot x_2$ как суперпозицию f_L, 0, 1 и $\overline{x}$. ■

9. Двойственные и самодвойственные функции. Замкнутость класса S. Принцип двойственности. Лемма о несамодвойственной функции.

Определение 1. Функция $g(x_1,\dots,x_n) := \overline{f(\overline{x}_1,\dots,\overline{x}_n)}$ называется *двойственной* к функции $f(\widetilde{x}^n)$. Обозначение $g = f^*$.

Примечание. Очевидно, что $(f^*)^* = f$. Таблица для функции f^* получается инвертированием всех битов таблицы для функции f.

Определение 2. Если $f = f^*$, то функция f называется *самодвойственной*.

Определение 3. $S := \{f \in P_2 : f = f^*\}$ — класс *самодвойственных* функций.

Теорема 1. Класс S замкнут.

Доказательство. Добавление/изъятие фиктивной переменной не выводит за пределы класса. Доказательство проведём индукцией для формулы Φ, которая реализует функцию g. База $\Phi = x_i$ — верно. Предположим, что Φ_i лежит в S как функция $f_i(x_1,\dots,x_m)$ (при необходимости добавим фиктивные переменные). Рассмотрим произвольную формулу над S, $\Phi = f(\Phi_1,\dots,\Phi_n)$, которая реализует функцию

$$g(x_1,\dots,x_m) = f(f_1(x_1,\dots,x_m),\dots,f_n(x_1,\dots,x_m)).$$

Тогда, поскольку $f, f_i \in S$,

$$g^*(x_1,\dots,x_m) = \overline{f(f_1(\overline{x}_1,\dots,\overline{x}_m),\dots,f_n(\overline{x}_1,\dots,\overline{x}_m))} = \overline{f(\overline{f_1(x_1,\dots,x_m)},\dots,\overline{f_n(x_1,\dots,x_m)})} =$$
$$= f(f_1(x_1,\dots,x_m),\dots,f_n(x_1,\dots,x_m)) = g(x_1,\dots,x_m) \Rightarrow g \in S.$$

А значит, любая суперпозиция функций из S также является функцией из S. ■

Теорема 2 (Принцип двойственности)**.** Если в произвольной формуле Φ, реализующей булеву функцию f, заменить все функциональные символы на функциональные символы двойственных функций, то получившаяся формула Φ^* будет реализовывать функцию f^*.

Доказательство. Проведём доказательство по индукции. База $\Phi = x_i, \Phi^* = x_i$. Пусть теорема верна для формул $\Phi_1,\dots,\Phi_m$, $\Phi_i = f_i(x_1,\dots,x_n)$. Докажем для $\Phi = f_0(\Phi_1,\dots,\Phi_m)$. По условию теоремы формула Φ задает булеву функцию $f(x_1,\dots,x_n)$, тогда

$$\Phi = f(x_1,\dots,x_n) = f_0(f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)).$$

Рассмотрим двойственную ей формулу:

$$\Phi^* = f_0^*(f_1^*(x_1,\dots,x_n),\dots,f_m^*(x_1,\dots,x_n)) = f_0^*(\overline{f_1(\overline{x}_1,\dots,\overline{x}_n)},\dots,\overline{f_m(\overline{x}_1,\dots,\overline{x}_n)}) =$$
$$= \overline{f_0(\overline{\overline{f_1(\overline{x}_1,\dots,\overline{x}_n)}},\dots,\overline{\overline{f_m(\overline{x}_1,\dots,\overline{x}_n)}})} = \overline{f_0(f_1(\overline{x}_1,\dots,\overline{x}_n),\dots,f_m(\overline{x}_1,\dots,\overline{x}_n))} = f^*(x_1,\dots,x_n).$$

■

Лемма 1 (О несамодвойственной функции)**.** Если $f_S \in P_2 \setminus S$, то из f_S и $\overline{x}$ суперпозициями можно получить константу.

Доказательство. Из $f_S \notin S$, найдётся $(\alpha_1,\dots,\alpha_n) \in B_n$ такое, что $f_S(\alpha_1,\dots,\alpha_n) = f_S(\overline{\alpha}_1,\dots,\overline{\alpha}_n)$. Рассмотрим функции $\varphi_i(x) := x^{\alpha_i}$ $(i = 1,\dots,n)$. Положим $\varphi(x) := f_S(\varphi_1(x),\dots,\varphi_n(x))$. Очевидно, функция φ получена суперпозициями из f_S и $\overline{x}$. Имеем:

$$\varphi(0) = f_S(\varphi_1(0),\dots,\varphi_n(0)) = f_S(0^{\alpha_1},\dots,0^{\alpha_n}) = f_S(\overline{\alpha_1},\dots,\overline{\alpha_n}) = f_S(\alpha_1,\dots,\alpha_n) =$$
$$= f_S(1^{\alpha_1},\dots,1^{\alpha_n}) = f_S(\varphi_1(1),\dots,\varphi_n(1)) = \varphi(1).$$

Значит, φ — константа. ■

Предложение 1. $|S \cap P_2(n)| = 2^{2^{n-1}}$.

Доказательство. Т. к. на инвертированных наборах функция $f \in S \cap P_2(n)$ принимает инвертированное значение, то её можно задать, заполнив половину таблицы, т. е. она однозначно определяется на $2^n/2 = 2^{n-1}$ наборах. ■

Упражнение 1. Докажите, что $S = [\{x \oplus y \oplus z, xy \vee xz \vee yz, \overline{x}\}]$.

10. Монотонные функции. Замкнутость класса M. Лемма о немонотонной функции.

Определение 1. Пусть $\widetilde{\alpha} = (\alpha_1,\dots,\alpha_n), \widetilde{\beta} = (\beta_1,\dots,\beta_n) \in B_n$. Скажем, что набор $\widetilde{\alpha}$ *не больше* набора $\widetilde{\beta}$ ($\widetilde{\alpha} \leqslant \widetilde{\beta}$), если $\alpha_i \leqslant \beta_i$ $\forall i = 1,\dots,n$.

Примечание. Данное отношение является отношением частичного порядка на B_n. Легко привести пару несравнимых наборов — $(0,1)$ и $(1,0)$.

Определение 2. $M := \{f \in P_2 : \widetilde{\alpha} \leqslant \widetilde{\beta} \Rightarrow f(\widetilde{\alpha}) \leqslant f(\widetilde{\beta})\}$ — множество *монотонных функций.*

Теорема 1. Класс M замкнут.

Доказательство. Добавление/изъятие фиктивной переменной не выводит за пределы класса. Доказательство проведём индукцией для формулы Φ, которая реализует функцию g. База $\Phi = x_i$ — верно. Предположим, что Φ_i лежит в M как функция $f_i(x_1,\dots,x_m)$ (при необходимости добавим фиктивные переменные). Рассмотрим произвольную формулу над M, $\Phi = f(\Phi_1,\dots,\Phi_n)$, которая реализует функцию

$$g(x_1,\dots,x_m) = f(f_1(x_1,\dots,x_m),\dots,f_n(x_1,\dots,x_m)).$$

Тогда, поскольку $f, f_i \in M$, для двух наборов $\widetilde{\alpha}$, $\widetilde{\beta}$: $\widetilde{\alpha} \leqslant \widetilde{\beta}$, $f_i(\widetilde{\alpha}) \leqslant f_i(\widetilde{\beta})$ и справедливо

$$g(\widetilde{\alpha}) = f(f_1(\widetilde{\alpha}),\dots,f_n(\widetilde{\alpha})) \leqslant f(f_1(\widetilde{\beta}),\dots,f_n(\widetilde{\beta})) = g(\widetilde{\beta}) \Rightarrow g \in M.$$

А значит, любая суперпозиция функций из M также является функцией из M. ■

Лемма 1 (О немонотонной функции)**.** Если $f_M \in P_2 \setminus M$, то из f_M, 0 и 1 суперпозициями можно получить $\overline{x}$.

Доказательство. Из $f_M \notin M$, найдутся наборы $\widetilde{\alpha}, \widetilde{\beta} \in B_n$ такие, что $\widetilde{\alpha} \leqslant \widetilde{\beta}$ и $f_M(\widetilde{\alpha}) = 1$, а $f_M(\widetilde{\beta}) = 0$. Последовательно будем менять набор $\widetilde{\alpha}$ так, чтобы $\alpha_i = \beta_i$ (покоординатно). В силу дискретной непрерывности найдётся такое j, что $f_M(\ldots, \alpha_j, \ldots) = 1$, $f_M(\ldots, \beta_j, \ldots) = 0$, $\alpha_j = 0 < 1 = \beta_j$, а значит, $\varphi(x) = f_M(\ldots, x, \ldots) = \overline{x}$. ■

Предложение 1. $|M \cap P_2(n)| \geqslant 2^{C_n^{\lfloor n/2 \rfloor}}$.

Доказательство. Рассмотрим множество всех наборов из B_n с числом единиц $\left\lfloor \frac{n}{2} \right\rfloor$. Таких наборов $C_n^{\left\lfloor \frac{n}{2} \right\rfloor}$. Зададим функцию следующим образом: на всех таких наборах выберем значения произвольным образом, на наборах с меньшим числом единиц — ноль, большим — единицу. Все такие функции монотонны, а количество способов определить функцию на $C_n^{\left\lfloor \frac{n}{2} \right\rfloor}$ наборах ровно $2^{C_n^{\lfloor n/2 \rfloor}}$. Оценка сверху — куда более сложная задача, которая здесь не рассматривается. ■

Предложение 2. Если $f(\widetilde{x}) \in M$, то $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1}, 0) \vee f(x_1, \ldots, x_{n-1}, 1)x_n$.

Доказательство. Очевидно верно при $x_n = 0$ и $x_n = 1$. ■

Предложение 3. $[\{0, 1, xy, x \vee y\}] = M$.

Доказательство. $M \subseteq [\{0, 1, xy, x \vee y\}]$, т. к. любую функцию из M можно выразить через эти функции (прямое следствие предложения 2). $[\{0, 1, xy, x \vee y\}] \subseteq M$, в силу монотонности замыкания ($\{0, 1, xy, x \vee y\} \subseteq M$, а значит, $[\{0, 1, xy, x \vee y\}] \subseteq [M] = M$). ■

11. Критерий Поста полноты множества функций в P_2. Следствие о существовании в любом полном множестве полного подмножества из не более чем 4 функций. Пример базиса в P_2, состоящего из четырех функций.

Теорема 1 (Критерий Поста)**.** Система функций из P_2 полна тогда и только тогда, когда она не содержится ни в одном из классов T_0, T_1, L, S, M.

Доказательство. $\Rightarrow$. Пусть F полна и $F \subseteq K$, где $K \in \{T_0, T_1, L, S, M\}$. Тогда $[F] \subseteq [K] = K \neq P_2$.

$\Leftarrow$. Обратно, пусть $F \not\subseteq T_0$, $F \not\subseteq T_1$, $F \not\subseteq L$, $F \not\subseteq S$, $F \not\subseteq M$. Тогда в F найдутся $f_0 \notin T_0$, $f_1 \notin T_1$, $f_L \notin L$, $f_S \notin S$, $f_M \notin M$. Возможны два случая:

1. $f_0 \in T_1$. Тогда $\varphi(x) := f_0(x, \ldots, x) = 1$. Так получаем константу 1. Чтобы получить константу 0, достаточно теперь воспользоваться функцией f_1. Теперь по лемме о немонотонной функции, из f_M, 0, 1 можно получить $\overline{x}$.

2. $f_0 \notin T_1$. Тогда $\varphi(x) := f_0(x, \ldots, x) = \overline{x}$. По лемме о несамодвойственной функции, из f_S и $\overline{x}$ можно получить константу. Имея отрицание, получаем также и другую константу.

По лемме о нелинейной функции, из f_L, 0, 1 и $\overline{x}$ можно получить $x_1 \cdot x_2$. Следовательно, из F можно выразить полную систему $\{\overline{x}, x_1 \cdot x_2\}$, поэтому F также полна. ■

Следствие 1. Каждый замкнутый класс функций из P_2, отличный от P_2, содержится хотя бы в одном из классов T_0, T_1, L, S, M.

Доказательство. Действительно, если бы он не содержался ни в одном из этих классов, то был бы полон, а т. к. замкнут, то совпал бы с P_2. ■

Следствие 2. В любой полной системе существует полная подсистема, состоящая не более, чем из 4 функций.

Доказательство. В первом случае доказательства нужно брать f_0, f_1, f_M, f_L, а во втором f_0, f_S, f_L. ■

Пример 1 (Полная система из 4 функций)**.** $\{0, 1, x \oplus y \oplus z, x\&y\}$.

12. Предполные классы. Теорема о предполных классах в P_2.

Лемма 1. Для любых двух классов из множества T_0, T_1, L, S, M найдется функция, лежащая в одном и не лежащая в другом.

Доказательство. Рассмотрим таблицу:

	T_0	T_1	S	M	L
0	$+$	$-$	$-$	$+$	$+$
1	$-$	$+$	$-$	$+$	$+$
$\overline{x}$	$-$	$-$	$+$	$-$	$+$
$x \cdot y$	$+$	$+$	$-$	$+$	$-$
$x \oplus y$	$+$	$-$	$-$	$-$	$+$
$x \oplus y \oplus z$	$+$	$+$	$+$	$-$	$+$
$m(x, y, z)$	$+$	$+$	$+$	$+$	$-$

$m(x, y, z)$ — *функция голосования* (см. билет 2). В приведённой таблице для каждой упорядоченной пары классов существует функция, содержащаяся в первом, но не содержащаяся во втором. ■

Определение 1. Класс функций $A \subset P_2$ называется *предполным*, если

1. система A не полная;
2. $\forall f \notin A$ система $A \cup \{f\}$ — полная.

Примечание. Любой предполный класс замкнут.

Доказательство. Предположим противное. Рассмотрим $f \in [K] \setminus K$. $[K \cup \{f\}] = P_2$. С другой стороны, $K \cup \{f\} \subseteq [K]$, а значит, $[K \cup \{f\}] \subseteq [[K]] = [K] \neq P_2$. Противоречие. ■

Теорема 1. В P_2 ровно 5 предполных классов: T_0, T_1, L, S, M.

Доказательство. Действительно, если класс K предполон, то он, согласно следствию 1 из билета 11, должен содержаться в одном из классов T_0, T_1, L, S, M. Пусть он содержится в классе Q. K не может быть собственным подмножеством Q, поскольку можно взять $f \in Q \setminus K$, и тогда $[K \cup \{f\}] \subseteq Q$. Противоречие, предполными классами могут быть только T_0, T_1, L, S, M.

Теперь докажем, что все они — предполные классы. Рассмотрим произвольный класс Q из указанных пяти классов. Возьмём произвольную функцию алгебры логики f, не принадлежащую Q. Тогда $[Q \cup \{f\}] = P_2$, поскольку ни один класс полностью не содержится в другом, и $f \notin Q$. ■

13. Функции k-значной логики ($k \geqslant 3$). Число функций k-значной логики от n фиксированных переменных. Существенные и фиктивные переменные для функций k-значной логики, отличие от случая булевых функций. Элементарные функции k-значной логики, их свойства.

Определение 1. $E_k := \{0, 1, \ldots, k-1\}$.

Определение 2. Функцию $f(x_1, \ldots, x_n) : E_k^n \to E_k$ будем называть *функцией k-значной логики.* Множество всех таких функций обозначается как P_k.

Теорема 1. Число функций k-значной логики от n переменных равно k^{k^n}.

Доказательство. В самом деле, наша функция определяется значениями, которые она принимает на k^n наборах. Для каждого набора k значений, а значит, способов выбрать значения k^{k^n}. ■

Определение 3. Функция k-значной логики $f(\widetilde{x}^n)$ называется *существенно зависящей от переменной* x_i $(i = 1, \ldots, n)$, если существуют значения $\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n$, σ', σ'' из E_k такие, что

$$f(\sigma_1, \ldots, \sigma_{i-1}, \sigma', \sigma_{i+1}, \ldots, \sigma_n) \neq f(\sigma_1, \ldots, \sigma_{i-1}, \sigma'', \sigma_{i+1}, \ldots, \sigma_n).$$

В этом случае x_i называется *существенной переменной функции* f. Переменная, не являющаяся существенной называется *фиктивной*.

Определение 4. Пусть x_i — фиктивная переменная функции $f(\widetilde{x}^n)$. Тогда функция

$$g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) := f(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$$

называется *полученной из* f *удалением фиктивной переменной* x_i. Обратно, говорят, что f *получена из* g *добавлением* i*-ой фиктивной переменной*.

Определение 5. Две функции k-значной логики f и g называются *одинаковыми*, если у них одинаковое множество переменных и на любом наборе этих переменных функции принимают одинаковые значения.

