Функциональные системы

Презентации к лекциям

Савицкий Игорь Владимирович

факультет ВМК МГУ

осень 2025

Лекция 1
Функции алгебры логики (повторение). Лемма о нелинейной функции. Классы T_0, T_1, T_{01}, M

Функции алгебры логики

Определение

- $E_2 = \{0, 1\}$. Функция алгебры логики (булева функция) от n переменных — это функция $f\colon E_2^n \to E_2$, $n \in \mathbb{N}$.
- Множество всех булевых функций обозначается P_2.

Табличное и векторное задание булевых функциий

- Булева функция определяется своей таблицей: слева указываются все возможные значения переменных, а справа — значения функции на этих наборах переменных. Например:

x	y	$x \mathbin{\&} y$
0	0	0
0	1	0
1	0	0
1	1	1

- В таблице наборы значений переменных обычно упорядочены стандартно — лексикографически.
- В случае стандартного порядка наборов достаточно задать только вектор функции.
- Например, вектор функции $x \mathbin{\&} y$ — (0001).

Функции алгебры логики

Табличное задание некоторых булевых функциий

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

x	y	$x \mathbin{\&} y$	$x \vee y$	$x \to y$	$x \sim y$	$x \oplus y$	$x \mid y$	$x \downarrow y$
0	0	0	0	1	1	0	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	0	0	1	1	0
1	1	1	1	1	1	0	0	0

Функции алгебры логики

Логические связки

- Считаем, что $0 = \text{false}$ (ложь), $1 = \text{true}$ (истина).
- $\overline{x} = \neg x =$ «x не истинно» — отрицание.
- $x \,\&\, y = x \cdot y = xy =$ «x истинно и y истинно» — конъюнкция (умножение по модулю 2).
- $x \vee y =$ «x истинно или y истинно» — дизъюнкция.
- $x \to y = \overline{x} \vee y =$ «если x истинно, то y истинно» — импликация.
- Импликация — это логическое следование, не имеющее отношения к причинно-следственным связям между x и y.

  Если известно, что x и $x \to y$ истинны, то y тоже истинно.

  Но $x \to y$ может быть истинно и не из-за внутренней связи x и y, а, например, потому что y — заведомо истинное утверждение.
- $x \sim y = \overline{x \oplus y} =$ «x истинно тогда и только тогда, когда y истинно» — эквивалентность.

Функции алгебры логики

Прочие функции

- $0, 1$ — константы.
- x — тождественная функция.
- $x \oplus y$ — сложение по модулю 2 (исключающее «или»).
- $x \mid y = \overline{xy}$ — штрих Шеффера.
- $x \downarrow y = \overline{x \vee y}$ — стрелка Пирса.
- Мнемоническое правило для выражения функций $x \mid y$ и $x \downarrow y$: поворачиваем черту на 90° и кладём сверху в виде отрицания. Внизу остаётся либо часть $\vee$ от стрелки (дизъюнкция), либо ничего (конъюнкция).
- $\mathrm{m}(x, y, z) = xy \vee xz \vee yz = xy \oplus xz \oplus yz$ — медиана (функция голосования). Эта функция подсчитывает число нулей и единиц среди значений своих трёх переменных и возвращает то значение, которое встречается большее число раз.

Функции алгебры логики

Основные тождества

- Коммутативность: $x \circ y = y \circ x$, где $\circ \in \{\&, \vee, \oplus, \sim, |, \downarrow\}$.
- Ассоциативность: $x \circ (y \circ z) = (x \circ y) \circ z$, где $\circ \in \{\&, \vee, \oplus, \sim\}$.
- Дистрибутивность конъюнкции относительно операций $\vee, \oplus$:
$$x(y \vee z) = xy \vee xz, \quad x(y \oplus z) = xy \oplus xz.$$
- Дистрибутивность дизъюнкции относительно конъюнкции:
$$x \vee yz = (x \vee y)(x \vee z).$$
- Правила де Моргана: $\overline{xy} = \overline{x} \vee \overline{y}, \quad \overline{x \vee y} = \overline{x}\,\overline{y}, \quad \overline{\overline{x}} = x.$
- Правила поглощения: $x \vee xy = x, \quad x(x \vee y) = x.$
- $x \cdot \overline{x} = x \cdot 0 = x \oplus x = 0, \quad x \vee \overline{x} = x \vee 1 = x \sim x = x \to x = 1.$
- $x \cdot x = x \vee x = x \cdot 1 = x \vee 0 = x \oplus 0 = x, \quad \overline{x} = x \oplus 1.$
- $x \sim y = x \oplus y \oplus 1, \quad x \to y = \overline{x} \vee y, \quad x \mid y = \overline{xy}, \quad x \downarrow y = \overline{x} \vee y.$
- $x \oplus y = \overline{x}y \vee x\overline{y} = (\overline{x} \vee \overline{y})(x \vee y), \quad x \sim y = \overline{x}\,\overline{y} \vee xy = (\overline{x} \vee y)(x \vee \overline{y}).$

Существенные и фиктивные переменные

Определение

Пусть $f(x_1, \dots x_n) \in P_2$. Переменная x_i существенная, если существуют такие числа $a_1, \dots, a_{i-1}$, $a_{i+1}, \dots, a_n \in E_2$, что

$$f(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) \neq f(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n).$$

В противном случае переменная x_i фиктивная.

- Фиктивные переменные — это переменные, от значений которых выход функции не зависит.
- У функции $f(x, y) = \overline{x}$ переменная y фиктивна.
- У функции $f(x, y) = xy\overline{x}$ обе переменные фиктивны.
- Хотя обычно говорят «у функции $f(x, y)$ переменная y фиктивна», правильнее это понимать так: «у функции f, зависящей от 2 переменных, вторая переменная фиктивна».

Формулы

- Считаем, что задано счётное множество символов переменных и что для каждой функции из P_2 задан функциональный символ.

Определение (формулы, реализующие булевы функции)

Пусть $Q \subseteq P_2$, $(x_1, \ldots, x_n)$ — упорядоченный набор различных символов переменных, а $X = \{x_1, \ldots, x_n\}$.

- Если f — символ функции из Q от k переменных, а $x_{i_1}, \ldots, x_{i_k} \in X$, то $f(x_{i_1}, \ldots, x_{i_k})$ — формула над Q. Она реализует функцию $h(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_k})$.
- Пусть f — символ функции из Q от k переменных, а $\Phi_1, \ldots, \Phi_k$ — формулы над Q (реализующие функции $g_j(x_1, \ldots, x_n)$, $j = \overline{1, k}$) или символы переменных из X (в этом случае $g_j(x_1, \ldots, x_n) = x_{i_j}$, где x_{i_j} соответствует переменной Φ_j).
  Тогда $f(\Phi_1, \ldots, \Phi_k)$ — формула над Q. Она реализует функцию $h(x_1, \ldots, x_n) = f(g_1(x_1, \ldots, x_n), \ldots, g_k(x_1, \ldots, x_n))$.

Формулы

Соглашения при записи формул

- Вместо $f(\Phi)$ можно писать $(f\ \Phi)$: $\neg(x) = (\neg x)$.
- Вместо $f(\Phi_1, \Phi_2)$ можно писать $(\Phi_1\ f\ \Phi_2)$: $\&(x, y) = (x \mathbin{\&} y)$.
- Можно опускать скобки с учётом приоритета операций для некоторых стандартных функциональных символов:
  - $\neg$ имеет наибольший приоритет, далее идут $\cdot$ и $\&$, далее все остальные функциональные символы.
  - Операции с одинаковым приоритетом применяются слева направо.
- Функциональный символ $\cdot$ в записи $\Phi_1 \cdot \Phi_2$ можно опускать.
- Вместо $\neg\Phi$ можно писать $\overline{\Phi}$.

Функции, реализуемые формулами

- Функция, реализуемая формулой, зависит не только от самой формулы, но и от выбранного набора переменных $(x_1, \ldots, x_n)$.

Пример

- Формула над $\{\to, \vee\}$:

$$\Phi = x_1 \vee (x_2 \to x_1).$$

- Формула Φ при наборе (x_1, x_2, x_3) реализует функцию

$$f(x_1, x_2, x_3) = x_1 \vee (x_2 \to x_1) = x_2 \to x_1 \quad (f(x, y, z) = y \to x).$$

- При наборе (x_2, x_1) формула Φ реализует функцию

$$f(x_2, x_1) = x_2 \vee (x_1 \to x_2) = x_1 \to x_2 \quad (f(x, y) = x \to y).$$

Функции, реализуемые формулами

Замечания

- В большинстве случаев при реализации функций формулами набор переменных понятен по контексту и не упоминается отдельно.
- Функциональные символы функций-констант, можно записывать без переменных (0 вместо $0(x)$).
- Каждая формула — это схема построения сложных функций путём подстановки простых функций друг в друга, а также путём переименования переменных.

Определение

Функция f является суперпозицией функций $f_1, \dots, f_s$, если её можно реализовать формулой над $\{f_1, \dots, f_s\}$.

- Частным случаем суперпозиции является отождествление переменных.

Замкнутые классы

Определение

Пусть $A \subseteq P_2$.

- Замыкание $[A]$ множества A (относительно операции суперпозиции) — это множество всех функций из P_2, которые можно реализовать с помощью формул над A.
- Множество $A \subseteq P_2$ является замкнутым классом, если $[A] = A$.

- Пересечение замкнутых классов является замкнутым классом.
- Замкнутые классы — это «ограничители» возможности выразить сложные функции через простые с помощью формул.
- Если все простые функции принадлежат какому-то замкнутому классу, то и всё, что можно получить из них формулами, принадлежит тому же классу.

Аксиомы замыкания

Определение

Пусть $[x]$ — оператор на множествах. Оператор называется **оператором замыкания**, если он удовлетворяет следующим свойствам:

1. Экстенсивность: $A \subseteq [A]$.
2. Монотонность: если $A \subseteq B$, то $[A] \subseteq [B]$.
3. Идемпотентность: $[[A]] = [A]$.

- Определённое ранее замыкание на множествах булевых функций удовлетворяет этим свойствам и является оператором замыкания.
- Другой пример оператора замыкания — замыкание на множествах в $\mathbb{R}^n$, заключающееся в добавлении во множество всех его предельных точек (в результате получается замкнутое множество: содержащее все свои предельные точки).

Порождающие множества и базисы

Определение

- Множество функций Q порождает замкнутый класс R (полно в R), если $[Q] = R$.
- Множество Q полно, если оно полно в P_2.
- Множество функций Q называется базисом замкнутого класса R, если $[Q] = R$ и $[Q_1] \neq R$ для любого подмножества Q_1 множества Q, отличного от Q.

Утверждение

Пусть множество Q_1 полно в замкнутом классе R, $Q_2 \subseteq R$ и функции множества Q_1 реализуются формулами над Q_2. Тогда множество Q_2 также полно в R.

Совершенная ДНФ

- Обозначим $x^\sigma = \begin{cases} \overline{x}, & \sigma = 0, \\ x, & \sigma = 1. \end{cases}$

Разложение Шеннона

Для любой булевой функции $f(x_1, \ldots, x_n)$ верно

$$f(x_1, \ldots, x_n) = \bigvee_{\sigma_1, \ldots, \sigma_k \in \{0,1\}} x_1^{\sigma_1} \ldots x_k^{\sigma_k} f(\sigma_1, \ldots, \sigma_k, x_{k+1}, \ldots, x_n)$$

Совершенная ДНФ

Для любой булевой функции $f(x_1, \ldots, x_n)$, не равной 0, верно

$$f(x_1, \ldots, x_n) = \bigvee_{\substack{\sigma_1, \ldots, \sigma_n \in \{0,1\} \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \ldots x_n^{\sigma_n}.$$

- Функцию 0 можно выразить в виде $x\overline{x}$.

Полные системы

Примеры полных систем

- $\{\overline{x},\ x \vee y,\ xy\}$
- $\{\overline{x},\ x \vee y\}$
- $\{\overline{x},\ xy\}$
- $\{1,\ x \oplus y,\ xy\}$
- $\{\overline{x},\ x \to y\}$

Двойственность

Двойственные функции

- Функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ из P_2 называются двойственными, если $f(x_1 \ldots, x_n) = \overline{g}(\overline{x}_1, \ldots, \overline{x}_n)$.
- Функция, двойственная к f обозначается f^*.
- Дважды двойственная функция совпадает с исходной: $f^{**} = f$.
- Примеры:
  - 0 двойственна 1.
  - x двойственна сама себе.
  - $\overline{x}$ двойственна сама себе.
  - xy двойственна $x \vee y$.
  - $x \oplus y$ двойственна $x \oplus y \oplus 1$.
  - $x \to y$ двойственна $\overline{x}y$.
  - $x \oplus y \oplus z$ двойственна сама себе.
  - $\mathrm{m}(x, y, z) = xy \vee xz \vee yz$ двойственна сама себе.