Определение 6. Две функции k-значной логики f и g называются *равными*, если одну из другой можно получить за конечное число применений операций добавления и удаления фиктивных переменных.

Отличие от случая булевых функций заключается в том, что при подстановке одной функции в другую существенная зависимость переменных не сохраняется, в отличие от P_2. Достаточно привести пример:

Пример 1.

Функция $\varphi(x, y)$ существенно зависит от переменных x, y.
Однако $\varphi(x, \varphi(x, y))$ — тождественный ноль.

x \ y	0	1	2
0	0	0	0
1	0	0	0
2	0	0	1

Как и в случае алгебры логики, выделяется некоторый **список элементарных функций**:

1. *Константы* $0, 1, \ldots, k-1$ и *тождественная функция* x.
2. $\overline{x} := x + 1 \pmod k$ — *отрицание Поста*.
3. $\sim x := k - 1 - x$ — *отрицание Лукашевича*.
4. $I_\sigma(x) := \begin{cases} k-1, & \text{если } x = \sigma, \\ 0, & \text{иначе} \end{cases}$ — *индикаторная функция*, принимающая в σ «большое значение».
5. $j_\sigma(x) := \begin{cases} 1, & \text{если } x = \sigma, \\ 0, & \text{иначе} \end{cases}$ — *индикаторная функция*, принимающая в σ «маленькое значение».
6. $\min(x, y)$ — возможное обобщение конъюнкции (часто будем обозначать через $x\&y$).
7. $x \cdot y \pmod k$ — другое возможное обобщение конъюнкции.
8. $\max(x, y)$ — возможное обобщение дизъюнкции (часто будем обозначать через $x \vee y$).
9. $x + y \pmod k$ — другое возможное обобщение дизъюнкции.

Отметим следующие **свойства операций**:

1. Операции $\min(x_1, x_2)$, $\max(x_1, x_2)$, $x_1 \cdot x_2 \pmod k$, $x_1 + x_2 \pmod k$ ассоциативны и коммутативны.
2. Дистрибутивности: $(x_1 \vee x_2)\&x_3 = (x_1\&x_3) \vee (x_2\&x_3)$, $(x_1\&x_2) \vee x_3 = (x_1 \vee x_3)\&(x_2 \vee x_3)$, $(x_1 + x_2) \cdot x_3 = x_1 \cdot x_3 + x_2 \cdot x_3 \pmod k$.
3. При $k > 2$: $\sim(\sim x) = x$, $\overline{\overline{x}} = x + 2 \pmod k$.
4. $\sim(\min(x_1, x_2)) = \max(\sim x_1, \sim x_2)$ — аналог закона де Моргана. Заметим, что для отрицания Поста аналогичное равенство при $k > 3$ тождеством не является.

14. Две универсальные формы представления произвольной функции k-значной логики. Полнота систем функций из этих универсальных форм.

Используя операции I_σ, $\vee$, $\&$ и константы, можно построить аналог СДНФ в k-значной логике. Именно, для произвольной функции $f \in P_k(n)$ имеет место следующее тождество:

Теорема 1.

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n)\in E_k^n} I_{\sigma_1}(x_1)\& \ldots \& I_{\sigma_n}(x_n)\& f(\sigma_1, \ldots, \sigma_n).$$

Доказательство. В самом деле, при $\widetilde{x} \neq \widetilde{\sigma}$, конъюнкция равна 0, и она не влияет на сумму. При $\widetilde{x} = \widetilde{\sigma}$ конъюнкция равна $f(\sigma_1, \ldots, \sigma_n)$. ■

Теорема 2.

$$f(x_1, \ldots, x_n) = \sum_{(\sigma_1,\ldots,\sigma_n)\in E_k^n} j_{\sigma_1}(x_1) \cdot \ldots \cdot j_{\sigma_n}(x_n) \cdot f(\sigma_1, \ldots, \sigma_n) \pmod k.$$

Доказательство. Аналогично. ■

Отсюда вытекают следующие теоремы:

Теорема 3. $[\{0, 1, \ldots, k-1, I_0(x), \ldots, I_{k-1}(x), x\&y, x \vee y\}] = P_k$.

Теорема 4. $[\{0, 1, \ldots, k-1, j_0(x), \ldots, j_{k-1}(x), x \cdot y \pmod k, x + y \pmod k\}] = P_k$.

15. Полнота системы $\{\max(x, y), \overline{x}\}$ в P_k. Функция Вебба. Полнота системы, состоящей только из функции Вебба

Теорема 1. Система $\{\max(x, y), \overline{x}\}$ полна в P_k.

Доказательство.

1. Получение констант. Построим сначала константы, начиная с $k-1$:

   $$k - 1 = \max(x, x + 1, \ldots, x + k - 1), \text{ где } x + i = \overline{\overline{\ldots \overline{x}}}.$$

   Остальные константы получаются при помощи функции $x + 1 \pmod k$.

2. Построение функций $I_i(x), i = 0, 1, \ldots, k-1$: $I_0(x) = \max(x, x + 1, \ldots, x + k - 2) + 1$;

   $$I_i(x) = I_0(x - i).$$

3. Получение функции $\min(x, y)$ при наличии функции $\sim x$:

   $$\min(x, y) = \sim (\max(\sim x, \sim y)).$$

4. Построение произвольной функции $g(x)$ одной переменной.

   4.1 Для произвольных α, β из E_k построим функцию $\varphi_{\alpha,\beta}(x) = \begin{cases} \beta, & \text{если } x = \alpha, \\ 0, & \text{иначе} \end{cases}$, используя формулу:

   $$\varphi_{\alpha,\beta}(x) = \max(I_\alpha(x), k - 1 - \beta) + \beta + 1 \pmod k.$$

   4.2 Представление функции $g(x)$:

   $$g(x) = \max(\varphi_{0,g(0)}(x), \varphi_{1,g(1)}(x), \ldots, \varphi_{k-1,g(k-1)}(x)).$$

Таким образом, получаем $\sim x$ и выражение системы из теоремы 3 через систему $\{\max(x,y), \overline{x}\}$. ■

Определение 1. $V_k(x,y) := \max(x,y) + 1 \pmod k$ — *функция Вебба.*

Теорема 2. Система $\{V_k(x,y)\}$ полна в P_k.

Доказательство. Из функции Вебба получается отрицание Поста $V_k(x,x) = x+1 = \overline{x}$. Следовательно, получаем функции $x+i$ $(i = 0, \ldots, k-1)$. Теперь получаем $\max(x,y) = V_k(x,y) + (k-1)$. Имеем всю полную систему $\{\overline{x}, \max(x,y)\}$. ■

16. Алгоритм распознавания полноты системы функций k-значной логики. Исследование полноты систем функций k-значной логики на практике.

Определение 1. Пусть F — произвольное множество функций из P_k , а $\widetilde{x}$ — набор переменных $(x_1, \ldots, x_p)$, $p \geqslant 1$. Через $F[\widetilde{x}]$ или через $F[x_1, \ldots, x_p]$ обозначим множество функций из F, зависящих от переменных $x_1, \ldots, x_p$.

Теорема 1. Существует алгоритм распознавания полноты конечных систем функций из P_k.

Доказательство. Пусть $F = \{f^1(x_1, \ldots, x_{n_1}), \ldots, f^t(x_1, \ldots, x_{n_t})\} \subset P_k$. Последовательно построим множества функций R_0, R_1, ... из $P_k[x_1, x_2]$:

1. $R_0 = \varnothing$;
2. Если построено множество R_s, то множество R_{s+1} — это множество всех функций, задаваемых формулами вида $f^i(A_1, \ldots, A_{n_i})$, где $f^i \in F$, а A_j либо x_1, x_2, либо функция из R_s.

Последовательность $R_0 \subseteq R_1 \subseteq \ldots \subseteq R_s \subseteq R_{s+1} \subseteq \ldots$ в какой-то момент стабилизируется (в силу ограниченности количества функций от двух переменных), т. е. найдётся такое r, что

$$R_r = R_{r+1} = \ldots.$$

Система F будет полной в том и только том случае, когда $V_k(x_1, x_2) \in R_r$. В самом деле, если $V_k(x_1, x_2) \in R_r$, то значит суперпозициями над F можно получить полную систему, а значит система F полна. И обратно, если $V_k(x_1, x_2) \notin R_r$, значит суперпозициями над F нельзя получить функцию из P_k, а значит, F неполна. ■

17. Классы сохранения множеств функций и их свойства. Теорема Кузнецова о функциональной полноте функций k-значной логики.

Пусть A — некоторое множество функций из P_k, удовлетворяющее следующим условиям:

1. Каждая функция из A зависит от одного и того же набора переменных y_1, ..., y_p, $p \geqslant 1$;
2. Функции $g_i(y_1, \ldots, y_p) = y_i$, $i = 1, \ldots, p$ лежат в A.

Определение 1. Функция $f(x_1, \ldots, x_n)$ *сохраняет множество функций* A, если $\forall h_1, \ldots, h_n \in A$, функция $f(h_1, \ldots, h_n) \in A$. Обозначим M_A — множество всех функций, сохраняющих A.

Лемма 1. M_A — замкнутый класс.

Доказательство. Множество M_A содержит тождественную функцию. Поэтому достаточно показать, что если $f_0(z_1, \ldots, z_m) \in M_A$ и $f_1, \ldots, f_m \in M_A$, то и $f = f_0(f_1, \ldots, f_m)$ принадлежит множеству M_A.

Возьмём произвольный набор функций $h_1, \ldots, h_n$ из A. Т. к. f_i $(i = 1, \ldots, m)$ сохраняет множество A, то $f_i(h_1, \ldots, h_n) \in A$, а значит, и $f_0(f_1(h_1, \ldots, h_n), \ldots, f_m(h_1, \ldots, h_n)) \in A$ — сохраняет множество A, следовательно, $f_0(f_1, \ldots, f_m) \in M_A$. ■

Лемма 2. Если $[A][\widetilde{x}] = A$, то $(M_A)[\widetilde{x}] = A$.

Доказательство. Рассмотрим $f(x_1, \ldots, x_p)$. Покажем включения в обе стороны:

1. $A \subseteq M_A[\widetilde{x}]$. Пусть $f \in A$. Для произвольных $h_1, \ldots, h_p \in A$, $g = f(h_1, \ldots, h_p) \in [A][\widetilde{x}]$. По условию $[A][\widetilde{x}] = A$, а значит, f сохраняет A, $f \in M_A$.

2. $M_A[\widetilde{x}] \subseteq A$. Пусть $f \in M_A[\widetilde{x}]$. Тогда f зависит только от $x_1, \ldots, x_p$. Следовательно,

$$f(x_1, \ldots, x_p) = f(g_1(x_1, \ldots, x_p), \ldots, g_p(x_1, \ldots, x_p)),$$

   где $g_i(x_1, \ldots, x_p) = x_i$. Так как функция f сохраняет множество A, а функции $g_1, \ldots, g_p$ лежат в множестве A, то $f(g_1, \ldots, g_p) \in A$, т. е. $f \in A$.

■

Теорема 1 (А. В. Кузнецов)**.** Для любого $k \geqslant 2$ в P_k существует конечное число замкнутых классов $M_1, \ldots, M_s$, таких, что ни один из них не содержится ни в одном из остальных и произвольная система F из P_k полна тогда и только тогда, когда F целиком не содержится ни в одном из классов $M_1, \ldots, M_s$.

Доказательство. Построим сначала систему классов. Пусть $A_1, \ldots, A_l$ — система всех собственных подмножеств множества $(P_k)[x_1, x_2]$, таких, что для всех $i = 1, \ldots, l$ выполняются следующие условия:

1. функции $g_1(x_1, x_2) = x_1$, $g_2(x_1, x_2) = x_2$ содержатся в A_i;
2. $[A_i][x_1, x_2] = A_i$.

Указанная система может быть построена путем перебора всех собственных подмножеств множества $P_k(2)$. Поскольку $|P_k(2)| = k^{k^2}$, то число таких подмножеств не превышает $2^{k^{k^2}}$.

Положим $G_i = M_{A_i}$. Из лемм следует, что G_i — замкнутый класс, такой, что $[G_i][x_1, x_2] = A_i$. Теперь из системы G_i удалим классы, которые содержатся в каком-либо из других, получаем систему $M_1, \ldots, M_s$, где $M_i \neq P_k$, $M_i \neq M_j$ при всех $i, j = 1, \ldots, s$, $i \neq j$.

Теперь покажем, что это искомая система классов. Пусть F — произвольная система из P_k. Если $F \subseteq M_i$, то $[F] \subseteq [M_i] = M_i \neq P_k$, то F — неполная система.

Пусть F — не содержится ни в одном из классов M_i. Положим $F_1 = F \cup \{g_1(x_1, x_2), g_2(x_1, x_2)\}$. Очевидно, что $[F] = P_k \Leftrightarrow [F_1] = P_k$. Положим $B = [F_1][x_1, x_2]$. Покажем, что B содержит все функции из P_k от переменных x_1 и x_2. Поскольку функции $g_1(x_1, x_2) = x_1$ и $g_2(x_1, x_2) = x_2$ содержатся в B, и $[B][x_1, x_2] = B$, то найдётся такое i, $1 \leqslant i \leqslant l$, что $B = A_i$. Так как каждая функция из F_1 сохраняет множество $B = [F_1][x_1, x_2]$, то $F_1 \subseteq G_i = M_{A_i}$. Поэтому найдётся такое j, $1 \leqslant j \leqslant s$, что $F_1 \subseteq M_j$. Получаем, что $F \subseteq M_j$, противоречие, а значит, $B = P_k[x_1, x_2]$, следовательно $[F][x_1, x_2]$ содержит $V_k(x_1, x_2)$. Значит, F полна. ■

18. Представление функций k-значной логики полиномами. Малая теорема Ферма. Условие представления всех функций k-значной логики полиномами.

Теорема 1 (Малая теорема Ферма)**.** Если k — простое и $a \not\equiv 0 \pmod{k}$, то $a^{k-1} \equiv 1 \pmod{k}$.

Доказательство. Докажем, что все остатки от деления на k чисел $a, \ldots, (k-1)a$ различны.
В самом деле, если бы нашлись 2 числа ia, ja $(1 \leqslant i < j \leqslant k-1)$, имеющие одинаковые остатки,

то $ja - ia = (j-i)a$ делилось бы на k. Т. к $1 \leqslant (j-i) \leqslant k-2$ не делится на k, то a делится на k, противоречие. А значит,

$$a \cdot 2a \cdot \ldots \cdot (k-1)a \equiv 1 \cdot 2 \cdot \ldots \cdot (k-1) \pmod{k} \iff (k-1)!\, a^{k-1} \equiv (k-1)! \pmod{k}.$$

Т. к. $(k-1)! \not\equiv 0 \pmod{k}$, то $a^{k-1} \equiv 1 \pmod{k}$. ■

Теорема 2. Система $F = \{0, 1, \ldots, k-1, xy \pmod{k}, x+y \pmod{k}\}$ полна в $P_k \Leftrightarrow k$ — простое.

Доказательство. Отдельно рассмотрим случаи простого и составного k.

1. Пусть k — простое число. Используем второе представление произвольной функции f k-значной логики

$$f(x_1, \ldots, x_n) = \sum_{(\sigma_1, \ldots, \sigma_n) \in E_k^n} j_{\sigma_1}(x_1) \cdot \ldots \cdot j_{\sigma_n}(x_n) \cdot f(\sigma_1, \ldots, \sigma_n).$$

   В силу малой теоремы Ферма $j_0(x) = 1 - x^{k-1}$. Кроме того, $j_\sigma(x) = j_0(x - \sigma)$.

2. Пусть $k = k_1 k_2$, где $1 < k_1, k_2 < k$. Покажем, что функцию $j_0(x)$ нельзя представить в виде полинома. Предположим, что это не так, тогда $j_0(x) = c_0 + c_1 x + \ldots + c_{k-1} x^{k-1}$.
   Заметим, что $j_0(0) = 1$, а значит, $c_0 = 1$. При $x = k_1$ имеем:

$$0 = j_0(k_1) = 1 + c_1 k_1 + \ldots + c_{k-1} k_1^{k-1}.$$

   Умножая обе части на k_2, получаем $0 \equiv k_2 \pmod{k}$, что противоречит предположению.

■

19. Пример Янова замкнутого класса k-значной логики, не имеющего базиса.

Определение 1. Множество B функций k-значной логики называется *базисом* в замкнутом классе F, если выполняются два условия:

1. $[B] = F$;
2. для любого собственного подмножества A множества B равенство $[A] = F$ не выполняется.

Теорема 1 (Ю. И. Янов)**.** При $k \geqslant 3$ в P_k существует замкнутый класс, не имеющий базиса.