Двойственность

Формулы с параметрами

- Будем пользоваться записью $\Phi(f_1, \ldots, f_n)$, для обозначения формулы, содержащей функциональные символы только из набора $\{f_1, \ldots, f_n\}$. При замене функциональных символов в скобках подразумеваем, что они заменяются и в самой формуле.
- Например, если $\Phi(\circ, \star, \times) = ((x \circ y) \times z) \circ (y \star z)$, то $\Phi(\oplus, \&, \vee) = ((x \oplus y) \vee z) \oplus (y \mathbin{\&} z)$ и $\Phi(\oplus, \&, \&) = ((x \oplus y) \mathbin{\&} z) \oplus (y \mathbin{\&} z)$.

Двойственность

Принцип двойственности

- Пусть $f_1, \dots, f_k$ — функциональные символы некоторых функций, а $f_1^*, \dots, f_k^*$ — функциональные символы двойственных им функций.
- Тогда, если формула $\Phi(f_1, \dots, f_k)$ для некоторого набора переменных реализует функцию $f \in P_2$, то формула $\Phi(f_1^*, \dots, f_k^*)$ для того же набора переменных реализует функцию f^*.
- Например, если $f(x, y) = xy \oplus z$, то $f^*(x, y) = (x \vee y) \oplus z \oplus 1$.

Двойственность

- Обозначим через Q^* класс всех функций, двойственных к функциям из Q.
- Если $Q_1 \subseteq Q_2$, то $Q_1^* \subseteq Q_2^*$.

Утверждение

Если Q — замкнутый класс, то Q^* — также замкнутый класс.

Утверждение

Если множество Q порождает замкнутый класс R, то множество Q^* порождает замкнутый класс R^*. В частности, если Q — базис класса R, то Q^* — базис класса R^*.

Двойственность

Класс самодвойственных функций

- Функция $f \in P_2$ называется самодвойственной, если $f = f^*$.
- Класс самодвойственных функций обозначается S и является замкнутым.

Лемма (о несамодвойственной функции)

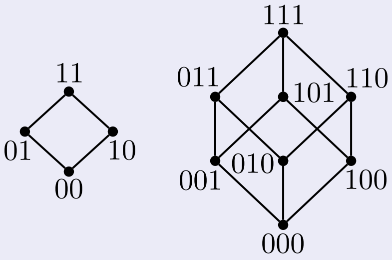
Из несамодвойственной функции путём подстановки вместо всех переменных функций x, $\overline{x}$ можно получить константу.

Класс монотонных функций

Частичный порядок на $\{0,1\}^n$

- Будем считать, что для $\alpha = (a_1, \dots, a_n)$ и $\beta = (b_1, \dots, b_n)$ из $\{0,1\}^n$ выполнено $\alpha \leqslant \beta$, если $a_1 \leqslant b_1$, $a_2 \leqslant b_2, \dots, a_n \leqslant b_n$.
- Отношение $\leqslant$ на множестве $\{0,1\}^n$ является отношением частичного порядка.

Примеры частичных порядков



$(0,0) \leqslant (0,1) \leqslant (1,1)$

$(0,1)$ и $(1,0)$ не сравнимы

$(0,0,0) \leqslant (0,1,0) \leqslant (0,1,1) \leqslant (1,1,1)$

$(0,1,0)$ и $(1,0,1)$ не сравнимы

Класс монотонных функций

Монотонность функции

- Функция $f(x_1, \dots, x_n)$ монотонна, если для любых $\alpha, \beta \in \{0,1\}^n$ из $\alpha \leqslant \beta$ следует $f(\alpha) \leqslant f(\beta)$.
- Класс монотонных функций в P_2 обозначается M. Класс монотонных функций является замкнутым.

- Функции 0, 1, x, xy, $x \vee y$ монотонны.
- Функции $\overline{x}$, $x \oplus y$, $x \to y$ не монотонны.

Лемма (о немонотонной функции)

Из немонотонной функции путём подстановки функций $0, 1, x$ вместо переменных можно получить $\overline{x}$.

Класс монотонных функций

Теорема

Для любой монотонной функции $f(x_1, \ldots, x_n)$ *имеет место представление*

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

Доказательство

- По разложению Шеннона

$$f(x_1, \ldots, x_n) = x_1 f(1, x_2, \ldots, x_n) \vee \overline{x}_1 f(0, x_2, \ldots, x_n).$$

- В силу монотонности функции, если $f(0, x_2, \ldots, x_n) = 1$, то и $f(1, x_2, \ldots, x_n)$. Поэтому

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

□

Класс монотонных функций

Теорема

Для любой монотонной функции $f(x_1, \ldots, x_n)$ *имеет место представление*

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

Следствие

Имеем $M = [0,\ 1,\ x \vee y,\ xy]$ (*базис*). *Если* f *— монотонная функция, отличная от константы, то* $f \in [x \vee y,\ xy]$.

Класс линейных функций

Полином Жегалкина

- Полином Жегалкина функции $f(x_1, \ldots, x_n)$ — это её представление в виде

$$f(x_1, \ldots, x_n) = a \oplus \bigoplus_{\substack{1 \leqslant i_1 < \ldots < i_s \leqslant n \\ s \in \{1, \ldots, n\}}} a_{i_1, \ldots, i_s} \cdot x_{i_1} \ldots x_{i_s}$$

- Каждая булева функция представима единственным полиномом Жегалкина (с точностью до перестановки слагаемых и множителей).

Линейные функции

- Функция f линейна, если её полином Жегалкина имеет только линейные слагаемые:

$$f(x_1, \ldots, x_n) = a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n.$$

Класс линейных функций

Линейные функции

- Класс линейных функций обозначается L. Этот класс замкнут.
- $L = [1, x \oplus y]$ (базис).

Класс линейных функций

Лемма (о нелинейной функции)

Из нелинейной функции путём подстановки вместо всех переменных функций $0, x, y$ можно получить нелинейную функцию от переменных x, y.

Доказательство

- Пусть $f(x_1, \ldots, x_n) \notin L$. Пусть $x_1 \ldots x_k$ — нелинейное слагаемое наименьшей степени в полиноме Жегалкина функции f.
- Заменим в функции $f(x_1, \ldots, x_n)$ переменную x_1 переменной x, переменные $x_2, \ldots, x_k$ — переменной y, а все остальные переменные — константой 0.
- Получим функцию от двух переменных. В силу минимальности $x_1 \ldots x_k$ все остальные нелинейные слагаемые содержат другие переменные и обнулятся, а данное слагаемое превратится в xy.

□

Функции, сохраняющие константы

Классы T_0 и T_1

- T_0 — это класс функций $f(x_1, \ldots, x_n) \in P_2$ таких, что $f(0, \ldots, 0) = 0$.
- T_1 — это класс функций $f(x_1, \ldots, x_n) \in P_2$ таких, что $f(1, \ldots, 1) = 1$.
- T_0 и T_1 являются замкнутыми классами.
- $T_1 = T_0^*$.

Функции, сохраняющие константы

Утверждение

$T_0 = [x \oplus y,\, xy] = [x \vee y,\, x\overline{y}]$ (*базисы*).

Доказательство

- Класс T_0 — это класс всех функций, в полиномах Жегалкина которых свободный член равен 0. Такие полиномы можно построить с помощью функций $\{x \oplus y,\, xy\}$ (в частности, $0 = x \oplus x$). Очевидно, что это базис.
- $x \oplus y = x\overline{y} \vee y\overline{x},\ \ xy = x(\overline{x} \vee y) = x\overline{x\overline{y}}$. Поэтому $T_0 = [x \vee y,\, x\overline{y}]$.
- Любая формула над $\{x\overline{y}\}$ имеет вид $x_i \cdot \Phi$. Если $x_i = 0$, то функция, реализуемая этой формулой, принимает 0. Но для функции $x \vee y$ нельзя найти такую переменную (какая бы переменная ни обратилась в 0, функция принимает значение 1, если в другой переменной 1). Поэтому $\{x \vee y,\, x\overline{y}\}$ — базис T_0.

$\square$

Функции, сохраняющие константы

Утверждение

$T_1 = [x \oplus y \oplus 1,\ x \vee y] = [xy,\ x \vee \overline{y}]$ (*базисы*).

Доказательство

- $T_0 = [x \oplus y,\ xy] = [x \vee y,\ x\overline{y}]$ (базисы).
- Поскольку $T_1 = T_0^*$, для получения базиса в T_1 достаточно взять двойственные функции к функциям базиса T_0.

$\square$

Предполные классы

Теорема (Пост)

Система булевых функций полна в P_2 тогда и только тогда, когда она целиком не содержится ни в одном из классов T_0, T_1, S, L, M.

Утверждение

Замкнутые классы T_0, T_1, S, L, M не содержатся друг в друге. Любой другой замкнутый класс, отличный от P_2, содержится хотя бы в одном из этих классов.

Определение

Замкнутый класс Q называется **предполным**, если $Q \neq P_2$, но для любой $f \notin Q$ система $Q \cup \{f\}$ полна в P_2.

Утверждение

T_0, T_1, S, L, M — *все предполные классы P_2.*

Конгруэнтные функции

Конгруэнтные функции

- Функции f и g называются конгруэнтными, если одну из них можно получить из другой перестановкой переменных и добавлением/удалением фиктивных переменных.
- Отношение конгруэнтности функций является отношением эквивалентности.
- Если Q — замкнутый класс и $f \in Q$, то все функции, конгруэнтные f, принадлежат Q.
- Пусть $\{f_\alpha \mid \alpha \in A\} \subseteq P_2$. Через $\{f_\alpha \mid \alpha \in A\}_c$ обозначим множество всех функций, конгруэнтных функциям $f_\alpha,\ \alpha \in A$.

Пример

- Функции $f(x, y) = x \to y$ и $g(x, y, z) = z \to x$ конгруэнтны.
- Функции $f(x, y) = x \to y$ и $g(x) = x \to x$ не конгруэнтны.

Другие замкнутые классы

Классы-пересечения

- $T_{01} = T_0 \cap T_1$.
- $M_0 = M \cap T_0 = M \setminus \{1\}_c = [xy,\, x \vee y,\, 0]$ (базис).
- $M_1 = M \cap T_1 = M \setminus \{0\}_c = [xy,\, x \vee y,\, 1]$ (базис).
- $M_{01} = M \cap T_{01} = M \setminus \{0, 1\}_c = [xy,\, x \vee y]$ (базис).

Другие замкнутые классы

Утверждение

$T_{01} = [xy,\, x \oplus y \oplus z] = [xy,\, x \vee y\bar{z}]$ (*базисы*).

Доказательство

- T_{01} — это класс функций, в полиномах Жегалкина которых нечётное число слагаемых, а свободный член равен 0. Такие полиномы можно построить с помощью функций $\{x \oplus y \oplus z,\, xy\}$. Очевидно, что это базис.
- $x \vee y = x \vee y\bar{x}$, $x \vee y\,\bar{z}\,\bar{w} = x \vee y\overline{(z \vee w)}$.
- Тогда можно построить $w \vee x\,\bar{y}\,\bar{z} \vee \bar{x}y\bar{z} \vee \bar{x}\,\bar{y}\,z$.
- Получаем $x \oplus y \oplus z = xyz \vee x\,\bar{y}\,\bar{z} \vee \bar{x}y\bar{z} \vee \bar{x}\,\bar{y}\,z$, $T_{01} = [xy,\, x \vee y\bar{z}]$.
- Формулы над $\{x \vee y\bar{z}\}$ имеют вид $x_i \vee \Phi$. Если $x_i = 1$, то функция обращается в 1. Но для xy, какая бы переменная ни равнялась 1, функция может обратиться в 0. Поэтому $\{xy,\, x \vee y\bar{z}\}$ — базис T_{01}.

□

Рассмотренные классы функций

Классы функций и их базисы

- $T_0 = [x \oplus y,\ xy] = [x \vee y,\ x\overline{y}]$.
- $T_1 = [x \oplus y \oplus 1,\ x \vee y] = [xy,\ x \vee \overline{y}]$.
- $T_{01} = T_0 \cap T_1 = [xy,\ x \oplus y \oplus z] = [xy,\ x \vee y\overline{z}]$.
- $L = [1,\ x \oplus y]$.
- $M = [0,\ 1,\ x \vee y,\ xy]$.
- $M_0 = M \cap T_0 = M \setminus \{1\}_c = [xy,\ x \vee y,\ 0]$.
- $M_1 = M \cap T_1 = M \setminus \{0\}_c = [xy,\ x \vee y,\ 1]$.
- $M_{01} = M \cap T_{01} = M \setminus \{0, 1\}_c = [xy,\ x \vee y]$.

Лекция 2
Классы функций одной переменной, дизъюнкций, конъюнкций и линейных функций. Лемма о самодвойственной нелинейной функции

Классы функций от одной переменной

Классы, лежащие в U

- $U = \{0, 1, x, \overline{x}\}_c$ — класс функций, существенно зависящих не более, чем от одной переменной.
- $C = \{0, 1\}_c$ — класс функций, не имеющих существенных переменных (константы).
- $U_0 = U \cap T_0 = \{0, x\}_c$.
- $U_1 = U \cap T_1 = \{1, x\}_c$.
- $MU = M \cap U = \{0, 1, x\}_c$.
- $SU = S \cap U = \{x, \overline{x}\}_c$.
- $U_{01} = U \cap T_{01} = \{x\}_c$.
- $C_0 = C \cap T_0 = \{0\}_c$.
- $C_1 = C \cap T_1 = \{1\}_c$.

Классы функций от одной переменной

Теорема

Произвольный замкнутый класс, целиком лежащий в классе U, совпадает с одним из следующих классов (указаны базисы классов):

$$U = [0, \overline{x}],\ U_0 = [0, x],\ U_1 = [1, x],\ MU = [0, 1, x],\ SU = [\overline{x}],$$
$$U_{01} = [x], \quad C = [0, 1], \quad C_0 = [0], \quad C_1 = [1].$$

Классы функций от одной переменной

Доказательство

- Перебираем все 16 подмножеств $\{0, 1, x, \overline{x}\}$.
- Исключаем из них часть подмножеств с учётом следующих правил:
  - Не рассматриваем пустое множество;
  - $x = \overline{\overline{x}}$, поэтому если класс содержит $\overline{x}$, то он содержит и x;
  - $0 = \overline{1}$, $1 = \overline{0}$, поэтому если класс содержит $\overline{x}$ и одну из констант, то он содержит и вторую константу.
- Остаётся 7 подмножеств, не содержащих $\overline{x}$ (всевозможные подмножества, кроме пустого), и 2 подмножества, содержащие $\overline{x}$ (без констант или с ними).
- Множество функций, конгруэнтных функциям любого оставшегося подмножества, является замкнутым классом.
- Различие этих 9 классов и построение базисов очевидно.

$\square$

Классы дизъюнкций и конъюнкций

Классы дизъюнкций

- $D = \{a_0 \vee a_1 x_1 \vee \ldots \vee a_n x_n \mid a_0, \ldots, a_n \in E_2,\ n \in \mathbb{N}\}$.
- $D_0 = D \cap T_0 = D \setminus \{1\}_c$.
- $D_1 = D \cap T_1 = D \setminus \{0\}_c$.
- $D_{01} = D \cap T_{01} = D \setminus \{0, 1\}_c$.

Классы конъюнкций

- $K = \{a_0 \,\&\, (a_1 \vee x_1) \,\&\, \ldots \,\&\, (a_n \vee x_n) \mid a_0, \ldots, a_n \in E_2,\ n \in \mathbb{N}\}$.
- $K_0 = K \cap T_0 = K \setminus \{1\}_c$.
- $K_1 = K \cap T_1 = K \setminus \{0\}_c$.
- $K_{01} = K \cap T_{01} = K \setminus \{0, 1\}_c$.

- $K = D^*,\ K_0 = D_1^*,\ K_1 = D_0^*,\ K_{01} = D_{01}^*$.

Классы дизъюнкций и конъюнкций

Теорема

Произвольный замкнутый класс, целиком лежащий в одном из классов D, K и не содержащийся в классе U, совпадает с одним из следующих классов (указаны базисы классов):

$$D = [0,\ 1,\ x \vee y],\ D_0 = [0,\ x \vee y],\ D_1 = [1,\ x \vee y],\ D_{01} = [x \vee y],$$
$$K = [0,\ 1,\ xy], \quad K_0 = [0,\ xy], \quad K_1 = [1,\ xy], \quad K_{01} = [xy].$$

Классы дизъюнкций и конъюнкций

Доказательство

- Базисы классов очевидны.
- Пусть F — замкнутый класс, $F \subseteq D$ и $F \not\subseteq U$. Тогда в F входит дизъюнкция с хотя бы двумя существенными переменными. Отождествлением переменных получаем $x \vee y$.
- Это значит, что $D_{01} \subseteq F$. В зависимости от вхождения в F констант получаем 4 варианта: $F \in \{D, D_0, D_1, D_{01}\}$
- Пусть $F \subseteq K$, $F \not\subseteq U$. Тогда $F^* \subseteq D$, $F^* \not\subseteq U$.
- По доказанному выше получаем, что $F^* \in \{D, D_0, D_1, D_{01}\}$.
- Значит, $F \in \{K, K_0, K_1, K_{01}\}$.

$\square$

Классы линейных функций

- Для $\alpha \in E_2^n$ через $|\alpha|$ обозначаем число единиц в наборе α.

Классы линейных функций

- $L = \{a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \mid a_0, \ldots, a_n \in E_2,\ n \in \mathbb{N}\}$.
- $L_0 = L \cap T_0 = \{0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \mid a_1, \ldots, a_n \in E_2,\ n \in \mathbb{N}\}$.
- $L_1 = L \cap T_1 = \{a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \mid |(a_0, \ldots, a_n)|$ неч., $n \in \mathbb{N}\}$.
- $SL = S \cap L = \{a_0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \mid |(a_1, \ldots, a_n)|$ неч., $n \in \mathbb{N}\}$.
- $L_{01} = L \cap T_{01} = \{0 \oplus a_1 x_1 \oplus \ldots \oplus a_n x_n \mid |(a_1, \ldots, a_n)|$ неч., $n \in \mathbb{N}\}$.

Классы линейных функций

Теорема

Произвольный замкнутый класс, целиком лежащий в классе L и не содержащийся в классе U, совпадает с одним из следующих классов (указаны базисы классов) :

$$L = [1, x \oplus y], \quad L_0 = [x \oplus y], \quad L_1 = [x \oplus y \oplus 1],$$
$$SL = [x \oplus y \oplus z \oplus 1], \quad L_{01} = [x \oplus y \oplus z].$$

Доказательство

- Пусть F — замкнутый класс, $F \subseteq L$ и $F \not\subseteq U$. Тогда в F есть функция с хотя бы двумя существенными переменными.
- Отождествлением переменных получаем $x \oplus y \oplus a$ или $x \oplus y \oplus z \oplus a$, $a \in \{0, 1\}$.
- Пусть можем получить $x \oplus y$ и $x \oplus y \oplus 1$. Тогда $1 = x \oplus x \oplus 1 \in F$, значит $F = L$.

Классы линейных функций

Доказательство (продолжение)

- Пусть можем получить $x \oplus y$, но не $x \oplus y \oplus 1$. Тогда $0 = x \oplus x \in F$, и легко видеть, что $L_0 \subseteq F$. Вместе с тем класс F не содержит функций не из T_0: иначе подстановкой 0 в такую функцию мы получили бы $1 \in F$, тогда $1 \oplus x \oplus y \in F$. Значит, $F = L_0$.
- Пусть можем получить $x \oplus y \oplus 1$, но не $x \oplus y$. Тогда $F^* = L_0$. Но нетрудно видеть, что $L_1 = L_0^*$. Поэтому $F = L_1$.
- Пусть $x \oplus y \oplus a \notin F,\ a \in \{0, 1\}$. Тогда каждая функция из F существенно зависит от нечётного числа переменных. Это значит, что $F \subseteq SL$.
- Если $1 \oplus x \oplus y \oplus z \in F$, то $x \oplus 1 \in F$ и $x \oplus y \oplus z \in F$. С помощью $x \oplus y \oplus z$ к любой линейной функции можно добавить две существенные переменные. Поэтому мы можем получить все функции из $SL,\ F = SL$.

Классы линейных функций

Доказательство (продолжение)

- Пусть $x \oplus y$, $x \oplus y \oplus 1$, $x \oplus y \oplus z \oplus 1 \notin F$. Тогда остаётся только $x \oplus y \oplus z \in F$. Аналогично случаю L_0 верно $F \subseteq T_0$. В этом случае требование $F \subseteq T_1$ совпадает с требованием $F \subseteq S$, значит $F \subseteq L_{01}$. При этом с помощью $x \oplus y \oplus z$ можно построить любую линейную функцию без свободного члена, зависящую от нечётного числа переменных. Поэтому $F = L_{01}$.
- Из хода доказательства следует, что приведённые системы функций являются базисами классов L_0, L_1, SL, L_{01}.

$\square$

Классы самодвойственных функций

Классы самодвойственных функций

- $S = \{f \in P_2 \colon f(x_1, \ldots, x_n) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_n)\}$.
- $S_{01} = S \cap T_0 = S \cap T_1 = S \cap T_{01}$.
- $SM = S \cap M$.

Медиана

- Функция $\mathrm{m}(x, y, z) = xy \vee xz \vee yz = xy \oplus xz \oplus yz$ называется медианой.
- $\mathrm{m}(x, y, z) \in (T_0 \cap T_1 \cap S \cap M) \setminus L$.
- Медиана не изменяется при перестановке переменных.
- $\mathrm{m}(x, x, y) = x$.

Классы самодвойственных функций

Лемма

Пусть $f \in S \setminus L$. Тогда отождествлением и перестановкой переменных из функции f можно получить одну из функций

$$\mathrm{m}(x, y, z), \quad \mathrm{m}(x, y, \overline{z}), \quad \mathrm{m}(x, \overline{y}, \overline{z}), \quad \mathrm{m}(\overline{x}, \overline{y}, \overline{z}).$$

Доказательство

- По лемме о нелинейной функции подстановкой $0, y, z$ вместо всех переменных f можно получить нелинейную функцию. Если мы будем вместо нулей подставлять переменную x, получим функцию $g(x, y, z)$ такую, что $g(0, y, z) \notin L$. Ясно, что $g(x, y, z) \in S \setminus L$.

Классы самодвойственных функций

Доказательство (продолжение)

- Полином нелинейной функции от переменных y, z имеет нелинейное слагаемое yz и может иметь или не иметь каждое из трёх слагаемых $y, z, 1$ (во всех случаях получаются разные функции). Поэтому всего таких функций 8.
- Возможные варианты $g(0, y, z)$. $y^{\sigma_1} z^{\sigma_2}$ двойственна к $y^{\sigma_1} \vee z^{\sigma_2}$.

$$yz,\ \overline{y}z,\ y\overline{z},\ \overline{y}\,\overline{z},\quad y \vee z,\ \overline{y} \vee z,\ y \vee \overline{z},\ \overline{y} \vee \overline{z}$$

- Поскольку $g \in S$, верно $g(1, y, z) = \overline{g}(0, \overline{y}, \overline{z})$, поэтому $g(x, y, z)$ строится однозначно по $g(0, y, z)$ и $g(1, y, z)$ является двойственной к $g(0, y, z)$.
- По $y^{\sigma_1} z^{\sigma_2}$ получаем $\overline{x} y^{\sigma_1} z^{\sigma_2} \vee x y^{\sigma_1} \vee x z^{\sigma_2} = \mathrm{m}(x, y^{\sigma_1}, z^{\sigma_2})$.
- По $y^{\sigma_1} \vee z^{\sigma_2}$ получаем $\overline{x} y^{\sigma_1} \vee \overline{x} z^{\sigma_2} \vee x y^{\sigma_1} z^{\sigma_2} = \mathrm{m}(\overline{x}, y^{\sigma_1}, z^{\sigma_2})$.

$\square$

Лекция 3
Классы самодвойственных функций. Определения и простейшие свойства классов O^{∞}, I^{∞}

Классы самодвойственных функций

Лемма

Имеют место соотношения (указаны базисы классов)

$$S = [\mathrm{m}(x, \overline{y}, \overline{z})] = [\mathrm{m}(\overline{x}, \overline{y}, \overline{z})] = [\mathrm{m}(x, y, z),\ \overline{x}],$$
$$S_{01} = [\mathrm{m}(x, y, \overline{z})], \quad SM = [\mathrm{m}(x, y, z)].$$

Доказательство

- Рассмотрим класс S. $\mathrm{m}(x, \overline{x}, \overline{x}) = \mathrm{m}(\overline{x}, \overline{x}, \overline{x}) = \overline{x}$. Поэтому $[\mathrm{m}(x, \overline{y}, \overline{z})] = [\mathrm{m}(\overline{x}, \overline{y}, \overline{z})] = [\mathrm{m}(x, y, z),\ \overline{x}]$. Также $\mathrm{m}(x, \overline{y}, \overline{z}) \in S$.
- $\mathrm{m}(0, \overline{y}, \overline{z}) = \overline{y}\,\overline{z} = y \downarrow z$ — стрелка Пирса. Поскольку $\overline{x} = x \downarrow x$, $xy = \overline{x} \downarrow \overline{y}$, стрелка Пирса является полной системой.
- То есть любую функцию можно реализовать формулой над $\mathrm{m}(0, \overline{y}, \overline{z})$.