Доказательство. Рассмотрим следующую систему функций $F = \{f_0, \ldots, f_n, \ldots\}$, где $f_0 = 0$ и при любом $n \geqslant 1$

$$f_n(x_1, \ldots, x_n) = \begin{cases} 1, & \text{если } x_1 = \ldots = x_n = 2; \\ 0, & \text{иначе.} \end{cases}$$

Положим $M_k = [F]$. Любая нетривиальная суперпозиция равна 0, поэтому каждая функция из M_k получается из функций системы F подстановкой переменных. При $n > m$, f_m получается из f_n отождествлением некоторых переменных, поэтому в базисе класса M_k не может быть более одной функции, но и одной быть не может, т. к. f_n нельзя выразить через f_m. ■

20. Пример Мучника замкнутого класса k-значной логики со счётным базисом. Континуальность семейства замкнутых классов функций k-значной логики.

Теорема 1 (А. А. Мучник)**.** При $k \geqslant 3$ семейство замкнутых классов функций k-значной логики континуально.

Доказательство. Количество замкнутых классов не более числа различных подмножеств счётного множества, т. е. семейство замкнутых классов функций k-значной логики не более чем континуально.

Построим континуальное семейство замкнутых классов. Для $s = 2, 3, \ldots$ определим (симметрическую) функцию $f_s(x_1, \ldots, x_s)$ следующим образом. Функция f_s принимает значение 1 на наборах, состоящих из $s-1$ двойки и одной единицы, и значение 0 на всех остальных наборах.

Положим $F = \bigcup\limits_{i=2}^{\infty} \{f_i\}$. Покажем, что $f_s \notin [F \setminus \{f_s\}]$ для любого $s \geqslant 2$. Пусть это не так, т. е.

$$f_s(x_1, \ldots, x_s) = f_n(A_1, \ldots, A_n).$$

Возможны три случая:

1. Если среди A_i хотя бы две нетривиальные формулы, то $f_n(A_1, \ldots, A_n)$ — тождественный 0, противоречие.

2. Если среди A_i одна нетривиальная формула (пусть это i-ая формула), то найдётся тривиальная формула $A_j = x_j$, тогда если $x_j = 1$, а оставшиеся переменные примем за 2, получим

   $$f_s(2, \ldots, 1, \ldots, 2) = 1 \neq 0 = f_n(2, \ldots, 1, \ldots, A_i, \ldots, 2),$$

   где A_i нетривиальная, поэтому на этом наборе равна 1 или 0. Противоречие.

3. Если среди A_i все формулы тривиальные, то т. к. $n > s$, хотя бы одна переменная x_j встретится дважды, тогда если $x_j = 1$, а оставшиеся переменные примем за 2, получим

   $$f_s(2, \ldots, 1, \ldots, 2) = 1 \neq 0 = f_n(2, \ldots, 1, \ldots, 1, \ldots, 2),$$

   что приводит к противоречию.

Осталось построить континуальное семейство замкнутых классов. Рассмотрим R — множество всех последовательностей 0 и 1. Для произвольной последовательности $\widetilde{\alpha} = (\alpha_1, \ldots, \alpha_s, \ldots)$ положим

$$F_{\widetilde{\alpha}} = \bigcup_{i:\, \alpha_i = 1} \{f_{i+1}\},$$

т. е. если на i-ом месте последовательности стоит 1, мы добавляем в систему f_{i+1}.

Если $\widetilde{\alpha}$, $\widetilde{\beta}$ — различные последовательности, то $[F_{\widetilde{\alpha}}] \neq [F_{\widetilde{\beta}}]$, потому что найдётся функция f_γ, которая есть в одной системе и которой нет в другой, и, как было показано ранее, её нельзя выразить через другую систему. Т. к. множество двоичных последовательностей континуально, получаем, что и семейство замкнутых классов $\{[F_{\widetilde{\alpha}}] : \widetilde{\alpha} \in R\}$ континуально. ■

21. Возведение в n-ю степень с использованием $\log_2 n + o(\log_2 n)$ операций умножения.

Лемма 1. Пусть $L(x^n) = s$, тогда $n \leqslant 2^s$.

Доказательство. Проведём индукцию по величине s.

База: $s = 0$ — верно, поскольку схема вычисляет переменную и неравенство $1 \leqslant 2^0$ выполнено.

Шаг: рассмотрим последний элемент в схеме. Этот элемент вычисляет x^n, перемножая x^a и x^b, вычисляемые в свою очередь, по предположению, схемами сложности не более $s-1$, тогда $n = a + b \leqslant 2^{s-1} + 2^{s-1} = 2^s$. ■

Следствие 1. $L(x^n) \geqslant \log_2 n$.

Теорема 1. $L(x^n) = \log_2 n + o(\log_2 n)$ при $n \to \infty$.

Доказательство. Пусть d — натуральный параметр, значение которого выберем позже. Представим n в системе счисления по основанию 2^d:

$$n = a_0(2^d)^0 + a_1(2^d)^1 + \ldots + a_s(2^d)^s,$$

где $0 \leqslant a_i \leqslant 2^d - 1$, $i = 0, \ldots, s$, $a_s \neq 0$. Очевидно $2^{sd} \leqslant n < 2^{(s+1)d}$.

На первом этапе, использовав sd операций умножения, путём последовательного возведения в квадрат вычисляем степени:

$$x^2, x^4, \ldots, x^{2^d}, \ldots, x^{2^{2d}}, \ldots, x^{2^{sd}}.$$

Положим $u_0 = x^{2^{0d}} = x, u_1 = x^{2^{1d}}, \ldots, u_s = x^{2^{sd}}$ и $I_k = \{i | a_i = k\}$, $J_k = \{j | a_j \geqslant k\}$.

Тогда

$$x^n = u_0^{a_0} u_1^{a_1} \ldots u_s^{a_s} = \left(\prod_{i \in I_{2^d-1}} u_i\right)^{2^d-1} \left(\prod_{i \in I_{2^d-2}} u_i\right)^{2^d-2} \ldots \left(\prod_{i \in I_1} u_i\right)^1 =$$

$$= \left(\prod_{i \in J_{2^d-1}} u_i\right) \left(\prod_{i \in J_{2^d-2}} u_i\right) \ldots \left(\prod_{i \in J_1} u_i\right).$$

Т. к. $J_{2^d-1} \subseteq J_{2^d-2} \subseteq \ldots \subseteq J_1$ можно последовательно вычислить произведения, используя не более s операций умножения (по одной операции для «присоединения» каждой новой переменной u_i). Для перемножения всех произведений потребуется ещё $2^d - 2$ операций умножения.

Таким образом, окончательно имеем:

$$L(x^n) \leqslant sd + s + 2^d - 2 \leqslant \log n + \frac{\log n}{d} + 2^d.$$

Теперь, полагая $d = \lfloor \log\log n - 2\log\log\log n \rfloor$, из предыдущего неравенства при $n \to \infty$ получаем

$$L(x^n) \leqslant \log n + \frac{\log n}{\log\log n \left(1 - \frac{2\log\log\log n + 1}{\log\log n}\right)} + \frac{\log n}{(\log\log n)^2} \leqslant$$

$$\leqslant \log n + \frac{\log n}{\log\log n}(1 + o(1)) + \frac{\log n}{(\log\log n)^2} = \log n + \frac{\log n}{\log\log n}(1 + o(1)) \leqslant \log_2 n + o(\log_2 n).$$

■

22. Граф (ориентированный и неориентированный). Основные понятия для графа. Геометрическая реализация графа. Изоморфизм графов. Подграф. Подграф, индуцированный множеством вершин. Пути, цепи, циклы на графе. Компоненты связности графа. Связные графы.

Определение 1. *Графом* $G(V, E, \rho)$, где $V = \{v_1, v_2, \ldots\}$ — конечное или счётное множество, называемое *вершинами графа*, $E = \{e_1, e_2, \ldots\}$ — конечное или счётное множество, называемое *рёбрами графа*, а ρ каждому ребру e из множества E сопоставляет элемент из множества $V_2 \cup V^2 \cup V$, где V_2 — множество всех двухэлементных подмножеств множества V, $V^2 = V \times V$ — множество всех упорядоченных пар элементов из V.

Если $\rho(e) = \{v_1, v_2\} \in V_2$, то e называют *неориентированным ребром* графа G.

Если $\rho(e) = (v_1, v_2) \in V^2$, то e называют *ориентированным ребром* графа G. Говорят, что ребро e выходит из вершины v_1 и входит в вершину v_2.

В обоих случаях говорят, что вершины v_1 и v_2 *инцидентны ребру* e.

Если $\rho(e) = v$ или $\rho(e) = (v, v)$, то ребро e называется *петлёй* или *ориентированной петлёй* соответственно.

Определение 2. *Неориентированный граф* — граф, в котором все рёбра неориентированные.

Определение 3. *Ориентированный граф* — граф, в котором все рёбра ориентированные.

Рёбра $e_1, \ldots, e_s$, удовлетворяющие условию $\rho(e_1) = \ldots = \rho(e_s)$, называются *кратными*.

Граф, в котором нет кратных рёбер и петель, называется *простым*. Неориентированный граф, в котором нет кратных рёбер и петель, называется *обыкновенным*.

Обозначим через $\deg v$ число рёбер, инцидентных вершине v (при этом петли считаются дважды). Вершина v называется *изолированной*, если $\deg v = 0$. Вершина v называется *висячей*, если $\deg v = 1$.

Определение 4. Последовательность $v_{s_1}, e_{t_1}, v_{s_2}, e_{t_2}, \ldots, v_{s_k}, e_{t_k}, v_{s_{k+1}}$ называется *путём* от вершины v_{s_1} (*начало пути*) к вершине $v_{s_{k+1}}$ (*конец пути*) длины k, $k \geqslant 1$, если для любого i, $i = 1, \ldots, k$, либо $\rho(e_{t_i}) = \{v_{s_i}, v_{s_{i+1}}\}$, либо $\rho(e_{t_i}) = (v_{s_i}, v_{s_{i+1}})$.

Определение 5. Путь, в котором нет повторяющихся вершин, называется *цепью*. Путь, в котором нет повторяющихся рёбер и совпадает начало и конец, называется *циклом*.

Определение 6. Неориентированный граф, в котором любые две вершины соединены путём, называется *связным*.

Определение 7. Граф $G'(V', E', \rho')$ называется *подграфом* графа $G(V, E, \rho)$, если $V' \subseteq V$, $E' \subseteq E$ и $\forall e \in E'$ верно $\rho'(e) = \rho(e)$.

Определение 8. Подграф $G'(V', E', \rho')$ называется *подграфом, индуцированным множеством вершин* V' графа $G(V, E, \rho)$, если E' состоит из всех рёбер $e \in E$, для которых $\rho(e) = \{v_i, v_j\}$ с $v_i, v_j \in V'$ (в неориентированном случае) или $\rho(e) = (v_i, v_j)$ с $v_i, v_j \in V'$ (в ориентированном случае), и при этом $\rho'(e) = \rho(e)$ для каждого $e \in E'$.

Определение 9. *Компонента связности* — максимальный (по включению) связный подграф, индуцированный каким-то множеством вершин.

Определение 10. Графы $G(V, E, \rho)$, $G'(V', E', \rho')$ называются *изоморфными*, если существуют биекции $f : V \to V'$, $g : E \to E'$, такие, что $\forall e, v_1, v_2$: если $\rho(e) = \{v_1, v_2\}$, то $\rho'(g(e)) = \{f(v_1), f(v_2)\}$; а если $\rho(e) = (v_1, v_2)$, то $\rho'(g(e)) = (f(v_1), f(v_2))$.

23. Деревья, характеристические свойства деревьев.

Определение 1. Неориентированный связный граф без циклов называется *деревом*.

Теорема 1. Пусть G — конечный обыкновенный граф. Тогда следующие высказывания равносильны:

1. Граф G — дерево.
2. В графе G любые две вершины соединены единственной цепью.
3. Граф G связен и число рёбер на единицу меньше числа вершин.
4. Граф G связен, но при удалении любого ребра перестаёт быть связным.
5. Граф G не содержит циклов, но при добавлении любого ребра образуется цикл.

Упражнение 1. Докажите данную теорему.

24. Ориентированные графы без ориентированных циклов. Лемма о правильной (монотонной) нумерации вершин в конечном ориентированном графе без циклов.

Определение 1. *Ориентированный цикл* — цикл, в котором все рёбра ориентированные.

Определение 2. Нумерацию вершин в конечном ориентированном графе без ориентированных циклов первыми идущими подряд натуральными числами будем называть *монотонной* или *правильной*, если любое ребро направлено от вершины с меньшим номером к вершине с большим.

Лемма 1 (О монотонной нумерации вершин)**.** У любого конечного ориентированного графа без ориентированных циклов существует монотонная нумерация.

Доказательство. Докажем индукцией по n — количеству вершин. База $n = 1$ — верно. Пусть в графе n вершин. Найдём такую, из которой не выходит ни одного ребра (так можно сделать, потому что граф без ориентированных циклов), сопоставим ей номер n. Остальные $n - 1$ вершин можно занумеровать по предположению. Получена монотонная нумерация для n вершин. ■

25. Схемы из функциональных элементов в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$. Определение функций, реализуемых в вершинах схемы. Независимость функций, реализуемых в вершинах схемы, от выбора монотонной нумерации вершин. Формулы как схемы. Схемы вычислений.

Пусть есть:

1. Множество «исходных данных» X (как правило, это переменные и, быть может, константы; в нашем случае $X = \{x_1, \ldots, x_n\}$);
2. Множество «базисных операций» B (в нашем случае $B_0 = \{x \vee y, x\&y, \overline{x}\}$).

Определение 1. *Схемой из функциональных элементов* в базисе B_0 называется ориентированный граф без ориентированных циклов, в котором входные степени вершин могут быть равны только 0, 1 или 2, при этом если входная степень вершины равна 0, то вершине приписывается символ переменной из множества X (такие вершины называются входами), если входная степень вершины равна 1, то вершине приписывается функциональный символ, соответствующий операции отрицания, а если входная степень вершины равна 2, то вершине приписывается функциональный символ, соответствующий либо двухместной конъюнкции, либо двухместной дизъюнкции. Вершины с ненулевой входной степенью (т. е. вершины, которым приписаны символы операций) будем называть *функциональными элементами*. Кроме того, одна или несколько вершин помечены дополнительно «звёздочкой» — эти вершины называются выходами (с них считывается информация).

Зафиксируем какую-либо правильную нумерацию вершин схемы. Далее в порядке увеличения номера естественным образом приписываем вершине вычисляемую функцию. Тем самым каждой вершине будет приписана своя функция.

Определение 2. Будем говорить, что СФЭ *реализует* (*вычисляет*) булеву функцию $f(x_1, \ldots, x_n)$ (систему функций $f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)$), если выходу (выходам) приписана эта функция (эта система функций). Удобно считать, что выходы СФЭ пронумерованы (упорядочены), и тем самым СФЭ вычисляет булеву (n, m)-функцию — вектор (набор) из m булевых функций от n переменных.

Отметим, что при всём формальном различии в определениях СФЭ и формулы любую формулу можно интерпретировать как СФЭ.

Определение 3. *Сложностью* схемы S называется число функциональных элементов схемы S.

Определение 4. *Схема вычислений* (над X) в базисе B — это последовательность равенств

$$z_1 = \varphi_1(y_{11}, \ldots, y_{1r_1});$$
$$\ldots\ldots\ldots$$
$$z_i = \varphi_i(y_{i1}, \ldots, y_{ir_i});$$
$$\ldots\ldots\ldots$$
$$z_l = \varphi_l(y_{l1}, \ldots, y_{lr_l}),$$

где каждая переменная y_{ij} $(i = 1, \ldots, l; j = 1, \ldots, r_i)$ — это либо одна из входных независимых переменных из множества X, либо одна из внутренних переменных $z_1, \ldots, z_{i-1}$, вычисленных на предыдущих шагах; $\varphi_1, \ldots, \varphi_l \in B$. Кроме того, одна или несколько внутренних переменных из множества $z_1, \ldots, z_l$ дополнительно помечены «звёздочкой» — эти переменные называются выходными (с них считывается информация).

Теорема 1. Функция, которую вычисляет СФЭ, не зависит от выбора монотонной нумерации.

Доказательство. Рассмотрим две различные монотонные нумерации Num_1 и Num_2. Пусть есть номер i — наименьший номер вершины в Num_1, что в этой вершине вычисляемая функция в Num_1 отличается от вычисляемой функции в Num_2. Т. к. нумерация монотонная, то все входы у функционального элемента в обоих нумерациях будут совпадать, а во-вторых, функциональный символ этой вершины совпадает, а значит, и функция, реализуемая в этой вершине, будет совпадать в обеих нумерациях. Противоречие, а значит, функция, которую вычисляет СФЭ, не зависит от выбора монотонной нумерации. ■

26. Сложность реализации функции (множества функций) схемами из функциональных элементов. Функция Шеннона. Простые верхняя и нижняя оценки функции Шеннона.