Классы самодвойственных функций

Доказательство (продолжение)

- Пусть $f(x_1, \dots, x_n) \in S$. Функцию $f(0, x_2, \dots, x_n)$ можно реализовать формулой $\Phi(\mathrm{m}(0, \overline{y}, \overline{z}))$.
- Легко видеть, что $\mathrm{m}(0, \overline{y}, \overline{z})$ и $\mathrm{m}(1, \overline{y}, \overline{z})$ двойственны.
- Так как $f \in S$, $f(1, x_2, \dots, x_n) = \overline{f}(0, \overline{x}_2, \dots, \overline{x}_n)$, то есть $f(0, x_2, \dots, x_n)$ и $f(1, x_2, \dots, x_n)$ двойственны.
- Тогда по принципу двойственности $f(1, x_2, \dots, x_n)$ реализуется формулой $\Phi(\mathrm{m}(1, \overline{y}, \overline{z}))$.
- Получаем, что $f(x_1, \dots, x_n)$ реализуется формулой $\Phi(\mathrm{m}(x_1, \overline{y}, \overline{z}))$, которая получается из $\Phi(\mathrm{m}(0, \overline{y}, \overline{z}))$ заменой нулей в медианах на переменную x_1.
- Это означает, что $S = [\mathrm{m}(x, \overline{y}, \overline{z})] = [\mathrm{m}(\overline{x}, \overline{y}, \overline{z})] = [\mathrm{m}(x, y, z),\ \overline{x}]$.
- То, что все три системы являются базисами, очевидно.

Классы самодвойственных функций

Доказательство (продолжение)

- Рассмотрим класс S_{01}. Ясно, что $\mathrm{m}(x, y, \overline{z}) \in S_{01}$. $\mathrm{m}(0, y, \overline{z}) = y\overline{z}$, $\mathrm{m}(x, y, \overline{0}) = x \vee y$. При этом $T_0 = [x \vee y,\ x\overline{y}]$.
- Пусть $f(x_1, \ldots, x_n) \in S_{01}$. Функцию $f(0, x_2, \ldots, x_n) \in T_0$ можно реализовать формулой $\Phi(\mathrm{m}(0, y, \overline{z}), \mathrm{m}(x, y, \overline{0}))$.
- Легко видеть, что $\mathrm{m}(0, y, \overline{z})$ двойственна к $\mathrm{m}(1, y, \overline{z})$, а $\mathrm{m}(x, y, \overline{0})$ двойственна к $\mathrm{m}(x, y, \overline{1})$.
- Так как $f \in S$, $f(0, x_2, \ldots, x_n)$ и $f(1, x_2, \ldots, x_n)$ двойственны.
- Тогда по принципу двойственности $f(1, x_2, \ldots, x_n)$ реализуется формулой $\Phi(\mathrm{m}(1, y, \overline{z}), \mathrm{m}(x, y, \overline{1}))$.
- Тогда $f(x_1, \ldots, x_n)$ реализуема как $\Phi(\mathrm{m}(x_1, y, \overline{z}), \mathrm{m}(x, y, \overline{x}_1))$; эта формула получается из $\Phi(\mathrm{m}(0, y, \overline{z}), \mathrm{m}(x, y, \overline{0}))$ заменой нулей в медианах с отрицаниями на переменную x_1.
- Значит, $S_{01} = [\mathrm{m}(x, y, \overline{z})]$.

Классы самодвойственных функций

Утверждение

Пусть $f(x_1, \ldots, x_n) \in SM,\ n \geqslant 3,\ \tilde{x} = (x_4, \ldots, x_n)$. *Тогда*

$$f(x_1, x_2, x_3, \tilde{x}) = \mathrm{m}(f(x_1, x_1, x_3, \tilde{x}), f(x_1, x_2, x_2, \tilde{x}), f(x_3, x_2, x_3, \tilde{x})).$$

Замечание

- В i-й позиции внутри медианы стоит функция f, у которой переменная x_i подставлена на место следующей (циклически) за ней переменной.
- Подставляем x_1 на место x_2: $f(x_1, x_1, x_3, \tilde{x})$.
- Подставляем x_2 на место x_3: $f(x_1, x_2, x_2, \tilde{x})$.
- Подставляем x_3 на место x_1: $f(x_3, x_2, x_3, \tilde{x})$.

Классы самодвойственных функций

Утверждение

Пусть $f(x_1, \ldots, x_n) \in SM$, $n \geqslant 3$, $\tilde{x} = (x_4, \ldots, x_n)$. *Тогда*

$$f(x_1, x_2, x_3, \tilde{x}) = \mathrm{m}(f(x_1, x_1, x_3, \tilde{x}), f(x_1, x_2, x_2, \tilde{x}), f(x_3, x_2, x_3, \tilde{x})).$$

Доказательство утверждения

- Функции слева и справа принадлежат S. Поэтому достаточно доказать их совпадение на половине всех наборов, не содержащей противоположных наборов, то есть на (x_1, x_2, x_3): $(0,0,0)$, $(1,0,0)$, $(0,1,0)$, $(0,0,1)$.
- Для $(1,0,0)$: $f(0,0,0,\tilde{x}) \leqslant f(1,0,0,\tilde{x}) \leqslant f(1,1,0,\tilde{x})$. Поэтому хотя бы два из этих значений совпадают и равны $f(1,0,0,\tilde{x})$, и медиана выдаст это значение. Случай $(0,0,0)$ очевиден.
- Случаи $(0,1,0)$, $(0,0,1)$ рассматриваются аналогично.

□

Классы самодвойственных функций

Доказательство леммы (продолжение)

- Рассмотрим класс SM. $\mathrm{m}(x,y,z)\in SM,\ \ x=\mathrm{m}(x,x,x)$.
- Из функций одной переменной SM принадлежит только x, а функции от двух переменных не бывают самодвойственными.
- Пусть $f(x_1,\dots,x_n)\in SM,\ \ n\geqslant 3$. Тогда по утверждению

  $$f(x_1,x_2,x_3,\tilde{x})=\mathrm{m}(f(x_1,x_1,x_3,\tilde{x}),f(x_1,x_2,x_2,\tilde{x}),f(x_3,x_2,x_3,\tilde{x})).$$

- Каждая из функций внутри медианы зависит от меньшего числа переменных. Применяем к ним то же утверждение. В конце концов получим формулу, содержащую медианы и функции от двух переменных. Но эти функции самодвойственны и монотонны, поэтому конгруэнтны x и выражаются символами переменных.
- Поэтому $SM=[\mathrm{m}(x,y,z)]$.

$\square$

Классы самодвойственных функций

Теорема

Произвольный замкнутый класс, целиком лежащий в классе S и не содержащийся в L, совпадает с одним из классов (указаны базисы)

$$S = [\mathrm{m}(x, y, z),\ \overline{x}], \quad S_{01} = [\mathrm{m}(x, y, \overline{z})], \quad SM = [\mathrm{m}(x, y, z)].$$

Доказательство

- Поскольку $M \subseteq T_{01} \cup \{0, 1\}_c$, а $0, 1 \notin S$, $SM \subseteq S_{01} \subseteq S$.
- Пусть F — замкнутый класс, $F \subseteq S$ и $F \not\subseteq L$. В силу доказанных лемм $SM \subseteq F$. Пусть $F \neq SM$, $f(x_1, \ldots, x_n) \in F \setminus M$.
- По лемме о немонотонной функции подстановкой в f функций $0, 1, z$ можно получить функцию $\overline{z}$.
- Будем вместо нулей подставлять x, а вместо единиц — y. Получим $g(x, y, z) \in F \setminus M$, $g(x, y, z) \in S$, $g(0, 1, z) = \overline{z}$.

Классы самодвойственных функций

Доказательство

- Чтобы определить функцию $g(x, y, z)$, достаточно задать подфункцию $g(0, 0, x)$, так как $g(0, 1, x) = \overline{x}$, а подфункция $g(1, x, y)$ определяется по самодвойственности. Варианты:
- $g_1(0,0,z) = 0,\ \ g_1(0,y,z) = y\overline{z},\ \ g_1(x,y,z) = \mathrm{m}(x,y,\overline{z}).$
  $g_2(0,0,z) = z,\ \ g_2(0,y,z) = y \oplus z,\ \ g_2(x,y,z) = x \oplus y \oplus z.$
  $g_3(0,0,z) = \overline{z},\ \ g_3(0,y,z) = \overline{z},\ \ g_3(x,y,z) = \overline{z}.$
  $g_4(0,0,z) = 1,\ \ g_4(0,y,z) = \overline{y} \vee \overline{z},\ \ g_4(x,y,z) = \mathrm{m}(\overline{x},\overline{y},\overline{z}).$
- То есть, хотя бы одна из функций g_1, g_2, g_3, g_4 принадлежит F. Если $g_3 \in F$ или $g_4 \in F$, то, очевидно, $F = S$.
- Пусть $g_3, g_4 \notin F$. $\mathrm{m}(x, y, \overline{z}) = \mathrm{m}(x, y, z) \oplus x \oplus y$, поэтому $\mathrm{m}(x, y, \overline{z}) \in F$ и $S_{01} \subseteq F$. Если $F \neq S_{01}$, то существует $h \in F \setminus T_0$. Тогда $h(x, \ldots, x) \in \{1, \overline{x}\}$. Но эта функция самодвойственна, поэтому $h(x, \ldots, x) = \overline{x} = g_3 \notin F$. Значит, $F = S_{01}$.

□

Классы вида O^∞ и I^∞

Класс O^∞

- O^∞ — класс функций, все нулевые наборы которых имеют общую нулевую компоненту.

$$O^\infty = \{f(x_1, \dots, x_n) \in P_2 \colon (\exists i)((f(x_1, \dots, x_n) = 0) \to (x_i = 0))\}.$$

- Можно записать это иначе:

$$O^\infty = \{f(x_1, \dots, x_n) \in P_2 \colon (\exists i)((x_i = 1) \to (f(x_1, \dots, x_n) = 1))\}.$$

- Тогда O^∞ — это класс функций, представимых в виде

$$f(x_1, \dots, x_n) = x_i \vee f(x_1, \dots, x_{i-1}, 0, x_{i+1}, \dots, x_n).$$

- Из этого представления ясно, что класс O^∞ замкнут.
- Отметим, что 1, $x \vee y \in O^\infty$ и $O^\infty \subseteq T_1$.

Классы вида O^∞ и I^∞

Класс I^∞

- I^∞ — класс функций, все единичные наборы которых имеют общую единичную компоненту.

$$I^\infty = \{f(x_1, \ldots, x_n) \in P_2 \colon (\exists i)((f(x_1, \ldots, x_n) = 1) \to (x_i = 1))\}.$$

- Можно записать это иначе:

$$I^\infty = \{f(x_1, \ldots, x_n) \in P_2 \colon (\exists i)((x_i = 0) \to (f(x_1, \ldots, x_n) = 0))\}.$$

- Тогда I^∞ — это класс функций, представимых в виде

$$f(x_1, \ldots, x_n) = x_i \cdot f(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n).$$

- Из этого представления ясно, что класс I^∞ замкнут.
- Отметим, что 0, $xy \in I^\infty$ и $I^\infty \subseteq T_0$.

Классы вида O^∞ и I^∞

Производные классы от O^∞ и I^∞

- O^∞, I^∞.
- $O_0^\infty = O^\infty \cap T_0$, $I_1^\infty = I^\infty \cap T_1$.
- $MO^\infty = M \cap O^\infty$, $MI^\infty = M \cap I^\infty$.
- $MO_0^\infty = M \cap O_0^\infty = MO^\infty \setminus \{1\}_c$, $MI_1^\infty = M \cap I_1^\infty = MI^\infty \setminus \{0\}_c$.

Двойственность классов вида O^∞ и I^∞

- $O^\infty = (I^\infty)^*$.
- $O_0^\infty = (I_1^\infty)^*$.
- $MO^\infty = (MI^\infty)^*$.
- $MO_0^\infty = (MI_1^\infty)^*$.

Лекция 4
Классы вида O^∞, I^∞

Классы вида O^∞ и I^∞

Лемма

Пусть $f(x_1, \ldots, x_n) \in O^\infty \setminus D$. Тогда в зависимости от соотношения

$$f \notin T_0, \quad f \in T_0 \setminus M, \quad f \in M$$

множество $[f]$ содержит функцию $x \vee \overline{y}$, $x \vee y\overline{z}$ или $x \vee yz$ соответственно.

Доказательство

- Отметим, что поскольку $f \notin D$, f не является константой. Поэтому три указанных в условии теоремы варианта не пересекаются и исчерпывают все возможные случаи выбора f.
- Пусть $f(x_1, \ldots, x_n) = x_1 \vee f(0, x_2, \ldots, x_n)$, обозначим $g(x_2, \ldots, x_n) = f(0, x_2, \ldots, x_n)$. Так как $f \notin D$, верно $g \notin D$.

Классы вида O^∞ и I^∞

Доказательство (продолжение)

- Пусть $g \notin M$. По лемме о немонотонной функции подстановкой на место переменных $f(0, x_2, \ldots, x_n)$ функций $0, 1, z$ можно получить функцию $\overline{z}$.
- Будем вместо нулей подставлять x, а вместо единиц — y. На место переменной x_1 функции f тоже подставим x. Получим функцию $h(x, y, z) \in [f]$ такую, что $h(0, 1, z) = \overline{z}$. При этом $h(x, y, z) = x \vee h(0, y, z)$.
- Возможные варианты $h(0, y, z)$: $y\overline{z}$, $\overline{z}$, $\overline{y}z \vee y\overline{z}$, $\overline{y} \vee \overline{z}$.
- Варианты $h(x, y, z)$: $x \vee y\overline{z}$, $x \vee \overline{z}$, $x \vee \overline{y}z \vee y\overline{z}$, $x \vee \overline{y} \vee \overline{z}$.
- Если $f \notin T_0$, то $h(0, 0, 0) = 1$. Тогда остаются $x \vee \overline{z}$, $x \vee \overline{y} \vee \overline{z}$ и $h(x, y, y) = x \vee \overline{y} \in [f]$.
- Если $f \in T_0 \setminus M$, то $h(0, 0, 0) = 0$. Остаются $x \vee y\overline{z}$, $x \vee \overline{y}z \vee y\overline{z}$. В первом случае нужная функция получена. Во втором $h(x, y, x) = x \vee y$, $h(x,\ y \vee z,\ z) = x \vee y\overline{z}$.

Классы вида O^∞ и I^∞

Доказательство (продолжение)

- Пусть теперь $g \in M$. Представим g в виде ДНФ без отрицаний и без поглощений (т. е. ДНФ, где невозможно удалить никакое слагаемое по правилу $A \vee AB = A$). Тогда $g = K_1 \vee \ldots \vee K_s$, $f = x_1 \vee K_1 \vee \ldots \vee K_s$. Поскольку $g \notin D$, среди $K_1, \ldots, K_s$ есть хотя бы одна ЭК из двух и более букв.
- Пусть неоднобуквенная ЭК наименьшего ранга в ДНФ есть $x_{i_1} \ldots x_{i_t}$. Подставим в f переменную x_1 вместо всех переменных, кроме $x_{i_1}, \ldots, x_{i_t}$.
- Тогда в каждой ЭК, кроме однобуквенных и $x_{i_1} \ldots x_{i_t}$, окажется переменная x_1. Однобуквенные ЭК не поглощают $x_{i_1} \ldots x_{i_t}$, поэтому превратятся в x_1. Применяя правила поглощения, получим $x_1 \vee x_{i_1} \ldots x_{i_t}$.
- Отождествляя далее переменные получим $x \vee yz \in [f]$.

$\square$

Классы вида O^∞ и I^∞

Следствие

Пусть $f(x_1, \dots, x_n) \notin O^\infty$ *и* $f \neq 0$. *Тогда в зависимости от соотношения*

$$f \notin T_0, \quad f \in T_0 \setminus M, \quad f \in M$$

множество $[x \vee y, f]$ *содержит функцию* $x \vee \overline{y}$, $x \vee y\overline{z}$ *или* $x \vee yz$ *соответственно.*

Доказательство

- Поскольку $f \neq 0, 1$, три указанных в условии теоремы варианта не пересекаются и исчерпывают все возможные случаи выбора f.
- Пусть $g(x_1, \dots, x_n, y) = f(x_1, \dots, x_n) \vee y \in [x \vee y, f]$. Тогда $g \in O^\infty$, но поскольку $D \setminus \{0\} \subseteq O^\infty$, $f, g \notin D$. При этом $(f \in T_0) \equiv (g \in T_0)$ и $(f \in M) \equiv (g \in M)$.
- Применяя лемму к g, получаем требуемый результат.

$\square$

Классы вида O^∞ и I^∞

Лемма

Имеют место соотношения (указаны базисы классов)

$$O^\infty = [x \vee \overline{y}],\ O_0^\infty = [x \vee y\overline{z}],\ MO^\infty = [1,\, x \vee yz],\ MO_0^\infty = [x \vee yz],$$
$$I^\infty = [x\overline{y}],\ I_1^\infty = [x(y \vee \overline{z})],\ MI^\infty = [0,\, x(y \vee z)],\ MI_1^\infty = [x(y \vee z)].$$

Доказательство

- Пусть $f \in MO_0^\infty$, $f(x_1, \ldots, x_n) = x_1 \vee f(0, x_2, \ldots, x_n)$. Тогда $f(0, x_2, \ldots, x_n) \in M$ и представима в виде ДНФ без отрицаний $K_1 \vee \ldots \vee K_s$. Тогда $f = x_1 \vee K_1 \vee \ldots \vee K_s$.
- $x \vee y = x \vee yy,\ x \vee yzv = x \vee y(x \vee zv),\ x \vee yzvw = x \vee yz(x \vee vw),\ \ldots$
- Получаем $x_1 \vee K$ для любой ЭК K без отрицаний. Далее $x_1 \vee K_1 \vee K_2 \vee \ldots \vee K_s = (x_1 \vee K_1) \vee (x_1 \vee K_2) \vee \ldots \vee (x_1 \vee K_s)$. Значит, $f \in [x \vee yz]$.

Классы вида O^∞ и I^∞

Доказательство (продолжение)

- $MO^\infty = MO_0^\infty \cup \{1\}_c$, поэтому $MO^\infty = [1, x \vee yz]$.
- Пусть $f \in O_0^\infty$, $f(x_1, \ldots, x_n) = x_1 \vee f(0, x_2, \ldots, x_n)$. Тогда $f(0, x_2, \ldots, x_n)$ представима в виде ДНФ $K_1 \vee \ldots \vee K_s$, а $f = x_1 \vee K_1 \vee \ldots \vee K_s$.
- Поскольку $f \in T_0$, каждое слагаемое в ДНФ имеет хотя бы одну переменную без отрицания.
- $x \vee y = x \vee y\overline{x}$, $x \vee yz = x \vee y\overline{(x \vee y\overline{z})}$. Получаем $x \vee K$ для любой ЭК K без отрицаний.
- $x_1 \vee x_2 \ldots x_k\overline{x}_{k+1} = x_1 \vee x_2 \ldots x_k(x_1 \vee x_2\overline{x}_{k+1})$
  $x_1 \vee x_2 \ldots x_k\overline{x}_{k+1}\overline{x}_{k+2} = x_1 \vee x_2 \ldots x_k\overline{x}_{k+1}(x_1 \vee x_2\overline{x}_{k+2})$
  Продолжая аналогично получаем $x_1 \vee K$ для любой ЭК K с хотя бы одной буквой без отрицания.
- Аналогично MO_0^∞ строим ДНФ f, получаем $f \in [x \vee y\overline{z}]$.

Классы вида O^∞ и I^∞

Доказательство (продолжение)

- Пусть $f \in O^\infty$, $f(x_1, \dots, x_n) = x_1 \vee f(0, x_2, \dots, x_n)$. Тогда $f(0, x_2, \dots, x_n)$ представима в виде ДНФ $K_1 \vee \dots \vee K_s$, а $f = x_1 \vee K_1 \vee \dots \vee K_s$.
- $x \vee y\overline{z} = x \vee \overline{(\overline{y} \vee z)}$. Получаем $x \vee y$ и $x \vee K$ для любой ЭК K, содержащей хотя бы одну букву без отрицания.
- $x \vee \overline{y}\,\overline{z} = x \vee \overline{(y \vee z)}$
  $x \vee \overline{y}\,\overline{z}\,\overline{v} = x \vee \overline{y}\overline{(z \vee v)}$
  Продолжая аналогично, получаем $x_1 \vee K$ для любой ЭК K, состоящей только из букв с отрицаниями, а значит и для произвольной ЭК.
- Аналогично MO_0^∞ строим ДНФ f, получаем $f \in [x \vee \overline{y}]$.
- Базисы для классов $I^\infty, I_1^\infty, MI^\infty, MI_1^\infty$ получаем по принципу двойственности.

$\square$

Классы вида O^∞ и I^∞

Теорема

Произвольный замкнутый класс, целиком лежащий в классе O^∞ и не содержащийся в D, совпадает с одним из классов (указаны базисы)

$$O^\infty = [x \vee \overline{y}],\ O_0^\infty = [x \vee y\overline{z}],\ MO^\infty = [1,\, x \vee yz],\ MO_0^\infty = [x \vee yz].$$

Произвольный замкнутый класс, целиком лежащий в классе I^∞ и не содержащийся в K, совпадает с одним из классов (указаны базисы)

$$I^\infty = [x\overline{y}],\ I_1^\infty = [x(y \vee \overline{z})],\ MI^\infty = [0,\, x(y \vee z)],\ MI_1^\infty = [x(y \vee z)].$$

Классы вида O^∞ и I^∞

Доказательство

- Пусть $R = [R] \subseteq O^\infty$, $R \not\subseteq D$.
- Пусть $R \not\subseteq M$. Тогда существует $f \in R \setminus M$. Ясно, что $f \notin D$.
- По лемме получаем $x \vee \overline{y}$ или $x \vee y\overline{z}$ (в зависимости от принадлежности f классу T_0), значит $x \vee y\overline{z} \in R$, $O_0^\infty \subseteq R$.
- Если $R \subseteq T_0$, то $R = O_0^\infty$.
- Если $R \not\subseteq T_0$, то существует функция $g \in R \setminus T_0$. Поскольку также $R \subseteq O^\infty \subseteq T_1$, $g(0, \ldots, 0) = g(1, \ldots, 1) = 1$.
- Тогда получаем $1 = g(x, \ldots, x) \in R$ и $x \vee \overline{y} = x \vee 1 \cdot \overline{y} \in R$. Значит, $R = O^\infty$.
- Пусть $R \subseteq M$. Тогда существует функция $f \in R \setminus D$, $f \in M$. По лемме получаем $x \vee yz \in R$ и $MO_0^\infty \subseteq R$.
- Поскольку $R \subseteq MO^\infty$, если $1 \in R$, то $R = MO^\infty$. Иначе $R = MO_0^\infty$.

Классы вида O^∞ и I^∞

Доказательство (продолжение)

- Пусть теперь $R = [R] \subseteq I^\infty$, $R \not\subseteq K$. Тогда $R^* \subseteq O^\infty$, $R^* \not\subseteq D$.
- По доказанному $R^* \in \{O^\infty, O_0^\infty, MO^\infty, MO_0^\infty\}$.
- Тогда $R \in \{I^\infty, I_1^\infty, MI^\infty, MI_1^\infty\}$.

$\square$

Лекция 5

Классы вида O^m, I^m: определения и лемма о получении d_m из функции из $T_1 \setminus O^\infty$

Классы вида O^m и I^m

Классы O^m

- Пусть $m \geqslant 2$. O^m — класс функций, любые m (или менее) нулевых наборов которых имеют общую нулевую компоненту.

$$O^m = \{f \in P_2 \colon (\forall \alpha^1 \ldots, \alpha^m)((f(\alpha^1) = \ldots = f(\alpha^m) = 0) \\ \rightarrow (\exists i)(\alpha_i^1 = \ldots = \alpha_i^m = 0))\}.$$

- Иначе говоря,

$$O^m = \{f \in P_2 \colon (\forall \alpha^1 \ldots, \alpha^m)(((\forall i)(\exists j)(\alpha_i^j = 1) \rightarrow (\exists j)(f(\alpha^j) = 1))\}.$$

- Указанное свойство сохраняется при подстановке $f(\bar{x}) = g_0(g_1(\bar{x}), \ldots, g_k(\bar{x}))$.
- Очевидно, что $O^\infty \subseteq O^m$. Значит, все функции $I_i^n(x_1, \ldots, x_n) = x_i,\ i = \overline{1, n},\ n \in \mathbb{N}$ принадлежат O^m.
- Из двух приведённых выше фактов следует, что класс O^m замкнут.

Классы вида O^m и I^m

Классы O^m

$$O^m = \{f \in P_2 \colon (\forall \alpha^1 \ldots, \alpha^m)((f(\alpha^1) = \ldots = f(\alpha^m) = 0) \\ \to (\exists i)(\alpha_i^1 = \ldots = \alpha_i^m = 0))\}.$$

- Очевидно, что $O^\infty \subseteq O^m \subseteq T_1$ и $O^{m+1} \subseteq O^m$ при $m \geqslant 2$.
- Получаем бесконечную цепочку

$$O^\infty \subseteq \ldots \subseteq O^{m+1} \subseteq O^m \subseteq \ldots \subseteq O^2 \subseteq T_1.$$

Классы вида O^m и I^m

Мажоритарные функции

- Пусть $m \geqslant 3$. Функция $f(x_1, \ldots, x_m)$ называется **мажоритарной**, если

$$f(y, x, \ldots, x) = f(x, y, x, \ldots, x) = \ldots = f(x, \ldots, x, y) = x.$$

- В частности, для мажоритарной функции верно $f(x, \ldots, x) = x$.
- Пусть $f \in P_2$, f — мажоритарная функция. Тогда
  - На нулевом наборе f равна 0.
  - На всех наборах с ровно одной единицей f равна 0.
  - На всех наборах с ровно одним нулём f равна 1.
  - На единичном наборе f равна 1.
  - На остальных наборах значение f может быть произвольным.