Если функция f (произвольной природы) реализуется какой-либо схемой S в базисе B, то, очевидно, найдутся еще схемы, реализующие функцию f в базисе B.

Определение 1. Определим величину $L_B(f)$ — *сложность реализации функции f схемами в базисе B* — равенством $L_B(f) = \min L(S)$, где минимум берётся по всем схемам S, реализующим функцию f в базисе B. Схема, в которой достигается минимум, называется *минимальной*.

Определение 2. *Сложность $L_B(\{f_1, \ldots, f_m\})$ реализации системы функций $\{f_1, \ldots, f_m\}$ схемами в базисе B*: $L_B(\{f_1, \ldots, f_m\}) = \min L(S)$, где минимум берётся по всем схемам S, реализующим систему функций $\{f_1, \ldots, f_m\}$ в базисе B.

Определение 3. *Функцией Шеннона* сложности реализации функций схемами в базисе B будем называть функцию $L_B(n)$, определяемую равенством $L_B(n) = \max\limits_{f \in P_2(n)} L_B(f)$.

Договоримся, что в случае, когда набором элементарных операций является классический базис B_0, индекс B_0 у функционалов сложности будем опускать.

Теорема 1 (Верхняя оценка функции Шеннона)**.** Для любого натурального n выполняется неравенство

$$L(n) \leqslant n2^n.$$

Доказательство. Константы можно реализовать схемами сложности 2: $0 = x_1 \cdot \overline{x}_1$, $1 = x_1 \vee \overline{x}_1$. Для любой функции $f(x_1, \ldots, x_n)$, отличной от константы рассмотрим представление в виде СДНФ и последовательно реализуем формулу СДНФ схемой. Тогда потребуется n операций для отрицаний всех переменных, по $n - 1$ операций конъюнкции на каждую из не более чем $2^n - 1$ элементарных

конъюнкций, а затем не более $2^n - 2$ операций дизъюнкции для реализации функции f.
Таким образом,

$$L(n) \leqslant n + (n-1)(2^n - 1) + 2^n - 2 < n2^n.$$

■

Теорема 2 (Нижняя оценка функции Шеннона)**.** Пусть B — конечное множество булевых функций, удовлетворяющее условию $[B] = P_2$. Тогда для произвольной булевой функции f, существенно зависящей от n переменных, выполняется неравенство

$$L_B(f) \geqslant \left\lceil \frac{n-1}{r(B)-1} \right\rceil,$$

где $r(B)$ — наибольшее число существенных переменных у функций базиса B.

Доказательство. Рассмотрим произвольную минимальную схему S в базисе B для функции f. Обозначим через $R(S)$ число рёбер в схеме S. В силу существенной зависимости функции f от всех n переменных и минимальности схемы S из всех вершин схемы S, кроме выходной, выходит по крайней мере по одному ребру, т. е.

$$R(S) \geqslant n + L(S) - 1.$$

С другой стороны, в каждый функциональный элемент входит не более $r(B)$ рёбер, поэтому

$$R(S) \leqslant r(B)L(S).$$

Получаем, что

$$n + L(S) - 1 \leqslant r(B)L(S) \quad \Longleftrightarrow \quad L_B(f) = L(S) \geqslant \frac{n-1}{r(B)-1}.$$

■

27. Асимптотически оптимальная по сложности реализация системы всех элементарных конъюнкций длины n.

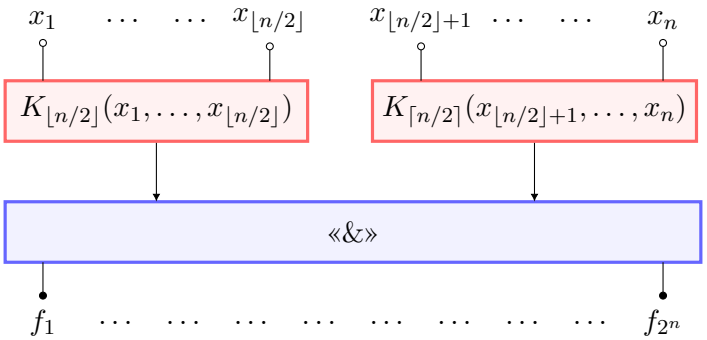
Обозначим через K_n множество всех 2^n элементарных конъюнкций от n переменных:

$$K_n(x_1, \ldots, x_n) \colon = \{x_1^{\sigma_1} \ldots x_n^{\sigma_n} \,|\, (\sigma_1, \ldots, \sigma_n) \in B_n\}.$$

Теорема 1. При $n \to \infty$ справедливо асимптотическое соотношение:

$$L(K_n) \sim 2^n.$$

Доказательство. Построим схему, реализующую систему функций $K_n(x_1, \ldots, x_n)$, как показано на рисунке: схема состоит из трёх блоков (подсхем).



Первая подсхема по переменным $x_1, \ldots, x_{\lfloor n/2 \rfloor}$ реализует систему конъюнкций $K_{\lfloor n/2 \rfloor}(x_1, \ldots, x_{\lfloor n/2 \rfloor})$, вторая подсхема по переменным $x_{\lfloor n/2 \rfloor + 1}, \ldots, x_n$ реализует $K_{\lceil n/2 \rceil}(x_{\lfloor n/2 \rfloor + 1}, \ldots, x_n)$, а третья — каждую элементарную конъюнкцию из множества $K_n(x_1, \ldots, x_n)$ «собирает» (с помощью одной операции конъюнкции) из двух её «половинок», реализованных на некоторых выходах первой и второй подсхемы соответственно. Все конъюнкции длины k можно тривиальным образом реализовать за $k + (k-1)2^k$ операций (k отрицаний, $k-1$ конъюнкций для 2^k элементарных конъюнкций). Имеем:

$$L(K_n) \leqslant L(K_{\lfloor n/2 \rfloor}) + L(K_{\lceil n/2 \rceil}) + 2^n \leqslant$$
$$\leqslant \left\lfloor \frac{n}{2} \right\rfloor + \left(\left\lfloor \frac{n}{2} \right\rfloor - 1 \right) 2^{\lfloor n/2 \rfloor} + \left\lceil \frac{n}{2} \right\rceil + \left(\left\lceil \frac{n}{2} \right\rceil - 1 \right) 2^{\lceil n/2 \rceil} + 2^n \leqslant 2^n + O(n\sqrt{2^n}).$$

■

28. Метод Шеннона получения верхней оценки функции Шеннона.

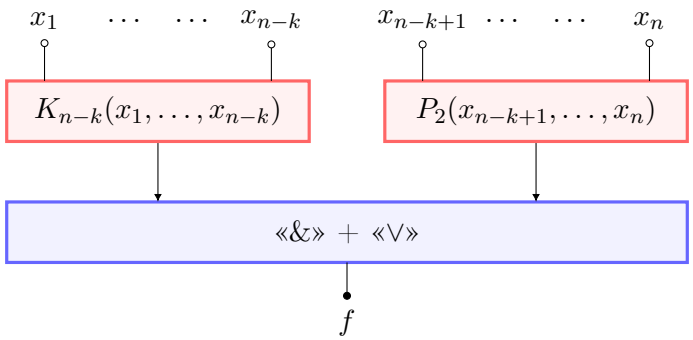
Теорема 1 (`Метод Шеннона`)**.** При $n \to \infty$ верна следующая верхняя оценка функции Шеннона

$$L(n) \lesssim 6\frac{2^n}{n}.$$

Доказательство. Пусть k — натуральный параметр, значение которого выберем позже. Разложим функцию $f(x_1, \ldots, x_n)$ по первым $n-k$ переменным:

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_{n-k})} x_1^{\sigma_1} \cdot \ldots \cdot x_{n-k}^{\sigma_{n-k}} f(\sigma_1, \ldots, \sigma_{n-k}, x_{n-k+1}, \ldots, x_n).$$

Построим схему, реализующую функцию f, как показано на рисунке: схема состоит из трёх блоков (подсхем).



Первая подсхема по переменным $x_1, \ldots, x_{n-k}$ реализует систему конъюнкций $K_{n-k}(x_1, \ldots, x_{n-k})$, вторая по переменным $x_{n-k+1}, \ldots, x_n$ реализует систему всех 2^{2^k} функций от этих k переменных, а третья в соответствии с указанным разложением функции f реализует саму функцию f. Третий блок реализуется не более чем за $2 \cdot 2^{n-k}$ операций (2^{n-k} конъюнкций и $2^{n-k} - 1$ дизъюнкций).

Применяя теоремы из билетов 26 и 27, получаем:

$$L(n) = L(f) \leqslant L(K_{n-k}) + L(k)2^{2^k} + 2 \cdot 2^{n-k} \leqslant 2^{n-k} + o(2^{n-k}) + k2^k 2^{2^k} + 2 \cdot 2^{n-k} = \frac{3 \cdot 2^n}{2^k} + o\left(\frac{2^n}{2^k}\right) + k2^k 2^{2^k}.$$

Полагая $k = \lfloor \log(n - 3\log n) \rfloor$, имеем $\dfrac{n - 3\log n}{2} < 2^k \leqslant n - 3\log n$. Окончательно получаем:

$$L(n) \leqslant 6\frac{2^n}{n} + o\left(\frac{2^n}{n}\right).$$

■

29. Метод каскадов получения верхней оценки функции Шеннона.

Теорема 1 (`Метод каскадов`)**.** При $n \to \infty$ верна следующая верхняя оценка функции Шеннона

$$L(n) \lesssim 6\frac{2^n}{n}.$$

Доказательство. Последовательно определим множества функций $G_0, G_1, \ldots, G_{n-1}$, имеющие вид $G_i = \{g_{i,1}(x_{i+1}, \ldots, x_n), \ldots, g_{i,r_i}(x_{i+1}, \ldots, x_n)\}$, следующим образом:

1. $G_0 = \{g_{0,1}(x_1, \ldots, x_n)\} = \{f(x_1, \ldots, x_n)\}$.
2. Если определено множество $G_{i-1} = \{g_{i-1,1}(x_i, \ldots, x_n), \ldots, g_{i-1,r_{i-1}}(x_i, \ldots, x_n)\}$, то

$$G_i = \{g_{i-1,1}(0, x_{i+1}, \ldots, x_n), \ldots, g_{i-1,r_{i-1}}(0, x_{i+1}, \ldots, x_n),\\ g_{i-1,1}(1, x_{i+1}, \ldots, x_n), \ldots, g_{i-1,r_{i-1}}(1, x_{i+1}, \ldots, x_n)\}.$$

Отметим некоторые свойства множеств G_i:

1. Для любой функции g из G_{i-1} найдутся такие функции $g^{(1)}$ и $g^{(2)}$ из G_i, что справедливо равенство $g(x_i, \ldots, x_n) = x_i g^{(1)}(x_{i+1}, \ldots, x_n) \vee \overline{x}_i g^{(2)}(x_{i+1}, \ldots, x_n)$.
2. При $i = 1, \ldots, n-1$ для количества r_i элементов множества G_i выполняются неравенства: $r_i \leqslant 2r_{i-1} \leqslant 2^i$ (в силу построения G_i), и $r_{n-i} \leqslant 2^{2^i}$ поскольку G_{n-i} содержит функции только от i переменных.

Перейдём к описанию схемы, последовательно реализующей эти множества.

Так как $G_{n-1} \subseteq \{0, 1, x_n, \overline{x}_n\}$, то для реализации функций из множества G_{n-1} потребуется не более трёх элементов.

После этого вычислим отрицания всех остальных переменных, затратив еще $n-1$ инвертор (т. е. элемент, реализующий отрицание функции, подаваемой на единственный вход этого элемента).

Далее, если уже реализованы все функции из множества G_i, то для вычисления любой функции из множества G_{i-1} в соответствии со свойством 1 достаточно трёх элементов (2 конъюнкции и дизъюнкция). Поэтому

$$L(f) \leqslant 3 + (n-1) + \sum_{i=0}^{n-2} 3r_i.$$

Введём натуральный параметр k. Для оценки сверху величины r_i в зависимости от выполнения условия $i \leqslant n-k-1$ применим разные оценки из свойства 2:

$$L(f) \leqslant n + 2 + 3(1 + 2 + \ldots + 2^{n-k-1}) + 3(2^{2^k} + \ldots + 2^{2^1}) \leqslant n + 3 \cdot 2^{n-k} + 6 \cdot 2^{2^k}.$$

Полагая $k = \lfloor \log(n - 2\log n) \rfloor$, получаем $\dfrac{n - 2\log n}{2} < 2^k \leqslant n - 2\log n$, а значит

$$L(n) \leqslant 6\frac{2^n}{n} + o\left(\frac{2^n}{n}\right).$$

■

30. Точное значение сложности реализации системы всех функций от n переменных в произвольном полном базисе.

Теорема 1. Пусть $[B] = P_2$. Тогда для любого натурального n справедливо равенство

$$L_B(P_2(x_1, \ldots, x_n)) = 2^{2^n} - n.$$

Доказательство. Оценка снизу очевидна (для каждой нетривиальной функции необходим хотя бы один ФЭ), оценим сверху. Рассмотрим произвольную схему, реализующую $P_2(n)$. Если два функциональных элемента будут реализовывать одинаковые функции, удалим один ФЭ и все исходящие из него рёбра заменим на те же рёбра, выходящие из другого ФЭ. Тем самым, можно добиться того, что каждой нетривиальной функции из $P_2(n)$ будет сопоставлен один ФЭ, а значит

$$L_B(P_2(x_1, \ldots, x_n)) \leqslant 2^{2^n} - n.$$

■

Лемма 1. Пусть B_1 и B_2 — конечные множества БФ, такие, что $[B_1] = [B_2] = P_2$, тогда существуют $c_1, c_2 > 0$ такие, что $\forall f \in P_2$ справедливо неравенство $c_1 L_{B_1}(f) \leqslant L_{B_2}(f) \leqslant c_2 L_{B_1}(f)$.

Доказательство. Очевидно верно для $c_2 = \max\limits_{\varphi \in B_1} L_{B_2}(\varphi), c_1 = \left(\max\limits_{\varphi \in B_2} L_{B_1}(\varphi)\right)^{-1}$. ■

31. Реализация симметрических булевых функций.

Определение 1. Обозначим через Σ_n булев оператор суммирования n-разрядных чисел, т. е. булеву $(2n, n+1)$-функцию, которая по двум n-разрядным двоичным числам вычисляет $(n+1)$-разрядное двоичное представление их суммы.

Определение 2. Обозначим через N_n булев оператор подсчёта числа единиц в наборе длины n, т. е. булеву $(n, \lceil \log(n+1) \rceil)$-функцию, которая по n-разрядному двоичному набору вычисляет $\lceil \log(n+1) \rceil$-разрядное двоичное представление количества единиц в этом наборе.

Лемма 1. Для любого конечного полного базиса B при $n \to \infty$ справедливо равенство

$$L_B(\Sigma_n) = O(n).$$

Доказательство. Пусть базис A содержит функции $x\&y$, $x \oplus y$, $x \oplus y \oplus z$ и $m(x, y, z)$. Для построения нашей схемы построим две подсхемы Σ_0 — на вход подаётся два последних бита, а на выход сумма разрядов по модулю 2 и перенос «десятка» (на деле двойки), Σ — на вход подаётся два бита и перенос «десятка», а на выход сумма по модулю 2 и перенос «десятка».