Классы вида O^m и I^m

Функции d_m

- Пусть $m \geqslant 2$. Обозначим

$$d_m(x_1, \ldots, x_m) = \bigvee_{1 \leqslant i < j \leqslant m} x_i x_j.$$

- Видно, что d_m равна 1 на наборах с 2 и более единицами, а на наборах из всех нулей или с одной единицей она равна 0.
- d_m не меняется при перестановке переменных, $d_m(x, \ldots, x) = x$.
- При $m \geqslant 3$ функция d_m является мажоритарной.
- $d_2(x, y) = xy,\ d_3(x, y, z) = \mathrm{m}(x, y, z)$.
- $d_2 \in T_1 \setminus O^2, \quad d_m \in O^{m-1} \setminus O^m,\ m \geqslant 3$.
- Поэтому в бесконечной цепочке все классы различны:

$$O^\infty \subset \ldots \subset O^{m+1} \subset O^m \subset \ldots \subset O^2 \subset T_1.$$

Классы вида O^m и I^m

Классы I^m

- Пусть $m \geqslant 2$. I^m — класс функций, любые m (или менее) единичных наборов которых имеют общую единичную компоненту.

$$I^m = \{f \in P_2 \colon (\forall \alpha^1 \dots, \alpha^m)((f(\alpha^1) = \dots = f(\alpha^m) = 1) \\ \to (\exists i)(\alpha_i^1 = \dots = \alpha_i^m = 1))\}.$$

- Можно заметить, что $I^m = (O^m)^*$. Поэтому класс I^m замкнут.
- По принципу двойственности $I^\infty \subseteq I^m \subseteq T_0$ и $I^{m+1} \subseteq I^m$ при $m \geqslant 2$. Кроме того, все эти классы различны.
- Получаем бесконечную цепочку различных классов:

$$I^\infty \subset \dots \subset I^{m+1} \subset I^m \subset \dots \subset I^2 \subset T_0.$$

Классы вида O^m и I^m

Функции d_m^*

- Пусть $m \geqslant 2$. Тогда по принципу двойственности

$$d_m^*(x_1, \dots, x_m) = \mathop{\&}_{1 \leqslant i < j \leqslant m} (x_i \vee x_j).$$

- Видно, что d_m^* равна 0 на наборах с 2 и более нулями, а на наборах из всех единиц или с одним нулём она равна 1.
- d_m^* не меняется при перестановке переменных, $d_m^*(x, \dots, x) = x$.
- При $m \geqslant 3$ функция d_m^* является мажоритарной.
- $d_2^*(x, y) = x \vee y$, $d_3^*(x, y, z) = \mathrm{m}(x, y, z)$.
- $d_2^* \in T_0 \setminus I^2$, $\quad d_m^* \in I^{m-1} \setminus I^m$, $m \geqslant 3$.

Классы вида O^m и I^m

Производные классы от O^m и I^m

- O^m, $\quad I^m$.
- $O_0^m = O^m \cap T_0$, $\quad I_1^m = I^m \cap T_1$.
- $MO^m = M \cap O^m$, $\quad MI^m = M \cap I^m$.
- $MO_0^m = M \cap O_0^m = MO^m \setminus \{1\}_c$, $\quad MI_1^m = M \cap I_1^m = MI^m \setminus \{0\}_c$.

Двойственность классов вида O^m и I^m

- $O^m = (I^m)^*$.
- $O_0^m = (I_1^m)^*$.
- $MO^m = (MI^m)^*$.
- $MO_0^m = (MI_1^m)^*$.

Классы вида O^m и I^m

Значение $z(f)$

- Пусть $f \in P_2$. Значение $z(f)$ равно числу элементов в наименьшем непустом множестве наборов, на которых функция f обращается в нуль и которые не имеют общей нулевой компоненты.
- $z(f)$ определяет положение функции f в бесконечной цепочке $O^\infty \subseteq \ldots \subseteq O^{m+1} \subseteq O^m \subseteq \ldots \subseteq O^2 \subseteq T_1 \subseteq P_2$.
- Если $z(f)$ не определено, то $f \in O^\infty$.
  $z(f) = m \geqslant 3$ значит $f \in O^{m-1} \setminus O^m$.
  $z(f) = 2$ значит $f \in T_1 \setminus O^2$.
  $z(f) = 1$ значит $f \notin T_1$.
- $z(d_m) = m,\ m \geqslant 2$.

Классы вида O^m и I^m

Лемма

Пусть $f \in T_1 \setminus O^\infty$. *Тогда* $d_{z(f)} \in [x \vee y,\ f]$.

Доказательство

- Так как $f \notin O^\infty$ и $f \neq 0$ (т. к. $f \in T_1$), по следствию из леммы о функции из $O^\infty \setminus D$ множеству $[x \vee y,\ f]$ принадлежит хотя бы одна из функций $x \vee \overline{y}$, $x \vee y\overline{z}$, $x \vee yz$. Тогда $x \vee yz \in [x \vee y,\ f]$ и $MO_0^\infty \subseteq [x \vee y,\ f]$.
- Поскольку $f \notin O^\infty$, значение $z(f)$ определено. Поскольку $f \in T_1$, верно $z(f) \geqslant 2$.
- Поскольку $f \notin O^\infty$, для любого i найдётся набор $\alpha \in E_2^n$ такой, что $f(\alpha) = 0$ и в i-й координате набора α стоит единица.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть $\{a^i = (a^i_1, \ldots, a^i_n),\ i = \overline{1,m}\}$ — наименьшее по мощности множество наборов таких, что $f(a^1) = \ldots = f(a^m) = 0$ и для любого j во множестве есть набор с единицей в j-й координате.
- Это наименьшее множество нулей f без общей нулевой компоненты, поэтому $m = z(f)$. Ясно, что $m \leqslant n$.
- Запишем матрицу:

$$A = \begin{pmatrix} a^1_1 & a^1_2 & \ldots & a^1_n \\ a^2_1 & a^2_2 & \ldots & a^2_n \\ \vdots & \vdots & \ddots & \vdots \\ a^m_1 & a^m_2 & \ldots & a^m_n \end{pmatrix}$$

- В каждом столбце матрицы A есть единица, но при удалении любой строки появится нулевой столбец.

Классы вида O^m и I^m

Доказательство (продолжение)

- Переставив столбцы в матрице A, можно получить матрицу $B = (b_j^i) \in \{0,1\}^{m\times n}$:

$$B = \begin{pmatrix} 1 & 0 & \dots & 0 & b_{m+1}^1 & \dots & b_n^1 \\ 0 & 1 & \dots & 0 & b_{m+1}^2 & \dots & b_n^2 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 & b_{m+1}^m & \dots & b_n^m \end{pmatrix}$$

- Пусть $g(x_1,\dots,x_n)$ получается из $f(x_1,\dots,x_n)$ перестановкой переменных, соответствующей произведённой перестановке столбцов. Тогда $g(b_1^i,\dots,b_n^i) = 0,\ i = \overline{1,m}$.
- Построим функцию $h(x_1,\dots,x_m)$, равную нулю на всех наборах с ровно одной единицей. Если $m = n$, то $h = g$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть $m < n$. При $k = \overline{1,\, n-m}$ обозначим $h_{m+k}(x_1, \ldots, x_m) = b^1_{m+k} x_1 \vee \ldots \vee b^m_{m+k} x_m$. Поскольку в каждом столбце B есть хотя бы одна единица, $h_{m+k} \in [x \vee y]$.
- Выберем

$$h(x_1, \ldots, x_m) = g(x_1, \ldots, x_m, h_{m+1}(x_1, \ldots, x_m), \ldots, h_n(x_1, \ldots, x_m)).$$

- При $i = \overline{1, m}$ пусть $\alpha^i = (0, \ldots, 0, 1, 0, \ldots, 0)$, причём единица стоит на i-й позиции. Тогда $h_{m+k}(\alpha^i) = b^i_{m+k}$.
- Тогда $h(\alpha^i) = g(\alpha^i, b^i_{m+1}, \ldots, b^i_n) = g(b^i_1, \ldots, b^i_n) = 0,\ i = \overline{1, m}$.
- Таким образом, в любом случае построили функцию $h(x_1, \ldots, x_m)$, равную нулю на наборах с одной единицей.

Классы вида O^m и I^m

Доказательство (продолжение)

- $y \vee d_m(x_1, \ldots, x_m) \in MO_0^\infty \subseteq [x \vee y,\ f]$.
- Тогда $h_1(x_1, \ldots, x_m) = h(x_1, \ldots, x_m) \vee d_m(x_1, \ldots, x_m) \in [x \vee y,\ f]$.
- Если $h(0, \ldots, 0) = 0$, то
  $d_m(x_1, \ldots, x_m) = h_1(x_1, \ldots, x_m) \in [x \vee y,\ f]$.
- Пусть $h(0, \ldots, 0) = 1$. Тогда функция $h_1(x_1, \ldots, x_m)$ отличается от d_m только в точке $(0, \ldots, 0)$.
- Покажем, что
  $h_1(x_1 \vee h_1(x_1, \ldots, x_m),\ x_2, \ldots, x_m) = d_m(x_1, \ldots, x_m)$.
- При $x_1 = 1$ это верно, поскольку h_1 и d_m отличаются только на нулевом наборе.
- При $x_1 = 0$ достаточно проверить случаи: среди $x_2, \ldots, x_n$ имеется 0, 1 или $\geqslant 2$ единиц.

$\square$

Лекция 6
Лемма о получении $f \in T_1 \setminus O^\infty$ из d_m. Базисы классов вида O^m, I^m. Лемма о функциях из $T_1 \setminus S$ и $T_1 \setminus L$

Классы вида O^m и I^m

Лемма

Пусть $f \in T_1 \setminus O^\infty$. *Тогда* $f \in [x \vee \overline{y},\, d_{z(f)}]$. *Если дополнительно* $f \in T_0$ *или* $f \in M$, *то соответственно* $f \in [x \vee y\overline{z},\, d_{z(f)}]$ *или* $f \in [x \vee yz,\, d_{z(f)}]$.

Доказательство

- Для любого $n \geqslant z(f)$ функция d_n получается из $d_{z(f)}$ с помощью функции $x \vee yz$ (а значит и с помощью $x \vee y\overline{z}$ или $x \vee \overline{y}$).
- Ясно, что f не является константой и что $z(f) \geqslant 2$. Легко видеть, что $M_{01} = [x \vee yz,\, xy]$.
- Пусть $z(f) = 2$. Тогда $d_{z(f)}(x, y) = xy$ и $f \in T_1 = [x \vee \overline{y},\, xy]$. Если дополнительно $f \in T_0$, то $f \in T_{01} = [x \vee y\overline{z},\, xy]$. Если же $f \in M$, то $f \in M_{01} = [x \vee yz,\, xy]$.
- Пусть $z(f) = t \geqslant 3$ и $\{a^1, \ldots, a^t\}$ — наименьшее по мощности множество наборов, на которых функция f принимает значение 0 и которые не имеют общей нулевой компоненты.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть $f \in M$, тогда $f \in M_{01}$. Верхний нуль f — это такой набор a, что $f(a) = 0$ и для любого $b \geqslant a$, $b \neq a$ верно $f(b) = 1$.
- Считаем все наборы $a^1, \ldots, a^t$ верхними нулями f (в противном случае заменим их на строго большие наборы, являющиеся верхними нулями f, без потери того, что $f(a^1) = \ldots = f(a^t) = 0$ и что эти наборы не имеют общей нулевой компоненты).
- Обозначим через f_i функцию, равную 1 на наборе a^i и совпадающую с f на всех остальных наборах. Поскольку $f \in M_{01}$, а в f_i верхний ноль f заменён на единицу, $f_i \in M_1$. Поскольку у f есть хотя бы $t \geqslant 2$ нулевых набора, нулевой набор не является верхним нулём и $f_i \in M_{01}$.
- Из свойства мажоритарности $d_{z(f)}$ следует

$$f(x_1, \ldots, x_n) = d_{z(f)}(f_1(x_1, \ldots, x_n), \ldots, f_t(x_1, \ldots, x_n)).$$

Классы вида O^m и I^m

Доказательство (продолжение)