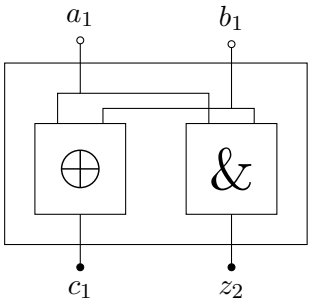


Рис. 1: Реализация Σ_0

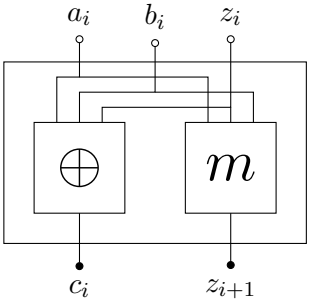


Рис. 2: Реализация Σ

Построим схему S, которая по двум группам входов — $(a_1, \ldots, a_n)$ и $(b_1, \ldots, b_n)$, на которые подаются двоичные n-разрядные числа (младшие разряды a_1 и b_1), вычисляет набор $(c_1, \ldots, c_{n+1})$, представляющий двоичную запись их суммы. Тогда, обозначив через $z_i, i = 2, \ldots, n+1$, значение переноса в i-й разряд, получаем:

$$c_1 = a_1 \oplus b_1, z_2 = a_1 \& b_1,$$
$$c_i = a_i \oplus b_i \oplus z_i, z_{i+1} = m(a_i, b_i, z_i),$$
$$c_{n+1} = z_{n+1},$$

или же в виде схемы:

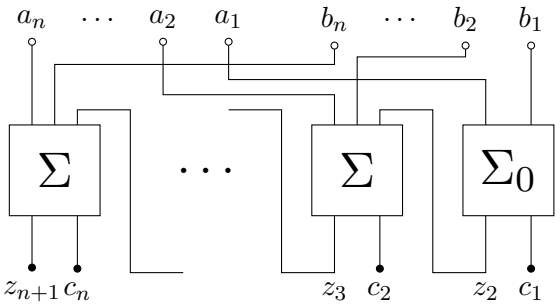


Рис. 3: Реализация Σ_n

На каждый сумматор уходит 2 ФЭ, а всего их n. Следовательно, пользуясь леммой, имеем

$$L_A(\Sigma_n) \leqslant 2n \Rightarrow L_B(\Sigma_n) = O(n).$$

■

Лемма 2. Для любого конечного полного базиса B при $n \to \infty$ справедливо равенство

$$L_B(N_n) = O(n).$$

Доказательство. Очевидно, что результат применения оператора N_n равен двоичной записи суммы n подаваемых на входы оператора одноразрядных двоичных чисел. Опишем способ вычисления этой суммы схемой линейной сложности. Сначала будем считать, что $n = 2^k$ для некоторого k. Построим схему S, имеющую k ярусов. Ярус с номером t, $t = 1, \ldots, k$, будет состоять из 2^{k-t} подсхем, каждая из которых реализует оператор Σ_t и, следовательно, имеет две группы по t входов, а также $t + 1$ выходов. Таким образом, считая в силу леммы 1, что $L_B(\Sigma_t) \leqslant ct$, в случае, когда $n = 2^k$, имеем:

$$L_B(N_n) \leqslant L_B(S) \leqslant \sum_{t=1}^{k} 2^{k-t} ct = c2^k \sum_{t=1}^{k} \frac{t}{2^t} < 2c2^k = 2cn.$$

Переходя к общему случаю, полагаем $n' = 2^{\lceil \log n \rceil}$. Очевидно, что $n \leqslant n' < 2n$. Схему, реализующую оператор N_n, можно получить из схемы S', реализующей оператор $N_{n'}$, подав на $n' - n$ входов схемы S' константу 0. Поэтому

$$L_B(N_n) \leqslant L_B(0) + L_B(N_{n'}) \leqslant L_B(0) + 2cn' \leqslant L_B(0) + 4cn = O(n).$$

■

Определение 3. Функция $f(x_1, \ldots, x_n)$ называется *симметрической*, если для любой перестановки σ из симметрической группы S_n выполняется равенство $f(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = f(x_1, \ldots, x_n)$.

Теорема 1. Для любого полного конечного базиса B существуют $c_1, c_2 > 0$ такие, что для любой симметрической булевой функции $f(x_1, \ldots, x_n)$, отличной от константы, выполняются неравенства

$$c_1 n \leqslant L_B(f(x_1, \ldots, x_n)) \leqslant c_2 n.$$

Доказательство. Нижняя оценка следует из неравенства $L_B(f) \geqslant \frac{n-1}{r(B)-1}$ (см. билет 26).

Переходя к доказательству верхней оценки, отметим, что произвольная симметрическая функция f от n переменных может быть задана двоичной последовательностью $\widetilde{\pi}(f) = (\pi_0(f), \ldots, \pi_n(f))$,

где $\pi_k(f)$ — значение функции f на наборах, состоящих из k единиц и $n-k$ нулей. На этом и основан метод построения схемы S, вычисляющей функцию $f(x_1, \ldots, x_n)$.

Схема S состоит из подсхем S_1 и S_2. Подсхема S_1 реализует оператор N_n, на выходах подсхемы S_1 вычисляется двоичная запись длины $\lceil \log(n+1) \rceil$ числа единиц во входном наборе. Подсхема S_2 по двоичной записи числа единиц во входном наборе вычисляет значение функции f на этом наборе. В силу леммы 2 и верхней оценки функции Шеннона, имеем

$$L_B(f) \leqslant L_B(N_n) + L_B(\lceil \log(n+1) \rceil) = O(n) + O\left(\frac{n}{\log n}\right) = O(n).$$

■

32. Мощностной метод получения нижних оценок функции Шеннона. Эффект Шеннона. Усиленная мощностная нижняя оценка функции Шеннона в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$.

Определение 1. Схему будем называть *приведённой* (*правильной*), если в ней нет двух разных элементов, реализующих одну и ту же функцию.

Лемма 1. Любая минимальная схема является приведённой.

Доказательство. Очевидно (проводим рассуждения, как в билете 30). ■

Обозначим через $N_=(k, n)$ число приведённых схем в базисе $B_0 = \{x \vee y, x\&y, \overline{x}\}$ со входами, которым приписаны переменные $x_1, \ldots, x_n$, и одним выходом, имеющих сложность в точности k, а через $N_\leqslant(k, n)$ — число приведённых схем в базисе B_0 со входами, которым приписаны переменные $x_1, \ldots, x_n$, и одним выходом, имеющих сложность не более k.

Пусть S — приведённая схема в базисе B_0 сложности k со входами $x_1, \ldots, x_n$ и одним выходом. Построим таблицу $T(S, Num)$ высоты k и ширины 3 для заданной схемы S и выбранной нумерации Num следующим образом:

1. В первый столбец по очереди записываем ФЭ, соответствующие номеру i в порядке от 1 до k.
2. В i-ю ($i = 1, \ldots, k$) строчку второго и третьего столбца записываем элементы из множества $\{x_1, \ldots, x_n\} \cup \{1, \ldots, k\}$ — переменные либо номера выходов других ФЭ, которые подаются на вход ФЭ, стоящему в первом столбце в этой же строчке.
3. Справа приписываем звёздочки к выходам.

Например,

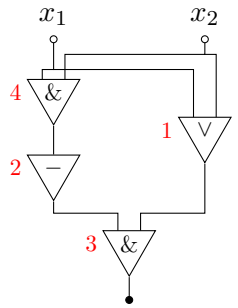


Рис. 4: Схема S с нумерацией Num

$\vee$	x_1	x_2	
—	4	4	
&	2	1	*
&	x_1	x_2	

Рис. 5: Таблица $T(S, Num)$

Лемма 2. Пусть S — приведённая схема в базисе B_0, а Num_1 и Num_2 — две отличные друг от друга нумерации элементов схемы S. Тогда

$$T(S, Num_1) \neq T(S, Num_2).$$

Доказательство. Предположим, что $Num_1 \neq Num_2$, но при этом $T(S, Num_1) = T(S, Num_2)$. Рассмотрим для схемы S монотонную нумерацию Num_0. Нумерация Num_0 обладает следующим свойством: для любого i, $1 \leqslant i \leqslant L(S)$, на каждый вход i-го относительно нумерации Num_0 элемента подаётся либо переменная, либо выход элемента с номером, меньшим i.

Найдём элемент E такой, что его номер различается в Num_1 (p-ый) и Num_2 (q-ый) и который имеет наименьший номер в нумерации Num_0. Очевидно, что второй и третий столбцы в строчках p и q будут совпадать в силу монотонности Num_0 и выбора E. Тогда в приведённой схеме найдутся два ФЭ, реализующих одну и ту же функцию, противоречие. ■

Лемма 3. Найдётся $c > 0$ такое, что при всех значениях k и n ($k \geqslant n$) справедливо неравенство:

$$N_{\leqslant}(k, n) \leqslant c^k k^k.$$

Доказательство. Оценим сверху число таблиц, которые соответствуют всевозможным нумерациям элементов всех приведённых схем со входами $x_1, \ldots, x_n$ и одним выходом сложности k. Каждую клетку первого столбца можно заполнить не более чем тремя способами, каждую клетку второго и третьего столбцов таблицы — не более чем $k + n$ способами. Кроме того, выбор места для пометки $*$ осуществляется $k + n$ способами. Поэтому всего таких таблиц не более $3^k(k+n)^{2k}(k+n)$ штук. Каждой приведённой схеме сложности k в силу леммы 2 соответствует $k!$ различных таблиц. Следовательно,

$$N_{=}(k, n) \leqslant \frac{3^k(k+n)^{2k}(k+n)}{k!}.$$

При условии, что $k \geqslant n$, справедливо $k! \geqslant (k/3)^k$ и неравенство $2k < 2^k$, получаем:

$$N_{=}(k, n) \leqslant \frac{3^k(2k)^{2k}(2k)}{(k/3)^k}.$$

Учитывая, что при $l \leqslant k$ $N_{=}(l, n) \leqslant N_{=}(k, n)$, получаем:

$$N_{\leqslant}(k, n) = \sum_{l=0}^{k} N_{=}(l, n) \leqslant (k+1)N_{=}(k, n) \leqslant 144^k k^k.$$

■

Теорема 1 (Мощностная нижняя оценка)**.** Для любого $\varepsilon > 0$ доля булевых функций f от n фиксированных переменных, удовлетворяющих условию

$$L(f) \geqslant (1 - \varepsilon)\frac{2^n}{n},$$

стремится к 1 при $n \to \infty$.

Доказательство. Положим $k_\varepsilon = (1 - \varepsilon)\dfrac{2^n}{n}$. Число функций f от n фиксированных переменных, удовлетворяющих условию $L(f) \leqslant k_\varepsilon$, не превосходит величины $N_{\leqslant}(k_\varepsilon, n)$. Поэтому достаточно установить, что при $n \to \infty$

$$\frac{N_{\leqslant}(k_\varepsilon, n)}{2^{2^n}} \to 0 \quad \Longleftrightarrow \quad \log_2 \frac{N_{\leqslant}(k_\varepsilon, n)}{2^{2^n}} \to -\infty.$$

Применяя лемму 3, имеем:

$$\log_2 \frac{N_{\leqslant}(k_\varepsilon, n)}{2^{2^n}} \leqslant k_\varepsilon \log_2 c + k_\varepsilon \log_2 k_\varepsilon - 2^n \leqslant (1-\varepsilon)\frac{2^n}{n}\log_2 c + (1-\varepsilon)\frac{2^n}{n}\log_2(2^n) - 2^n = -\varepsilon 2^n + O\left(\frac{2^n}{n}\right).$$

Последнее выражение стремится к $-\infty$ при $n \to \infty$. ■

Следствие 1. При $n \to \infty$ выполняется асимптотическое неравенство $L(n) \gtrsim \frac{2^n}{n}$.

Теорема 2 (Усиленная мощностная нижняя оценка)**.** Для любого $\varepsilon > 0$ доля булевых функций f от n фиксированных переменных, удовлетворяющих условию

$$L(f) \geqslant \frac{2^n}{n}\left(1 + (1-\varepsilon)\frac{\log_2 n}{n}\right),$$

стремится к 1 при $n \to \infty$.

Доказательство. Положим $k_\varepsilon = \dfrac{2^n}{n} + (1-\varepsilon)\dfrac{2^n \log_2 n}{n^2}$.

Установим, что при $n \to \infty$

$$\log_2 \frac{N_{\leqslant}(k_\varepsilon, n)}{2^{2^n}} \to -\infty.$$

Применяя лемму 3, имеем

$$\log_2 \frac{N_{\leqslant}(k_\varepsilon, n)}{2^{2^n}} \leqslant k_\varepsilon \log_2 c + k_\varepsilon \log_2 k_\varepsilon - 2^n \leqslant$$
$$\leqslant O\left(\frac{2^n}{n}\right) + \left(\frac{2^n}{n} + (1-\varepsilon)\frac{2^n \log_2 n}{n^2}\right)\log_2\left(2\frac{2^n}{n}\right) - 2^n = -\varepsilon\frac{2^n \log_2 n}{n} + O\left(\frac{2^n}{n}\right).$$

■

33. Порядок роста функции Шеннона в произвольном полном конечном базисе.

Теорема 1. Пусть B — конечный полный базис, тогда существуют $a, b > 0$ такие, что при $n \to \infty$ выполняется асимптотическое неравенство:

$$a\frac{2^n}{n} \lesssim L_B(n) \lesssim b\frac{2^n}{n}.$$

Доказательство. Прямое следствие леммы 1 из билета 30 и верхней и нижней оценок функции Шеннона. ■

34. Асимптотически наилучший метод (метод Лупанова) построения схем в базисе $\{x \vee y, x\&y, \overline{x}\}$. Асимптотика роста функции Шеннона в этом базисе.

Теорема 1 (О. Б. Лупанов)**.** Пусть $n \to \infty$, тогда

$$L(n) \leqslant \frac{2^n}{n}\left(1 + O\left(\frac{\log n}{n}\right)\right).$$

Доказательство. Опишем метод, который позволяет для произвольной функции от n переменных построить схему, состоящую не более чем из $\frac{2^n}{n}\left(1 + O\left(\frac{\log n}{n}\right)\right)$ элементов.

Введём натуральный параметр k. Таблицу из 2^n значений произвольной функции $f(x_1, \ldots, x_n)$ представим в виде прямоугольной таблицы высоты 2^k и ширины 2^{n-k} как показано на рис. 6.

Пусть s — также натуральный параметр, причём $k, s, \frac{2^k}{s} \to \infty$. Разобьём таблицу на горизонтальные полосы $A_1, \ldots, A_p$ высоты s (полоса A_p имеет высоту $s' \leqslant s$), $p = \left\lceil \frac{2^k}{s} \right\rceil$.

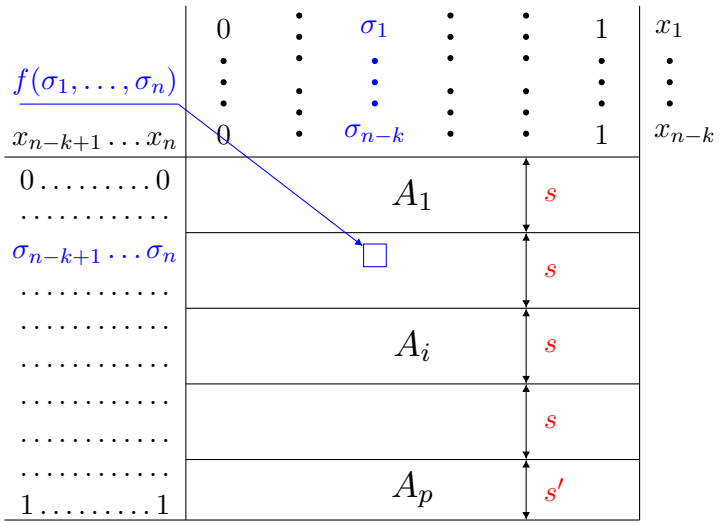


Рис. 6: Таблица

Через $f_i(x_1,\ldots,x_n)$ обозначим функцию, значения которой совпадают со значениями функции $f(x_1,\ldots,x_n)$ на полосе A_i, и равны 0 на остальных полосах. Тогда

$$f(x_1,\ldots,x_n)=\bigvee_{i=1}^{p} f_i(x_1,\ldots,x_n).$$

Теперь для каждой пары $(i,\widetilde{\tau})$, $i=1,\ldots,p$, $\widetilde{\tau}\in E^s$ (или $\widetilde{\tau}\in E^{s'}$ при $i=p$) — последовательность 0 и 1 длины s или s'. Обозначим через $f_{i,\widetilde{\tau}}(x_1,\ldots,x_n)$ функцию, таблица которой получается из таблицы функции $f_i(x_1,\ldots,x_n)$ путём обнуления всех столбцов полосы A_i, значения в которых не совпадают с набором $\widetilde{\tau}$. Тогда

$$f(x_1,\ldots,x_n)=\bigvee_{i=1}^{p}\bigvee_{\widetilde{\tau}} f_{i,\widetilde{\tau}}(x_1,\ldots,x_n).$$

Наконец, у каждой функции $f_{i,\widetilde{\tau}}(x_1,\ldots,x_n)$ можно разделить переменные, точнее представить эту функцию в виде:

$$f_{i,\widetilde{\tau}}(x_1,\ldots,x_n)=f^{(1)}_{i,\widetilde{\tau}}(x_1,\ldots,x_{n-k})f^{(2)}_{i,\widetilde{\tau}}(x_{n-k+1},\ldots,x_n),$$

где в таблице функции $f^{(1)}_{i,\widetilde{\tau}}(x_1,\ldots,x_{n-k})$ обращается в единицу только на наборах $(\sigma_1,\ldots,\sigma_{n-k})$, таких что в соответствующих этим наборам столбцах полосы A_i находится набор $\widetilde{\tau}$, т. е. в таблице этой функции будут стоять столбцы 1 на местах, где стоят столбцы $\widetilde{\tau}$ в полосе A_i. А столбец значений функции $f^{(2)}_{i,\widetilde{\tau}}(x_{n-k+1},\ldots,x_n)$ совпадает с набором $\widetilde{\tau}$ на полосе A_i, а на наборах вне полосы A_i функция $f^{(2)}_{i,\widetilde{\tau}}(x_{n-k+1},\ldots,x_n)$ равна 0, т. е. в таблице этой функции будет столбец $\widetilde{\tau}$ в полосе A_i, а в остальных местах 0.