- Если $f_i \in O^\infty$, то $f_i \in MO_0^\infty = [x \vee yz]$.
- Пусть $f_i \notin O^\infty$, то есть $z(f_i)$ определено. Поскольку в f_i по сравнению с f исчез один нулевой набор, то в нём не могло появиться новых, меньших по мощности, множеств нулевых наборов, не имеющих общей нулевой компоненты. Это значит, что размер наименьшего множества нулевых наборов, не имеющих общей нулевой компоненты не уменьшился, то есть $z(f_i) \geqslant z(f)$.
- Итак, f строится с помощью $d_{z(f)}$ и f_i, где каждая f_i либо входит в $[x \vee yz]$, либо принадлежит $T_1 \setminus O^\infty$, принадлежит M_{01} и имеет $z(f_i) \geqslant z(f) \geqslant 3$.
- Применяем к каждой f_i ту же операцию, что и к f, продолжая процесс рекурсивно. Таким образом мы будем строить формулу над d_n, $n \geqslant z(f)$ и над $x \vee yz$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Поскольку на каждом шаге число нулей у очередной функции f_i уменьшается, в конце концов оно станет меньше $z(f)$, а значит случай $f_i \notin O^\infty$ окажется невозможен. Поэтому процесс построения закончится не позже, чем через 2^n шагов.
- Поскольку d_n при $n \geqslant z(f)$ выражается с помощью $d_{z(f)}$ и $x \vee yz$, в результате получится формула для f, включающая в себя только функции $d_{z(f)}$ и $x \vee yz$. То есть $f \in [x \vee yz, d_{z(f)}]$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть теперь $f \in T_0$, то есть $f \in T_{01}$. Строим формулу для f так же, как и в случае $f \in M$.
- Поскольку каждая функция f_i получается из предыдущей заменой верхнего нуля (при этом не единственного) на единицу, значение функции на нулевом или единичном наборе заменено быть не может, то есть $f_i \in T_{01}$.
- Если $f_i \in O^\infty$, то $f_i \in O_0^\infty = [x \vee y\overline{z}]$. Иначе $f_i \in T_{01} \setminus O^\infty$ и построение формулы продолжается с помощью функции d_n, $n \geqslant z(f)$, которую можно получить из $d_{z(f)}$ и $x \vee y\overline{z}$.
- Таким образом, в данном случае получится формула над $x \vee y\overline{z},\ d_{z(f)}$. То есть $f \in [x \vee y\overline{z},\ d_{z(f)}]$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть теперь на $f \in T_1$ без дополнительных ограничений. Строим формулу для f так же, как и в случае $f \in M$.
- Поскольку каждая функция f_i получается из предыдущей заменой нуля на единицу, значение функции на единичном наборе заменено быть не может, то есть $f_i \in T_1$.
- Если $f_i \in O^\infty$, то $f_i \in [x \vee \overline{y}]$. Иначе $f_i \in T_1 \setminus O^\infty$ и построение формулы продолжается с помощью функции d_n, $n \geqslant z(f)$, которую можно получить из $d_{z(f)}$ и $x \vee \overline{y}$.
- Таким образом, в данном случае получится формула над $x \vee \overline{y},\ d_{z(f)}$. То есть $f \in [x \vee \overline{y}, d_{z(f)}]$.

$\square$

Классы вида O^m и I^m

Лемма

Имеют место соотношения (*указаны базисы классов*)

$$O^m = [x \vee \overline{y},\, d_{m+1}],\ O_0^m = [x \vee y\overline{z},\, d_{m+1}],\ MO^m = [1,\, d_{m+1}],\ m \geqslant 2;$$
$$MO_0^2 = [x \vee y,\, \mathrm{m}(x, y, z)], \quad MO_0^m = [d_{m+1}],\ m \geqslant 3;$$
$$I^m = [x\overline{y},\, d_{m+1}^*],\ I_1^m = [x(y \vee \overline{z}),\, d_{m+1}^*],\ MI^m = [0,\, d_{m+1}^*],\ m \geqslant 2;$$
$$MI_1^2 = [xy,\, \mathrm{m}(x, y, z)], \quad MI_0^m = [d_{m+1}^*],\ m \geqslant 3.$$

Доказательство

- Пусть $f \in O^m$, $m \geqslant 2$. Тогда $f \in T_1$ и либо $f \in O^\infty$, либо $z(f) \geqslant m + 1$. Поскольку $O^\infty = [x \vee \overline{y}]$, а $d_{z(f)}$ получается из d_{m+1} с помощью $x \vee \overline{y}$, с учётом предыдущей леммы $f \in [x \vee \overline{y},\, d_{m+1}]$. То есть $O^m = [x \vee \overline{y},\, d_{m+1}]$. Очевидно, это базис.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть $f \in O_0^m,\ m \geqslant 2$. Тогда $f \in T_{01}$ и либо $f \in O_0^\infty$, либо $z(f) \geqslant m+1$. Поскольку $O_0^\infty = [x \vee y\overline{z}]$, а $d_{z(f)}$ получается из d_{m+1} с помощью $x \vee y\overline{z}$, с учётом предыдущей леммы $f \in [x \vee y\overline{z},\ d_{m+1}]$. $O_0^m = [x \vee y\overline{z},\ d_{m+1}]$. Очевидно, это базис.
- Пусть $f \in MO^m,\ m \geqslant 2$. Тогда $f \in M_1$ и либо $f \in MO^\infty$, либо $z(f) \geqslant m+1$. Поскольку $MO^\infty = [1,\ x \vee yz]$, а $d_{z(f)}$ получается из d_{m+1} с помощью $x \vee yz$, с учётом предыдущей леммы $f \in [1,\ x \vee yz,\ d_{m+1}]$.
- Заметим, что $x \vee y = d_{m+1}(1, x, y, \ldots, y)$.
  Далее $x \vee yz = x \vee d_{m+1}(x, \ldots, x, y, z)$. Поэтому $f \in [1,\ d_{m+1}]$.
  $MO^m = [1,\ d_{m+1}]$. Очевидно, это базис.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть $f \in MO_0^m$, $m \geqslant 2$. Тогда $f \in M_{01}$ и либо $f \in MO_0^\infty$, либо $z(f) \geqslant m+1$. Поскольку $MO_0^\infty = [x \vee yz]$, а $d_{z(f)}$ получается из d_{m+1} с помощью $x \vee yz$, с учётом предыдущей леммы $f \in [x \vee yz,\ d_{m+1}]$.
- Пусть $m \geqslant 3$. Напомним, что

$$d_{m+1} = \bigvee_{1 \leqslant i < j \leqslant m+1} x_i x_j.$$

Имеем $x \vee yz = d_{m+1}(y, z, x, \ldots, x)$ (переменная x подставлена не менее двух раз). Таким образом, $MO_0^m = [d_{m+1}]$. Ясно, что это базис.
- Пусть $m = 2$. Тогда $f \in [x \vee yz,\ \mathrm{m}(x,y,z)]$. $x \vee \mathrm{m}(x,y,z) = x \vee yz$, поэтому $f \in [x \vee y,\ \mathrm{m}(x,y,z)]$. То есть, $MO_0^2 = [x \vee y,\ \mathrm{m}(x,y,z)]$. Очевидно, что это базис.

Классы вида O^m и I^m

Доказательство (продолжение)

- Базисы классов I^m, I_0^m, MI^m, MI_0^m получаются по принципу двойственности. Отметим только, что $d_3(x, y, z) = d_3^*(x, y, z) = \mathrm{m}(x, y, z)$.

$\square$

Лемма о функциях из $T_1 \setminus S$ и $T_1 \setminus L$

Лемма

Пусть $f_1 \in T_1 \setminus S$, $f_2 \in T_1 \setminus L$. *Тогда множество* $[f_1, f_2]$ *содержит хотя бы одну из функций* $x \vee y$, xy.

Доказательство

- Так как $f_1 \notin S$, по лемме о несамодвойственной функции подстановками $x, \overline{x}$ из неё можно получить константу.
- Вместо $\overline{x}$ будем подставлять y. Получим $g_1(x, y) \in T_1 \setminus S$ такую, что $g_1(0, 1) = g_1(1, 0)$. Ясно, что $g_1(1, 1) = 1$.
- Возможные варианты g_1: xy, $x \vee y$, $x \oplus y \oplus 1$, 1. В первых двух случаях получена нужная функция.
- Иначе получаем 1 $(x \oplus x \oplus 1 = 1)$ и будем анализировать f_2.

Лемма о функциях из $T_1 \setminus S$ и $T_1 \setminus L$

Доказательство (продолжение)

- $f_2 \notin L$, поэтому $f_2^* \notin L$.
- По лемме о нелинейной функции подстановкой в f_2^* функций $0, x, y$ получаем нелинейную функцию $g_2'(x, y)$.
- По принципу двойственности функция $g_2(x, y) = (g_2'(x, y))^*$ получается из f_2 подстановкой функций $1, x, y$.
- Поскольку $g_2' \notin L$, верно $g_2 \notin L$. Поскольку $f_2, 1 \in T_1$, верно $g_2(1, 1) = 1$.
- Возможные варианты g_2: xy, $x \vee y$, $\overline{x} \vee y$, $x \vee \overline{y}$.
- $x \vee y = x \vee \overline{(x \vee \overline{y})}$, поэтому в любом случае получаем требуемую функцию.

$\square$

Лекция 7
Классы, содержащиеся в T_1 (T_0). Перечисление всех замкнутых классов алгебры логики. Функции k-значной логики

Классы вида O^m и I^m

Теорема

Произвольный замкнутый класс, целиком лежащий в классе T_1 и не содержащийся в классах $S, L, O^\infty, I^\infty, K$, совпадает с одним из следующих классов (указаны базисы классов):

$$T_1 = [x \vee \overline{y},\ xy], \quad T_{01} = [x \vee y\overline{z},\ xy],$$
$$M_1 = [1,\ x \vee y,\ xy], \quad M_{01} = [x \vee y,\ xy];$$
$$O^m = [x \vee \overline{y},\ d_{m+1}],\ O_0^m = [x \vee y\overline{z},\ d_{m+1}],\ MO^m = [1,\ d_{m+1}],\ m \geqslant 2;$$
$$MO_0^2 = [x \vee y,\ \mathrm{m}(x,y,z)], \quad MO_0^m = [d_{m+1}],\ m \geqslant 3;$$
$$I_1^m = [x(y \vee \overline{z}),\ d_{m+1}^*],\ m \geqslant 2;$$
$$MI_1^2 = [xy,\ \mathrm{m}(x,y,z)], \quad MI_1^m = [d_{m+1}^*]\ m \geqslant 3.$$

Классы вида O^m и I^m

Доказательство

- Пусть $F = [F] \subseteq T_1$, $F \nsubseteq S, L, O^\infty, I^\infty, K$. По лемме о функциях из $T_1 \setminus S$ и $T_1 \setminus L$ классу F принадлежит одна из фунций $x \vee y$, xy.
- Пусть $x \vee y \in F$. Выберем $f \in F \setminus O^\infty$. По лемме о функции из $T_1 \setminus O^\infty$ класс $[f,\, x \vee y]$ содержит функцию $d_{z(f)}$, где $z(f) \geqslant 2$. Выберем наименьшее такое $z(f)$ и обозначим его $m+1$.
- $y \vee d_{m+1}(x_1, \ldots, x_{m+1}) \in F$. Подставляя y вместо всех переменных x_i, кроме двух, получаем $x \vee yz \in F$, то есть $MO_0^\infty \subseteq F$.
- Обозначим $F^\infty = F \cap O^\infty$. Ясно, что $F^\infty \in \{O^\infty, O_0^\infty, MO^\infty, MO_0^\infty\}$.
- Пусть $m = 1$. Тогда $xy \in F$, то есть $M_{01} = [x \vee y,\, xy] \subseteq F$. Если $F^\infty = O^\infty$, то $x \vee \overline{y} \in F$. Тогда $T_1 = [x \vee \overline{y},\, xy] \subseteq F$, то есть $F = T_1$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Если $F^\infty = O_0^\infty$, то $F \subseteq T_0$ (иначе, т. к. $F \subseteq T_1$, для $f \in F \setminus T_0$ верно $f(x,\dots,x) = 1 \in F^\infty \setminus O_0^\infty$).
  Но тогда $T_{01} = [x \vee y\overline{z},\, xy] \subseteq F$, то есть $F = T_{01}$.
- Если $F^\infty \in \{MO^\infty, MO_0^\infty\}$, то $F \subseteq M$ (иначе для $f \in F \setminus M$ верно $y \vee f(x_1,\dots,x_n) \in F^\infty \setminus MO^\infty$). Тогда $M_{01} \subseteq F \subseteq M_1$.
  Так как $M_1 = M_{01} \cup \{1\}_c$, верно $F \in \{M_{01}, M_1\}$.
- Пусть $m \geqslant 2$. Любая функция $f \in F$ имеет $z(f) \geqslant m+1$ (если определено) и по одной из прошлых лемм принадлежит $[x \vee \overline{y},\, d_{z(f)}]$ (в т.ч. $[x \vee \overline{y}]$, если $z(f)$ не определено).