Возвращаясь к представлению функции f, окончательно получаем:

$$f(x_1,\ldots,x_n)=\bigvee_{i=1}^{p}\bigvee_{\widetilde{\tau}} f^{(1)}_{i,\widetilde{\tau}}(x_1,\ldots,x_{n-k})f^{(2)}_{i,\widetilde{\tau}}(x_{n-k+1},\ldots,x_n).$$

Схема S, реализующая функцию $f(x_1,\ldots,x_n)$, будет состоять из подсхем S_i — см. рис. 7.

В силу теоремы о сложности реализации конъюнкций, при $n\to\infty$ имеем

$$L(S_1)=2^{n-k}+o(2^{n-k})\leqslant 2\cdot 2^{n-k},\ L(S_2)\leqslant 2\cdot 2^k.$$

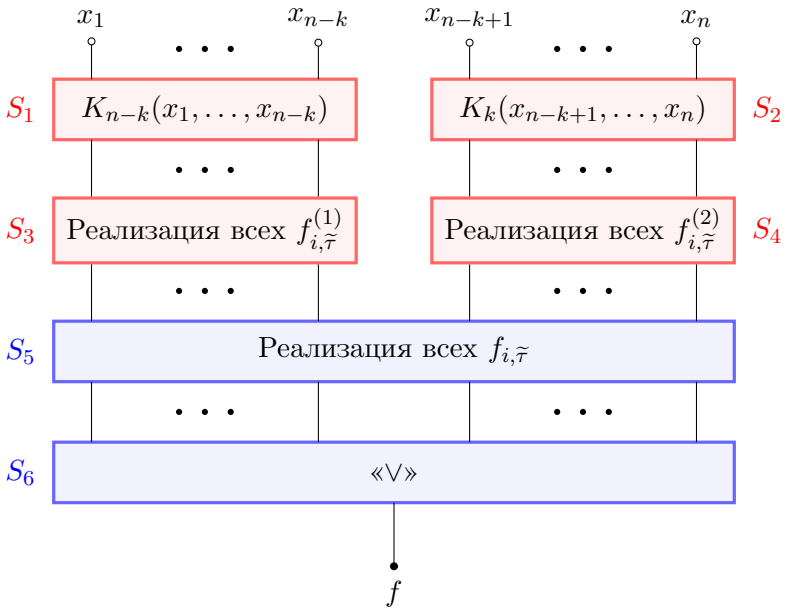


Рис. 7: Разбиение на подсхемы

Подсхема S_3 состоит только из дизъюнкторов (получаем $f^{(1)}_{(i,\widetilde{\tau})}$ через СДНФ). Для реализации всех функций для конкретного i необходимо не больше 2^{n-k} дизъюнкций (т. к. всего $n-k$ переменных), получаем

$$L(S_3) \leqslant p2^{n-k}.$$

Подсхема S_4 также состоит из дизъюнкторов. Аналогично, для конкретного i, $\widetilde{\tau}$ не больше s дизъюнкций. Количество способов выбрать $\widetilde{\tau}$ равно 2^s, получаем

$$L(S_4) \leqslant p2^s s.$$

Подсхема S_5 состоит только из конъюнкторов. Их количество не больше числа пар $(i, \widetilde{\tau})$, а значит

$$L(S_5) \leqslant p2^s.$$

Подсхема S_6 состоит только из дизъюнкторов. Аналогично,

$$L(S_6) \leqslant p2^s.$$

Окончательно получаем:

$$\begin{aligned} L(f) \leqslant L(S) = \sum_{i=1}^{6} L(S_i) &\leqslant 2^{n-k+1} + 2^{k+1} + p2^{n-k} + p2^s s + 2p2^s \leqslant \\ &\leqslant \left(\frac{2^k}{s} + 1\right) 2^{n-k} + \left(\frac{2^k}{s} + 1\right) 2^s (s+2) + 2^{n-k+1} + 2^{k+1} \leqslant \\ &\leqslant \frac{2^n}{s} + 4 \cdot 2^{s+k} + 3 \cdot 2^{n-k} + 2 \cdot 2^k. \end{aligned}$$

Полагая $k = \lfloor 3 \log n \rfloor$, $s = \lfloor n - 5 \log n \rfloor$, и подставляя их в неравенство, имеем:

$$L(f) \leqslant \frac{2^n}{n} \left(1 + O\left(\frac{\log n}{n}\right)\right).$$

■

35. Асимптотика роста функции Шеннона в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$ для класса самодвойственных функций.

Определение 1. Определим *функцию Шеннона сложности реализации самодвойственных функций* в базисе B_0 равенством

$$L^S(n) = \max_{f(x_1,\ldots,x_n)\in S} L(f).$$

Теорема 1. При $n \to \infty$ справедливо асимптотическое равенство

$$L^S(n) \sim \frac{2^{n-1}}{n}.$$

Доказательство. Если в доказательстве мощностной оценки функции Шеннона (см. билет 32) положить

$$k_\varepsilon = (1-\varepsilon)\frac{2^{n-1}}{n}$$

и сравнить величину $N_{\leqslant}(k_\varepsilon, n)$ с $2^{2^{n-1}}$ — числом самодвойственных функций от n переменных, то получается нижняя оценка:

$$L^S(n) \gtrsim \frac{2^{n-1}}{n-1} \sim \frac{2^{n-1}}{n}.$$

Построим схему в базисе B_0 для произвольной самодвойственной функции $f(x_1,\ldots,x_n)$. Положим $g(x_1,\ldots,x_{n-1}) = f(x_1,\ldots,x_{n-1},0)$. Тогда $f(x_1,\ldots,x_{n-1},1) = \overline{f(\overline{x}_1,\ldots,\overline{x}_{n-1},0)} = \overline{g(\overline{x}_1,\ldots,\overline{x}_{n-1})}$.

Нетрудно видеть (верно при $x_n = 0$ и $x_n = 1$, т. к. $x \oplus 1 = \overline{x}$), что

$$f(x_1,\ldots,x_n) = g(x_1 \oplus x_n, x_2 \oplus x_n, \ldots, x_{n-1} \oplus x_n) \oplus x_n.$$

Тогда схема функции f будет состоять из схемы S_g функции g и n схем $S_\oplus$ суммы по модулю 2. Сумма по модулю 2 реализована на рисунке 4 (см. билет 32). В силу оценки роста функции Шеннона, имеем

$$L^S(n) = L(f) = L(S_g) + nL(S_\oplus) \lesssim \frac{2^{n-1}}{n-1} + 4n \sim \frac{2^{n-1}}{n}.$$

■

36. Минимальное число инверторов, достаточное для реализации системы функций $\{\overline{x},\ \overline{y},\ \overline{z}\}$ в базисе $\{x \vee y,\ x\&y,\ \overline{x}\}$.

Теорема 1. Для реализации системы функций $\{\overline{x},\ \overline{y},\ \overline{z}\}$ в базисе B_0 нужно хотя бы 2 инвертора.

Доказательство. Очевидно, необходим хотя бы один инвертор, поскольку $x \vee y$, xy — монотонные функции, а значит, любая схема из этих функций реализует монотонную функцию.

Покажем, что одного инвертора недостаточно. Предположим, что в схеме был ровно один инвертор. Тогда при подаче $(x, y) = (0, 1)$ схема выдавала $(1, 0)$, а инвертор мог выдавать два значения:

1. Если инвертор выдавал 0, то подадим $(x, y) = (1, 1)$. Тогда всё, что было до инвертора, не уменьшится, а значит, инвертор так и будет выдавать 0, и то, что вне инвертора, тоже не уменьшится (в силу монотонности). Значения, которые выдаёт схема, должны были не уменьшиться, но в этом случае схема должна выдавать $(0, 0) \leqslant (1, 0)$, противоречие.

2. Если инвертор выдавал 1, то подадим $(x, y) = (0, 0)$. Тогда всё, что было до инвертора, не увеличится, а значит, инвертор так и будет выдавать 1, и то, что вне инвертора, тоже не увеличится (в силу монотонности). Значения, которые выдаёт схема, должны были не увеличиться, но в этом случае схема должна выдавать $(1, 1) \geqslant (1, 0)$, противоречие.

Теперь приведём пример схемы, состоящей из двух инверторов. Сначала построим все симметрические функции от трёх переменных. Обозначим $s^{i_1,\dots,i_k}$ — симметрическая функция, которая принимает 1 на наборах из $i_1,\dots,i_k$ единиц, и 0 иначе. Построим s^0, s^1, s^2, s^3 — функции от трёх переменных:

$$s^3 = xyz, \quad s^{23} = m(x,y,z) = xy \vee xz \vee yz, \quad s^{123} = x \vee y \vee z,$$
$$s^{01} = \overline{s^{23}}, \quad s^1 = s^{01} \cdot s^{123}, \quad s^{13} = s^1 \vee s^3, \quad s^{02} = \overline{s^{13}},$$
$$s^0 = s^{01} \cdot s^{02}, \quad s^2 = s^{02} \cdot s^{23}.$$

Далее получим все функции вида $x^{\sigma_1}y^{\sigma_2}z^{\sigma_3}$:

1. $xyz = s^3$.
2. $xy\overline{z} = xy \cdot s^2$, поскольку $s^2 = \overline{x}yz \vee x\overline{y}z \vee xy\overline{z}$. Остальные конъюнкции с одним отрицанием аналогично.
3. $x\overline{yz} = x \cdot s^1$, поскольку $s^1 = \overline{xy}z \vee \overline{x}y\overline{z} \vee x\overline{yz}$. Остальные конъюнкции с двумя отрицаниями аналогично.
4. $\overline{xyz} = s^0$.

Таким образом, можно построить схему для любой системы функций от трёх переменных (СДНФ), в том числе $\{\overline{x}, \overline{y}, \overline{z}\}$. ■

37. Детерминированные функции. Информационное дерево. Вес детерминированной функции. Ограниченно-детерминированные функции. Состояния, диаграмма переходов (диаграмма Мура), таблица переходов и канонические уравнения ограниченно-детерминированной функции.

Определение 1. *Алфавит* — набор символов $A = \{a_1,\dots,a_\nu\}$. *Словом* w над алфавитом A будем называть произвольную конечную последовательность символов алфавита A. Обозначим A^n — множество всех слов длины n, A^∞ — множество всех бесконечных последовательностей символов.

Определение 2. Пусть есть два алфавита $A = \{a_1,\dots,a_p\}$, $B = \{b_1,\dots,b_q\}$.
Функция $f : A^\infty \to B^\infty$ переводит некоторое бесконечное слово $x = (x(1), x(2),\dots,x(t),\dots)$ в $y = f(x) = (y(1), y(2),\dots,y(t),\dots)$. Говорят, что алфавит A является *входным*, а B — *выходным*.

Определение 3. Функция f называется *детерминированной*, если

$$\forall k \in \mathbb{N} \quad \forall x', x'' \in A^\infty \quad \forall i = 1,\dots,k \quad x'(i) = x''(i),\ y' = f(x'),\ y'' = f(x''),$$

выполнено $y'(i) = y''(i) \quad \forall i = 1,\dots,k$. Иначе говоря $y(t)$ выражается как функция от $x(1),\dots,x(t)$.

Детерминированные функции можно задавать при помощи информационных деревьев.

Определение 4. *Информационным деревом в алфавитах A и B* называется бесконечное ориентированное дерево, удовлетворяющее следующим условиям:

1. Существует вершина v_0 — *корень* информационного дерева, в которую не входит ни одно ребро;
2. В каждую вершину, отличную от корневой, входит ровно одно ребро;
3. Из каждой вершины выходит $p = |A|$ рёбер, которым приписаны пары $(a_1, b_{i_1}),\dots,(a_p, b_{i_p})$.

Таким образом, любая вершина дерева достижима из корневой и каждой выходящей из корня бесконечной ориентированной цепи в информационном дереве соответствует пара последовательностей $\alpha \in A^\infty$, $\beta \in B^\infty$, которые составлены из приписанных рёбрам этой цепи букв алфавитов. Поэтому каждое информационное дерево задаёт детерминированную функцию и обратно, каждая детерминированная функция задаёт информационное дерево.

Рассмотрим в дереве T произвольную вершину v и рассмотрим бесконечное поддерево T_v дерева T с вершиной v в качестве корня, содержащее все вершины дерева T, достижимые из вершины v. Тогда T_v задаёт детерминированную функцию.

Определение 5. Два информационных дерева T_1 и T_2, задающих одну и ту же детерминированную функцию называются *эквивалентными* ($T_1 \sim T_2$). Иными словами, существует изоморфизм соответствующих бесконечных деревьев, сохраняющий пометки на рёбрах.

Определение 6. Детерминированная функция $f(x)$ называется *ограниченно-детерминированной функцией*, если в информационном дереве, задающем функцию f, содержится лишь конечное число попарно неэквивалентных информационных поддеревьев. Максимальное число попарно неэквивалентных поддеревьев в информационном дереве, задающем о.-д. функцию f, называется *весом* функции f.

Пусть $f(x)$ — о.-д. функция веса r, T — информационное дерево, задающее f, v_0 — его корень, а $v_0, \ldots, v_{r-1}$ — корни попарно неэквивалентных деревьев. Занумеруем все вершины дерева T числами $0, 1, \ldots, r-1$ следующим образом:

1. вершины $v_0, \ldots, v_{r-1}$ нумеруются числами $0, 1, \ldots, r-1$.
2. корни эквивалентных информационных поддеревьев нумеруются одинаково.

Определение 7. Номера $0, 1, \ldots, r-1$ называются *состояниями* функции f, $Q = \{0, \ldots, r-1\}$ — множество состояний.

Определение 8. *Усечённым деревом* называется конечное ориентированное дерево, которое является подграфом дерева T с сохранением всех пометок на вершинах и рёбрах, содержащее v_0 — корень дерева T, и, кроме того, из каждой неконцевой вершины усечённого дерева выходит $p = |A|$ рёбер и любая ориентированная цепь, выходящая из корня, содержит ровно 2 вершины с одинаковыми номерами, а никакое его собственное поддерево этим свойством не обладает.

О.-д. функции удобно задавать *диаграммами Мура*, получающимися из усечённых деревьев отождествлением вершин с одинаковыми номерами.

Определение 9. *Диаграмма переходов* (*диаграмма Мура*) — это конечный ориентированный граф с r вершинами, которые занумерованы числами $0, \ldots, r-1$, и $p \cdot r$ рёбрами; при этом из каждой вершины графа выходит p рёбер, которым приписаны пары $(a_1, b_{i_1}), \ldots, (a_p, b_{i_p})$, где $\{a_1, \ldots, a_p\} = A$, $b_{i_j} \in B \quad \forall j = 1, \ldots, p$. Кроме того, вершина этого графа, соответствующая корню исходного информационного дерева T, обычно помечается $*$.

С диаграммами переходов можно связать две функции, $F : A \times Q \to B$ и $G : A \times Q \to Q$, которые называются *функциями выходов и переходов* соответственно. Значения этих функций для всех $a_i \in A$, $q_j \in Q$ находятся в соответствии с рис. 8.

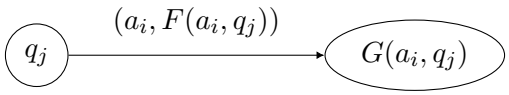


Рис. 8: Определение функций F и G

В результате получаем способ задания о.-д. функций с помощью таблиц переходов (см. рис. 9).

x	q	F	G
$\ldots$	$\ldots$	$\ldots$	$\ldots$
a_i	q_j	$F(a_i, q_j)$	$G(a_i, q_j)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$

Рис. 9: Таблица переходов

О.-д. функции можно задавать при помощи *канонических уравнений*:

$$\begin{cases} y(t) = F(x(t), q(t)); \\ q(t+1) = G(x(t), q(t)); \\ q(1) = q_0, \end{cases}$$

где $x(t) \in A$, $y(t) \in B$, $q(t) \in Q$ при всех $t = 1, 2, \ldots$; q_0 — номер вершины в диаграмме переходов, которая отмечена $*$, $q_0 \in Q$.

38. Автомат. Инициальный автомат. Задание автомата с помощью таблицы, канонических уравнений и диаграммы Мура. Автомат «счётчик чётности». Автомат задержки. Автоматные функции. Тождественность ограниченно-детерминированных и автоматных функций

Конечный автомат — это устройство, функционирующее в дискретные моменты времени $t = 0, 1, \ldots$, имеющее вход, выход и конечное число состояний $q_0, q_1, \ldots, q_\lambda$. В момент времени t автомат находится в состоянии $q(t) \in Q = \{q_0, \ldots, q_\lambda\}$, на его вход подаётся $x(t)$ из конечного множества A, а на выходе выдаётся $y(t)$ из конечного множества B. При этом входной символ $x(t)$ и состояние автомата $q(t)$ однозначно определяют выходной символ $y(t)$ и состояние $q(t+1)$ автомата в следующий момент времени.

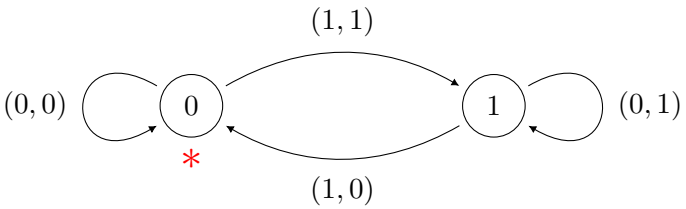
Определение 1. *Конечным автоматом* называется объект $V = (A, B, Q, F, G)$, где A — входной алфавит, B — выходной алфавит, Q — алфавит состояний, $F : A \times Q \to B$ — функция выходов, $G : A \times Q \to Q$ — функция переходов. Автомат называется *инициальным*, если задано его начальное состояние q_0 в момент времени $t = 0$.

Легко видеть, что каждый инициальный автомат V_{q_0} вычисляет некоторую функцию, определённую на множестве A^∞ и принимающую значения из множества B^∞. Эта функция называется *автоматной* и обозначается $f_{V_{q_0}}$.

Определение 2. Функция $f : A^\infty \to B^\infty$ называется *автоматной*, если существует конечный инициальный автомат, вычисляющий эту функцию.

Пример 1. Автомат «счётчик чётности».

$$y(t) = \begin{cases} x(1) \oplus \ldots \oplus x(t) & \text{при } t \geqslant 1, \\ 0 & \text{при } t = 0. \end{cases}$$

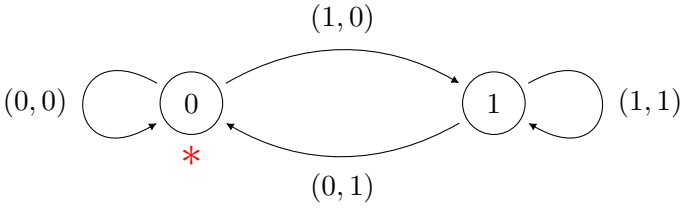


x	q	F	G
0	0	0	0
0	1	1	1
1	0	1	1
1	1	0	0

$$\begin{cases} y(t) = x(t) \oplus q(t), \\ q(t+1) = x(t) \oplus q(t), \\ q(0) = 0. \end{cases}$$

Пример 2. Автомат задержки.

$$y(t) = \begin{cases} x(t-1) & \text{при } t \geqslant 1, \\ 0 & \text{при } t = 0. \end{cases}$$



x	q	F	G
0	0	0	0
0	1	1	0
1	0	0	1
1	1	1	1

$$\begin{cases} y(t) = q(t), \\ q(t+1) = x(t), \\ q(0) = 0. \end{cases}$$

Легко видеть, что для каждой о.-д. функции веса r существует конечный инициальный автомат с r состояниями, вычисляющий эту функцию, и, наоборот, каждый конечный инициальный автомат с λ состояниями вычисляет некоторую о.-д. функцию веса r, где $r \leqslant \lambda$. Тем самым, функция является автоматной тогда и только тогда, когда она ограниченно-детерминированная.

Отметим, что конечные автоматы (как и о.-д. функции) можно задавать при помощи таблиц, диаграмм переходов, информационных деревьев и их конечных фрагментов.

39. Периодические последовательности. Лемма о преобразовании автоматом периодических последовательностей.

Пусть $\alpha = (\alpha(1), \alpha(2), \ldots)$ — некоторая последовательность из A^∞.

Определение 1. Натуральное число d называется *периодом* последовательности α, если существует такой номер N, что для любого $t \geqslant N$ выполняется равенство $\alpha(t+d) = \alpha(t)$. Последовательность называется *периодической*, если для неё существует хотя бы один период.

Поскольку из всех периодов периодической последовательности α можно выбрать минимальный период d_0, то все периоды последовательности кратны d_0.

Лемма 1 (Лемма о преобразовании автоматом периодических последовательностей)**.** Конечный инициальный автомат с λ состояниями преобразует периодическую последовательность с периодом d в периодическую последовательность с периодом $\lambda_1 \cdot d$, где $\lambda_1 \in \mathbb{N}, \lambda_1 \leqslant \lambda$.

Доказательство. Пусть $V_{q_0} = (A, B, Q, F, G_{q_0})$ — инициальный автомат, $|Q| = \lambda$, $q_0 \in Q$, $f_{V_{q_0}}(x)$ — автоматная функция, вычисляемая автоматом V_{q_0}, $\alpha = (\alpha(1), \alpha(2), \ldots)$ — периодическая последовательность A^∞ с периодом d, а $\beta = f_{V_{q_0}}(\alpha) = (\beta_1, \beta_2, \ldots)$ — последовательность из B^∞.

Так как d — период последовательности α, то существует такое N, что для любого $t \geqslant N$ выполняется равенство $\alpha(t + d) = \alpha(t)$. Поэтому

$$\alpha(N) = \alpha(N + d) = \alpha(N + 2d) = \ldots = \alpha(N + \lambda d).$$

Рассмотрим $\lambda + 1$ состояний автомата: $q(N), q(N + d), q(N + 2d), \ldots, q(N + \lambda d)$. Так как $|Q| = \lambda$, то среди них найдутся по крайней мере два одинаковых. То есть существуют такие i, j, $0 \leqslant i < j \leqslant \lambda$, что $q(N + id) = q(N + jd)$. Положим $\lambda_1 = j - i$. Поскольку состояния в моменты $N + id$, $N + jd$ совпадают и подаваемые последовательности после этих моментов тоже, то эти моменты времени «неотличимы», следовательно, выходные символы в эти моменты времени и последующие, отличающиеся на $\lambda_1 d$ совпадают, а значит, β — периодическая с периодом $\lambda_1 d$. ■

Обозначим через A_k множество периодических последовательностей из A^∞, у которых минимальные периоды не имеют простых делителей больших k. Из леммы о периодической последовательности получаем

Следствие 1. Конечный инициальный автомат с λ состояниями при $\lambda \leqslant k$ преобразует последовательности из A_k в последовательности из A_k.

40. Автоматные функции от нескольких переменных. Операция суперпозиции на автоматных функциях. Отсутствие конечной полной системы автоматных функций относительно операции суперпозиции.

Определение 1. *Конечный автомат с n входами*, занумерованными числами от 1 до n — объект $V = (A, B, Q, F, G)$. В момент времени $t = 0, 1, \ldots$, автомат находится в состоянии $q(t)$ из *алфавита состояний* $Q = \{q_1, \ldots, q_\lambda\}$, на его входы $1, \ldots, n$ подаются соответственно $x_1(t), \ldots, x_n(t)$ из *входного алфавита* $A = \{a_1, \ldots, a_p\}$, а на выходе получается $y(t)$ из *выходного алфавита*

$B = \{b_1, \ldots, b_q\}$. При этом входные символы $x_1(t), \ldots, x_n(t)$ и состояние автомата $q(t)$ однозначно определяют выходной символ $y(t)$ и состояние автомата в следующий момент времени:

$$\begin{cases} y(t) = F(x_1(t), x_2(t), \ldots, x_n(t), q(t)), \\ q(t+1) = G(x_1(t), x_2(t), \ldots, x_n(t), q(t)), \end{cases}$$

где функции $F : A^n \times Q \to B$ и $G : A^n \times Q \to Q$ называются *функциями выходов и переходов* соответственно. Автомат называется *инициальным*, если задано его начальное состояние $q(0)$.

Аналогично понятию автоматной функции строится понятие автоматной функции от нескольких переменных.

Определение 2. Функция $f(x_1, \ldots, x_n)$, определённая на множестве $(A^\infty)^n$, и принимающая значения из B^∞ называется *автоматной*, если существует конечный инициальный автомат с n входами, вычисляющий эту функцию.

Примечание. Описанный выше автомат с n входами можно рассматривать, как автомат с одним входом, где символ $x(t) = (x_1(t), \ldots, x_n(t)) \in (A^n)^\infty$.

Примечание. Аналогичным образом можно ввести понятие автомата с n входами и m выходами. Только вместо функции выходов F будет набор функций $F_i : A^n \times Q \to B$. Или же в каноническом виде:

$$\begin{cases} y_1(t) = F_1(x_1(t), \ldots, x_n(t), q(t)), \\ \quad \ldots \\ y_m(t) = F_m(x_1(t), \ldots, x_n(t), q(t)), \\ q(t+1) = G(x_1(t), x_2(t), \ldots, x_n(t), q(t)). \end{cases}$$

Автоматы с n входами и m выходами вычисляют упорядоченный набор автоматных функций.

Определение 3. Обозначим P_A — множество всех автоматных функций, для которых входной и выходной алфавиты равны A. Пусть $F = \{f_1^{(n_1)}(x_1, \ldots, x_{n_1}), \ldots, f_k^{(n_k)}(x_1, \ldots, x_{n_k})\} \subseteq P_A$. Аналогично понятию схемы из функциональных элементов вводится понятие *схемы из автоматных элементов в базисе* F путём рассмотрения конечного ориентированного графа без ориентированных циклов и т. д., вершины, которым приписаны переменные, называются *входами* схемы, вершины, которым приписаны символы $f_i^{(n_i)}$, называются *элементами* (*автоматными элементами*).

Очевидно, что функции, которые реализуются схемами из автоматных элементов в базисе $B \subseteq P_A$, являются автоматными, т. е. принадлежат P_A.

Определение 4. Пусть $F \subseteq P_A$. *Замыканием* системы функций F называется множество $\Sigma(F)$, состоящее из всех функций, которые реализуются схемами из автоматных элементов в базисе F. Система F называется *полной*, если $\Sigma(F) = P_A$.

Лемма 1. Пусть $k \in \mathbb{N}$, F — конечная система функций из P_A, каждая из которых имеет не более k состояний, S — схема из автоматных элементов в базисе F, $f(x_1, \ldots, x_n)$ — автоматная функция, реализуемая схемой S, $\alpha_1, \ldots, \alpha_n$ — последовательности из A_k. Тогда последовательность $\beta = f(\alpha_1, \ldots, \alpha_n) \in A_k$.

Доказательство. Доказательство проведём индукцией по количеству элементов в схеме — N.

1. База $N = 1$. Обозначим $\alpha_1, \ldots, \alpha_n$ — входные последовательности с минимальными периодами $d_1, \ldots d_n$. Поскольку автомат с n входами можно рассматривать, как автомат с одним входом, на который поступает бесконечная последовательность $\alpha = (\alpha_1, \ldots, \alpha_n) \in (A^n)^\infty$. Очевидно, что α — периодическая последовательность с минимальным периодом $d = (d_1, \ldots, d_n)$. Поэтому по лемме о периодической последовательности на выходе выдаётся периодическая последовательность $\beta = f(\alpha) \in A^\infty$ с периодом $\lambda_1 d$, где $\lambda_1 \leqslant \lambda \leqslant k$. d не имеет простых делителей, больших k, поскольку d_i не имеет простых делителей, больших k. А значит, $\lambda_1 d$ не имеет простых делителей, больших k. А значит, $\beta \in A_k$.

2. Докажем для $N+1$. Выделим в схеме S «последний автомат», с которого считывается выход. На его входы по предположению передаются функции из A_k, а значит, и последний автомат выдаст последовательность из A_k.

■

Теорема 1. Пусть $|A| \geqslant 2$. Тогда в P_A не существует конечных полных систем автоматных функций.

Доказательство. Предположим, что в P_A существует конечная полная система F. Обозначим через k максимальное число состояний у функции системы F. Пусть p — простое число, такое, что $p > k$, а β — периодическая последовательность из A^∞ с периодом p следующего вида:

$$\beta = (\underbrace{a_1, \ldots, a_1}_{p-1}, a_2, \underbrace{a_1, \ldots, a_1}_{p-1}, a_2, \ldots),$$

где $a_1, a_2 \in A$, $a_1 \neq a_2$. Очевидно, что $\beta \notin A_k$. Рассмотрим функцию $f : A^\infty \to A^\infty$, которая на всех входных последовательностях принимает β.

Так как F полна по предположению, то существует схема S в базисе F, реализующая эту функцию. Подадим на неё последовательность $\gamma = (a_1, a_1, \ldots)$ — постоянную (с периодом 1), а значит, $\gamma \in A_k$. В силу предыдущей леммы $f(\gamma) \in A_k$, но $\beta \notin A_k$, противоречие. ■

41. Канонические уравнения автомата в скалярном (булевом) виде. Операция обратной связи. Конечные полные системы автоматных функций относительно операций суперпозиции и обратной связи. Реализация автомата схемами из функциональных элементов и элементов задержки.

Отметим, что функциональные элементы можно рассматривать как автоматы с одним состоянием.

Определение 1. Канонические уравнения для автоматов, соответствующих элементам дизъюнкции, конъюнкции и отрицания, имеют следующий вид:

$$\begin{cases} y(t) = x_1(t) \vee x_2(t), \\ q(t+1) = q(t), \\ q(0) = 0, \end{cases} \qquad \begin{cases} y(t) = x_1(t) \& x_2(t), \\ q(t+1) = q(t), \\ q(0) = 0, \end{cases} \qquad \begin{cases} y(t) = \overline{x(t)}, \\ q(t+1) = q(t), \\ q(0) = 0, \end{cases}$$

Будем обозначать автоматные функции из P_E, где $E = \{0, 1\}$, которые вычисляются этими автоматами через $f_\vee(x_1, x_2), f_\&(x_1, x_2), f_\_(x)$.

Определение 2. *Элемент единичной задержки* — автомат с каноническим уравнением:

$$\begin{cases} y(t) = q(t), \\ q(t+1) = x(t), \\ q(0) = 0, \end{cases}$$

соответствующая автоматная функция обозначается через $\vec{f}(x)$.

Рассмотрим произвольную автоматную функцию $f(x_1, \ldots, x_n)$ из P_E и инициальный автомат $V_{q_0} = (A, B, Q, F, G_{q_0})$, вычисляющий её, где $A = E^n$, $B = E$, $Q = \{q_1, \ldots, q_\lambda\}$, $q_0 \in Q$, $F : E^n \times Q \to E$, $G : E^n \times Q \to Q$ с каноническими уравнениями:

$$\begin{cases} y(t) = F(x_1(t), \ldots, x_n(t), q(t)), \\ q(t+1) = G(x_1(t), \ldots, x_n(t), q(t)), \\ q(0) = q_0. \end{cases}$$

Определение 3. Положим $l = \lceil \log \lambda \rceil$. Занумеруем состояния $q_1, \ldots, q_\lambda$ наборами 0 и 1, причём начальному состоянию q_0 сопоставим набор $(0, \ldots, 0)$, т. е. состояние автомата $q(t)$ в момент времени t будет кодироваться l двоичными состояниями: $(q_1(t), \ldots, q_l(t))$. Рассмотрим новые функции $F^1 : E^{n+l} \to B$, $G^1 = (G_1, \ldots, G_l)$, где $G_i : E^{n+l} \to E$, $G^1 : E^{n+l} \to E^l$, т. е.

$$\begin{cases} y(t) = F^1(x_1(t), \ldots, x_n(t), q_1(t), \ldots, q_l(t)), \\ (q_1(t+1), \ldots, q_l(t+1)) = G^1(x_1(t), \ldots, x_n(t), q_1(t), \ldots, q_l(t)), \\ (q_1(0), \ldots, q_l(0)) = (0, \ldots, 0). \end{cases}$$

Или же в общем виде:

$$\begin{cases} y(t) = F^1(x_1(t), \ldots, x_n(t), q_1(t), \ldots, q_l(t)), \\ q_1(t+1) = G_1(x_1(t), \ldots, x_n(t), q_1(t), \ldots, q_l(t)), \\ \ldots \\ q_l(t+1) = G_l(x_1(t), \ldots, x_n(t), q_1(t), \ldots, q_l(t)), \\ q_1(0) = 0, \\ \ldots \\ q_l(0) = 0. \end{cases}$$

Эти уравнения называются *каноническими уравнениями автомата в скалярном (булевом) виде*. Таким образом мы построили инициальный автомат $V^1_{\tilde{q}_0} = (E^n, E, E^l, F^1, G^1)$.

Рассмотрим СФЭ в базисе $\{\vee, \&, \overline{x}\}$ S с входами $x_1, \ldots, x_n, q_1, \ldots, q_l$ и с выходами $y, z_1, \ldots, z_l$, где $z_i = G_i(x_1, \ldots, x_n, q_1, \ldots, q_l)$. Преобразуем S следующим образом. Соединим z_i с q_i, добавив элемент единичной задержки, тем самым добавив l элементов единичной задержки. Кроме того, заменим x_i на $x_i(t)$, q_j на $q_j(t)$, y на $y(t)$, а ФЭ $\vee, \&, \overline{x}$ на символы $f_\vee, f_\&, f_{\_}$ соответственно. В результате получим схему S_1 из автоматных элементов в базисе $f_\vee, f_\&, f_{\_}, \vec{f}$.

Примечание. В схеме S_1 мы вышли за рамки данного ранее определения схемы из автоматных элементов, поскольку появились ориентированные циклы, однако очевидно (по индукции), что если в момент времени t подавать на входы схемы S_1 значения $x_1(t), \ldots, x_n(t)$, то на её выходе будет выдаваться значение $y(t)$, которое вычисляется в соответствии с каноническими уравнениями $V^1_{\tilde{q}_0}$. А значит, схема S_1 реализует автоматную функцию $f(x_1, \ldots, x_n)$.

Определение 4. Операция построения в схемах ориентированных циклов, проходящих через элементы задержки, называется *операцией обратной связи*.

Теорема 1. Любую автоматную функцию из P_E можно реализовать схемой из автоматных элементов в базисе $\{f_\vee, f_\&, f_{\_}, \vec{f}\}$ с использованием операции обратной связи.

Доказательство. Прямое следствие построения нового инициального автомата по каноническим уравнениям автомата в скалярном виде и предыдущих замечаний. ■

42. Изоморфизм автоматов. Отличимость состояний автомата на входном слове и множестве входных слов. Неотличимость состояний и автоматов. Приведённый автомат. Теорема о существовании и единственности приведённого автомата.

Определение 1. Два автомата $V'(A, B, Q', F', G')$ и $V''(A, B, Q'', F'', G'')$ с одинаковыми входным и выходным алфавитами называются *изоморфными*, если существует биекция $\varphi : Q' \to Q''$ такая, что $\varphi(G'(a, q)) = G''(a, \varphi(q))$ и $F'(a, q) = F''(a, \varphi(q))$ для любых $q \in Q'$, $a \in A$.

Определение 2. *Слово* w — последовательность символов из A, $w \in A^n$, где n — какое-то натуральное число. Множество $A^+ = \bigcup_{n=1}^{\infty} A^n$ — множество всех слов.

Определение 3. Пусть $V = (A, B, Q, F, G)$ — конечный автомат. Функции выхода и переходов можно обобщить на функции: $\overline{F} : A^+ \times Q \to B^+$ и $\overline{G} : A^+ \times Q \to Q$, определяемые следующим рекурсивным образом:

1. $\overline{F}(a, q) = F(a, q)$, $\overline{G}(a, q) = G(a, q)$ для $a \in A$.
2. $\overline{F}(aw, q) = F(a, q)\overline{F}(w, G(a, q))$, $\overline{G}(aw, q) = \overline{G}(w, G(a, q))$ для $a \in A$, $w \in A^+$.

Определение 4. Пусть $V'(A, B, Q', F', G')$ и $V''(A, B, Q'', F'', G'')$ — два автомата с одинаковыми входным и выходным алфавитами, $q' \in Q'$, $q'' \in Q''$, $w \in A^+$. Состояния q' и q'' *отличимы на слове* w, если $\overline{F}'(w, q') \neq \overline{F}''(w, q'')$. В противном случае, q' и q'' *неотличимы на слове* w.

Определение 5. Пусть $W \subseteq A^+$ — произвольное множество входных слов. Состояния q' и q'' *отличимы на множестве* W, если они отличимы хотя бы на одном слове из W, в противном случае, они *неотличимы на множестве* W. Обозначение: $q' \overset{W}{\sim} q''$. В случае $W = A^+$ опускается фраза на множестве W и обозначается $q' \sim q''$.

Примечание. Отношение неотличимости на множестве W — это отношение эквивалентности.

Определение 6. Автоматы V' и V'' называются *неотличимыми* ($V' \approx V''$), если

1. $\forall q' \in Q' \quad \exists q'' \in Q'' \quad q' \sim q''$,
2. $\forall q'' \in Q'' \quad \exists q' \in Q' \quad q'' \sim q'$.

Примечание. Изоморфные автоматы являются неотличимыми, неотличимые автоматы могут быть неизоморфными.

Определение 7. Автомат называется *приведённым*, если любые два его состояния отличимы.

Теорема 1. Для любого конечного автомата V существует единственный с точностью до изоморфизма приведённый автомат, неотличимый от V.

Доказательство. Пусть $V = (A, B, Q, F, G)$ — произвольный конечный автомат. Разобьём множество состояний Q на классы эквивалентности относительно отношения неотличимости. Пусть $\hat{Q}$ — множество всех этих классов состояний автомата V. Построим новый автомат $\hat{V} = (A, B, \hat{Q}, \hat{F}, \hat{G})$.

Положим $\hat{G}(a, \hat{q}) = \hat{q}'$, $\hat{F}(a, \hat{q}) = F(a, q)$, где q — некоторое состояние из класса $\hat{q}$, а $\hat{q}'$ — класс, содержащий состояние $G(a, q)$.

Корректность определения очевидна из неотличимости состояний из одного класса.

Пусть $q \in \hat{q}$. Покажем (индукцией по длине слова), что состояния q и $\hat{q}$ неотличимы, т. е. $\overline{F}(w, q) = \overline{\hat{F}}(w, \hat{q})$ для любого слова $w \in A^+$.

1. База $w = a \in A$, тогда $\overline{\hat{F}}(a, \hat{q}) = \hat{F}(a, \hat{q}) = F(a, q) = \overline{F}(a, q)$.
2. Пусть теперь длина слова w больше 1 и $\overline{F}(w', q) = \overline{\hat{F}}(w', \hat{q})$ для любых состояний $q \in \hat{q}$ и любого слова w' длины меньшей, чем длина w. Положим $w = aw'$, где $a \in A$. Тогда

$$\overline{F}(w, q) = F(a, q)\overline{F}(w', G(a, q)), \qquad \overline{\hat{F}}(w, \hat{q}) = \hat{F}(a, \hat{q})\overline{\hat{F}}(w', \hat{G}(a, \hat{q})).$$

По предположению индукции $\overline{F}(w', G(a, q)) = \overline{\hat{F}}(w', \hat{G}(a, \hat{q}))$. Кроме того, $\hat{F}(a, \hat{q}) = F(a, q)$.

Таким образом, $\overline{F}(w, q) = \overline{\hat{F}}(w, \hat{q})$. Следовательно, автоматы V и $\hat{V}$ неотличимы.

Построенный автомат $\hat{V}$ приведённый, т. е. все его состояния отличимы. В самом деле, состояния из разных классов эквивалентности отличимы.

Осталось показать единственность (с точностью до изоморфизма) приведённого автомата.

Пусть $V' = (A, B, Q', F', G')$ — приведённый автомат, неотличимый от V. Покажем, что тогда V' изоморфен $\hat{V}$.

Так как $V \approx \hat{V}$ и $V \approx V'$, то $V' \approx \hat{V}$. Поэтому для каждого состояния автомата V' в $\hat{V}$ найдётся состояние, неотличимое от этого состояния, и, поскольку V' является приведённым, то все эти

состояния автомата $\hat{V}$ должны быть различными. Таким образом, число состояний автомата $\hat{V}$ не меньше числа состояний автомата V'. Аналогично число состояний автомата V' не меньше числа состояний автомата $\hat{V}$. Следовательно, число состояний автомата $\hat{V}$ равно числу состояний автомата V'. А значит, между неотличимыми состояниями автоматов V' и $\hat{V}$ существует биекция, которая и будет являться изоморфизмом. ■

43. Отличимость состояний автомата на входных словах заданной длины. 1-я и 2-я теоремы Мура. Примеры автоматов, для которых утверждения теорем Мура не могут быть усилены.

Теорема 1 (1-я теорема Мура)**.** Пусть $V = (A, B, Q, F, G)$ — конечный автомат с k состояниями. Тогда два состояния $q', q'' \in Q$ автомата V являются неотличимыми тогда и только тогда, когда они неотличимы на множестве A^{k-1}.

Доказательство. Если два состояния автомата V являются неотличимыми, то они неотличимы на множестве A^{k-1}. Теперь докажем, что если они неотличимы на множестве A^{k-1}, то они неотличимы.

Как было показано в билете 42, для любого натурального i отношение неотличимости на множестве A^i является отношением эквивалентности. Поэтому множество Q разбивается на классы эквивалентности относительно данного отношения. Обозначим через $R_i = \{\hat{q}_1^i, \hat{q}_2^i, \ldots, \hat{q}_{k_i}^i\}$ множество всех таких классов.

Если два состояния содержатся в одном классе из R_{i+1}, то они содержатся в одном классе из R_i. Поэтому каждый класс из R_i является объединением некоторых классов из R_{i+1}. Таким образом, $|R_i| \leqslant |R_{i+1}|$, причём $|R_i| = |R_{i+1}|$ тогда и только тогда, когда $R_i = R_{i+1}$.

Так как $|R_i| \leqslant |R_{i+1}|$ и $|R_i| \leqslant k$ при всех i, то найдётся минимальный номер s, такой, что $|R_s| = |R_{s+1}|$, т. е. $R_s = R_{s+1}$. Покажем, что тогда $R_s = R_{s+1} = R_{s+2} = \ldots$

Пусть это не так, т. е. для некоторого $t > s$ верно $R_t \neq R_{t+1}$. Тогда существуют два состояния $q', q'' \in Q$ такие, что $q' \overset{A^t}{\sim} q''$, но q' и q'' отличимы на A^{t+1}, т. е. существует входное слово длины $t+1$, что $\overline{F}(w, q') \neq \overline{F}(w, q'')$.

Пусть u — префикс длины $t - s$ в слове w. Положим $q_1' = \overline{G}(u, q')$, $q_1'' = \overline{G}(u, q'')$. Покажем, что $q_1' \overset{A^s}{\sim} q_1''$. Рассмотрим произвольное входное слово $v \in A^s$ и составим слово $uv \in A^t$.

Так как $q' \overset{A^t}{\sim} q''$, то $\overline{F}(uv, q') = \overline{F}(uv, q'')$, при этом

$$\overline{F}(uv, q') = \overline{F}(u, q')\overline{F}(v, q_1'),$$
$$\overline{F}(uv, q'') = \overline{F}(u, q'')\overline{F}(v, q_1'').$$

т. е. $\overline{F}(u, q') = \overline{F}(u, q'')$ и $\overline{F}(v, q_1') = \overline{F}(v, q_1'')$. Первое равенство используем позже, а из второго следует, что $q_1' \overset{A^s}{\sim} q_1''$.

Возвращаясь к слову $w \in A^{t+1}$, имеющему префикс u и удовлетворяющему условию $\overline{F}(w, q') \neq \overline{F}(w, q'')$, обозначим в слове w через v' суффикс длины $s+1$, получая представление $w = uv'$.

Тогда

$$\overline{F}(w, q') = \overline{F}(uv', q') = \overline{F}(u, q')\overline{F}(v', q_1'),$$
$$\overline{F}(w, q'') = \overline{F}(uv', q'') = \overline{F}(u, q'')\overline{F}(v', q_1'').$$

Слова $\overline{F}(w, q')$ и $\overline{F}(w, q'')$ отличаются, а префиксы $\overline{F}(u, q')$ и $\overline{F}(u, q'')$ — нет. Поэтому

$$\overline{F}(v', q_1') \neq \overline{F}(v', q_1'').$$

Получаем, что q_1' и q_1'' содержатся в одном классе из R_s, но в разных классах из R_{s+1}, что противоречит равенству $R_s = R_{s+1}$. Таким образом, $R_s = R_{s+1} = R_{s+2} = \ldots$

Следовательно, если два состояния из Q неотличимы на множестве A^s, то они неотличимы на любом входном слове, т. е. являются неотличимыми.

С другой стороны,

$$|R_1| < |R_2| < \ldots < |R_s|.$$

Так как $|R_{i+1}| \geqslant |R_i| + 1$, и $|R_s| \leqslant k$, получаем, что $s \leqslant k - 1$.

Таким образом, $q' \overset{A^{k-1}}{\sim} q'' \Rightarrow q' \overset{A^s}{\sim} q'' \Rightarrow q' \sim q''$. ■

Пример 1. 1-я теорема Мура не может быть усилена.

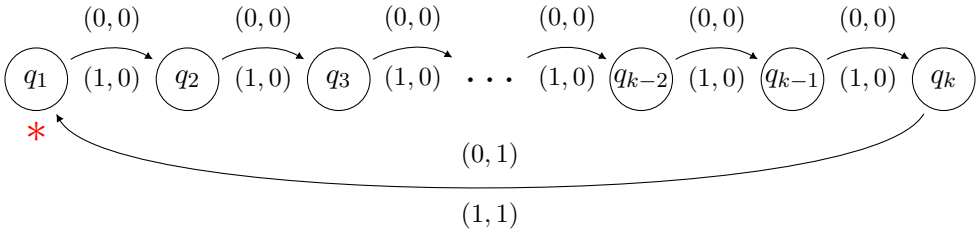


Рис. 10: Диаграмма Мура контрпримера

Нетрудно заметить, что $q_1 \overset{A^{k-2}}{\sim} q_2$, однако $q_1 \not\sim q_2$.

Теорема 2 (2-я теорема Мура)**.** Пусть $V' = (A, B, Q', F', G'), V'' = (A, B, Q'', F'', G'')$ — конечные автоматы, $|Q'| = k'$, $|Q''| = k'', q' \in Q', q'' \in Q''$. Тогда состояния q' и q'' являются неотличимыми тогда и только тогда, когда они неотличимы на множестве $A^{k'+k''-1}$.

Доказательство. Применим первую теорему Мура для автомата $V''' = (A, B, Q''', F''', G''')$, у которого $Q''' = Q' \sqcup Q''$,

$$G'''(a,q) = \begin{cases} G'(a,q), & \text{если } q \in Q', \\ G''(a,q), & \text{если } q \in Q'', \end{cases} \qquad F'''(a,q) = \begin{cases} F'(a,q), & \text{если } q \in Q', \\ F''(a,q), & \text{если } q \in Q''. \end{cases}$$

■

Пример 2. 2-я теорема Мура не может быть усилена. В качестве контрпримера на рисунке приведены два автомата, заданные диаграммами Мура.

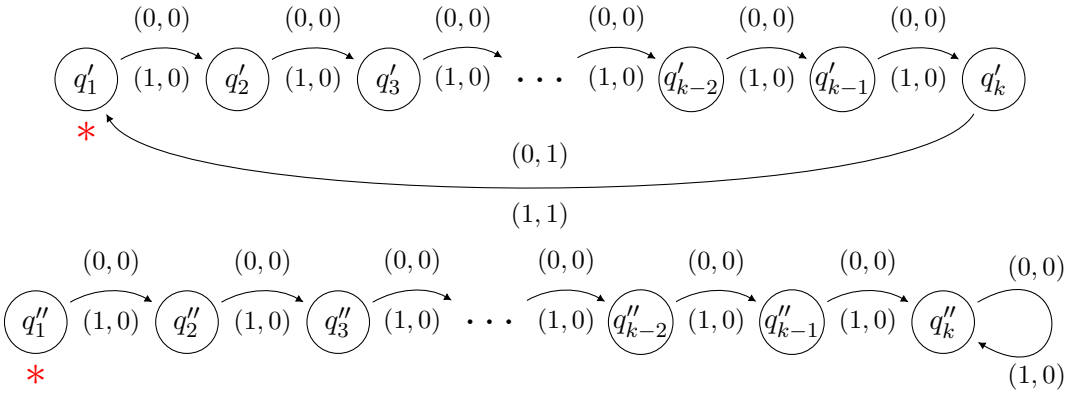


Рис. 11: Диаграмма Мура контрпримера

С одной стороны, при $k' \geqslant k'' \geqslant 2$ выполняется соотношение $q''_1 \overset{A^{k'+k''-2}}{\sim} q'_{k'-k''+2}$, так как на любых входных словах длины $k'+k''-2$ в этих состояниях на выходе выдается слово $\underbrace{00\ldots0}_{k''-2}1\underbrace{00\ldots0}_{k'-1}$, а с другой стороны, справедливо соотношение $q''_1 \not\sim q'_{k'-k''+2}$.