Классы вида O^m и I^m

Доказательство (продолжение)

- Поскольку любую функцию d_k при $k \geqslant m+1$ можно получить из d_{m+1} и $x \vee yz$, получаем, что $F \subseteq [x \vee \overline{y},\, d_{m+1}] = O^m$. Поскольку $[x \vee y,\, d_{m+1}] = MO_0^m$, верно $MO_0^m \subseteq F$.
- Если $F^\infty = O^\infty$, то $x \vee \overline{y} \in F$. Тогда $O^m = [x \vee \overline{y},\, d_{m+1}] \subseteq F$, то есть $F = O^m$.
- Если $F^\infty = O_0^\infty$, то $F \subseteq T_0$ (как и раньше). Но $O_0^m = [x \vee y\overline{z},\, d_{m+1}] \subseteq F$, и тогда $F = O_0^m$.
- Если $F^\infty \in \{MO^\infty, MO_0^\infty\}$, то $F \subseteq M$ (как и раньше). Тогда $MO_0^m \subseteq F \subseteq MO^m$. Так как $MO^m = MO_0^m \cup \{1\}_c$, верно $F \in \{MO_0^m, MO^m\}$.
- Итак, в случае $x \vee y \in F$ класс F совпадает с одним из классов $T_1, T_{01}, M_1, M_{01}, O^m, O_0^m, MO^m, MO_0^m,\ m \geqslant 2$. Это соответствует условию теоремы.

Классы вида O^m и I^m

Доказательство (продолжение)

- Пусть теперь $xy \in F$. Пусть $F \subseteq T_0$ (при этом в любом случае $F \subseteq T_1$). Тогда $F^* \subseteq T_{01}$ и $x \vee y \in F^*$. Поскольку $F \nsubseteq I^\infty$, верно $F^* \nsubseteq O^\infty$.
- По проведённым ранее рассуждениям F^* совпадает с одним из классов $T_{01}, M_{01}, O_0^m, MO_0^m,\ m \geqslant 2$. Тогда $F \in \{T_{01}, M_{01}, I_1^m, MI_1^m,\ m \geqslant 2\}$. Это соответствует условию теоремы.
- Пусть теперь $xy \in F$ и $F \nsubseteq T_0$. Поскольку $F \subseteq T_1$, для $f \in F \setminus T_0$ получаем $f(x, \dots, x) = 1 \in F$.
- Рассмотрим класс F^*. Ясно, что $x \vee y \in F^*$ и $F^* \nsubseteq D$. Пусть $f \in F^* \setminus D$. Если $f \in O^\infty$, то по лемме о функции из $O^\infty \setminus D$ верно $x \vee yz \in [f] \subseteq F^*$. Если $f \notin O^\infty$, то (так как $f \neq 0 \in D$) по следствию из той же леммы верно $x \vee yz \in [x \vee y,\ f] \subseteq F^*$.

Классы вида O^m и I^m

Доказательство (продолжение)

- Таким образом, $x \vee yz \in F^*$, значит $x(y \vee z) \in F$. Тогда $x \vee y = 1 \cdot (x \vee y) \in F$.
- Тогда по доказанному ранее F совпадает с одним из классов $T_1, T_{01}, M_1, M_{01}, O^m, O_0^m, MO^m, MO_0^m,\ m \geqslant 2$. Поскольку в этом случае $x \vee y$, xy, $1 \in F$, подходят только варианты T_1 и M_1. Это соответствует условию теоремы.

$\square$

Классы вида O^m и I^m

Теорема

Произвольный замкнутый класс, целиком лежащий в классе T_0 и не содержащийся в классах $S, L, O^\infty, I^\infty, D$, совпадает с одним из следующих классов (указаны базисы классов):

$$T_0 = [x\overline{y},\ x \vee y], \quad T_{01} = [x(y \vee \overline{z}),\ x \vee y],$$
$$M_0 = [0,\ x \vee y,\ xy], \quad M_{01} = [x \vee y,\ xy];$$
$$I^m = [x\overline{y},\ d^*_{m+1}],\ I^m_1 = [x(y \vee \overline{z}),\ d^*_{m+1}],\ MI^m = [0,\ d^*_{m+1}],\ m \geqslant 2;$$
$$MI^2_1 = [xy,\ \mathrm{m}(x, y, z)], \quad MI^m_1 = [d^*_{m+1}],\ m \geqslant 3;$$
$$O^m_0 = [x \vee y\overline{z},\ d_{m+1}],\ m \geqslant 2;$$
$$MO^2_0 = [x \vee y,\ \mathrm{m}(x, y, z)], \quad MO^m_0 = [d_{m+1}]\ m \geqslant 3.$$

Классы вида O^m и I^m

Доказательство

- Отметим, что в этой теореме указывается, что $\{x(y \vee \overline{z}),\ x \vee y\}$ — базис в T_{01}. Это верно, так как $T_{01} = T_{01}^*$ и двойственная к данной система $\{x \vee y\overline{z},\ xy\}$ является базисом в T_{01}.
- Все классы, указанные в утверждении теоремы, двойственны к классам из утверждения предыдущей теоремы.
- Пусть $F \subseteq T_0$ и $F \nsubseteq S, L, O^\infty, I^\infty, K$.
  Тогда $F^* \subseteq T_1$ и $F^* \nsubseteq S, L, O^\infty, I^\infty, D$.
- По предыдущей теореме
  $F^* \in \{T_1, T_{01}, M_1, M_{01}, O^m, O_0^m, MO^m, MO_0^m, I_1^m, MI_1^m,\ m \geqslant 2\}$.
- Тогда по принципу двойственности
  $F \in \{T_0, T_{01}, M_0, M_{01}, I^m, I_1^m, MI^m, MI_1^m, O_0^m, MO_0^m,\ m \geqslant 2\}$.
  Это удовлетворяет условию теоремы.

$\square$

Класс M

Теорема

Произвольный замкнутый класс, целиком лежащий в классе M и не содержащийся в T_0, T_1, D, K, совпадает с классом (указан базис)

$$M = [0,\ 1,\ xy,\ x \vee y].$$

Доказательство

- Пусть $F \subseteq M$ и $F \nsubseteq T_0, T_1, D, K$. Так как $M \setminus T_0 = \{1\}_c$ и $M \setminus T_1 = \{0\}_c$, верно $0, 1 \in F$.
- Пусть $f \in F \setminus D$. Так как $f \in M$, у f есть ДНФ без отрицаний. Выберем такую ДНФ, в которой нельзя применить ни одну операцию поглощения $A \vee AB = A$.
- Поскольку $f \notin D$, в ДНФ есть слагаемые с более, чем одной буквой. Выберем неоднобуквенное слагаемое K с минимальным числом букв. Считаем, что $K = x_1 \dots x_l$.

Класс M

Доказательство (продолжение)

- Поскольку в ДНФ нет поглощений, никакие однобуквенные слагаемые в ДНФ не являются переменными, входящими в K.
- Подставим нули во все переменные, кроме переменных K. Получим $x_1 \dots x_l$. Отождествлением переменных получаем $xy \in [0,\ f] \subseteq F$.
- Пусть теперь $f \in F \setminus K$. Тогда $f^* \notin D$. По доказанному выше xy реализуется формулой $\Phi(0, f^*)$. Тогда $x \vee y$ реализуется формулой $\Phi(1, f)$, то есть $x \vee y \in F$.
- Тогда $M = [0,\ 1,\ xy,\ x \vee y] \subseteq F$. Значит, $F = M$.

$\square$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе U, совпадает с одним из следующих классов (указаны базисы классов):

$$U = [0, \overline{x}],\ U_0 = [0, x],\ U_1 = [1, x],\ MU = [0, 1, x],\ SU = [\overline{x}],$$
$$U_{01} = [x], \quad C = [0, 1], \quad C_0 = [0], \quad C_1 = [1].$$

Теорема

Произвольный замкнутый класс, целиком лежащий в одном из классов D, K и не содержащийся в классе U, совпадает с одним из следующих классов (указаны базисы классов):

$$D = [0,\ 1,\ x \vee y],\ D_0 = [0,\ x \vee y],\ D_1 = [1,\ x \vee y],\ D_{01} = [x \vee y],$$
$$K = [0,\ 1,\ xy], \quad K_0 = [0,\ xy], \quad K_1 = [1,\ xy], \quad K_{01} = [xy].$$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе L и не содержащийся в классе U, совпадает с одним из следующих классов (указаны базисы классов):

$$L = [1,\, x \oplus y], \quad L_0 = [x \oplus y], \quad L_1 = [x \oplus y \oplus 1],$$
$$SL = [x \oplus y \oplus z \oplus 1], \quad L_{01} = [x \oplus y \oplus z].$$

Теорема

Произвольный замкнутый класс, целиком лежащий в классе S и не содержащийся в L, совпадает с одним из классов (указаны базисы)

$$S = [\mathrm{m}(x, y, z),\ \overline{x}], \quad S_{01} = [\mathrm{m}(x, y, \overline{z})], \quad SM = [\mathrm{m}(x, y, z)].$$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе O^∞ и не содержащийся в D, совпадает с одним из классов (указаны базисы)

$$O^\infty = [x \vee \overline{y}],\ O_0^\infty = [x \vee y\overline{z}],\ MO^\infty = [1,\, x \vee yz],\ MO_0^\infty = [x \vee yz].$$

Произвольный замкнутый класс, целиком лежащий в классе I^∞ и не содержащийся в K, совпадает с одним из классов (указаны базисы)

$$I^\infty = [x\overline{y}],\ I_1^\infty = [x(y \vee \overline{z})],\ MI^\infty = [0,\, x(y \vee z)],\ MI_1^\infty = [x(y \vee z)].$$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе T_1 и не содержащийся в классах $S, L, O^\infty, I^\infty, K$, совпадает с одним из следующих классов (указаны базисы классов):

$$T_1 = [x \vee \overline{y},\, xy], \quad T_{01} = [x \vee y\overline{z},\, xy],$$
$$M_1 = [1,\, x \vee y,\, xy], \quad M_{01} = [x \vee y,\, xy];$$
$$O^m = [x \vee \overline{y},\, d_{m+1}],\ O_0^m = [x \vee y\overline{z},\, d_{m+1}],\ MO^m = [1,\, d_{m+1}],\ m \geqslant 2;$$
$$MO_0^2 = [x \vee y,\, \mathrm{m}(x, y, z)], \quad MO_0^m = [d_{m+1}],\ m \geqslant 3;$$
$$I_1^m = [x(y \vee \overline{z}),\, d^*_{m+1}],\ m \geqslant 2;$$
$$MI_1^2 = [xy,\, \mathrm{m}(x, y, z)], \quad MI_1^m = [d^*_{m+1}]\ m \geqslant 3.$$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе T_0 и не содержащийся в классах $S, L, O^\infty, I^\infty, D$, совпадает с одним из следующих классов (указаны базисы классов):

$$T_0 = [x\overline{y},\, x \vee y], \quad T_{01} = [x(y \vee \overline{z}),\, x \vee y],$$
$$M_0 = [0,\, x \vee y,\, xy], \quad M_{01} = [x \vee y,\, xy];$$
$$I^m = [x\overline{y},\, d^*_{m+1}],\ I^m_1 = [x(y \vee \overline{z}),\, d^*_{m+1}],\ MI^m = [0,\, d^*_{m+1}],\ m \geqslant 2;$$
$$MI^2_1 = [xy,\, \mathrm{m}(x,y,z)], \quad MI^m_1 = [d^*_{m+1}],\ m \geqslant 3;$$
$$O^m_0 = [x \vee y\overline{z},\, d_{m+1}],\ m \geqslant 2;$$
$$MO^2_0 = [x \vee y,\, \mathrm{m}(x,y,z)], \quad MO^m_0 = [d_{m+1}]\ m \geqslant 3.$$

Все теоремы о замкнутых классах

Теорема

Произвольный замкнутый класс, целиком лежащий в классе M и не содержащийся в T_0, T_1, D, K, совпадает с классом (указан базис)

$$M = [0,\ 1,\ xy,\ x \vee y].$$

Теорема (Пост)

Произвольный замкнутый класс, не содержащийся в T_0, T_1, S, L, M, совпадает с классом (указан базис)

$$P_2 = [\overline{x},\ xy].$$

Все теоремы о замкнутых классах

Теорема (Пост)

Совокупность всех замкнутых классов булевых функций счётна и состоит из следующих классов.

1. *Классы, содержащие константы* 0 *и* 1:

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

2. *Классы, содержащие* 0 *и не содержащие* 1:

$$L_0,\ M_0,\ T_0,\ D_0,\ K_0,\ U_0,\ C_0,\ I^m,\ MI^m,\ m = 2, 3, \ldots, \infty.$$

3. *Классы, содержащие* 1 *и не содержащие* 0:

$$L_1,\ M_1,\ T_1,\ D_1,\ K_1,\ U_1,\ C_1,\ O^m,\ MO^m,\ m = 2, 3, \ldots, \infty.$$

(*Продолжение списка на следующем слайде*)

Все теоремы о замкнутых классах

Теорема (Пост, продолжение)

4. *Классы, не содержащие* 0 *и* 1*:*

$$L_{01},\ M_{01},\ S_{01},\ T_{01},\ D_{01},\ K_{01},\ U_{01},\ S,\ SL,\ SM,\ SU,$$
$$I_1^m,\ MI_1^m,\ O_0^m,\ MO_0^m,\quad m = 2, 3, \ldots, \infty.$$

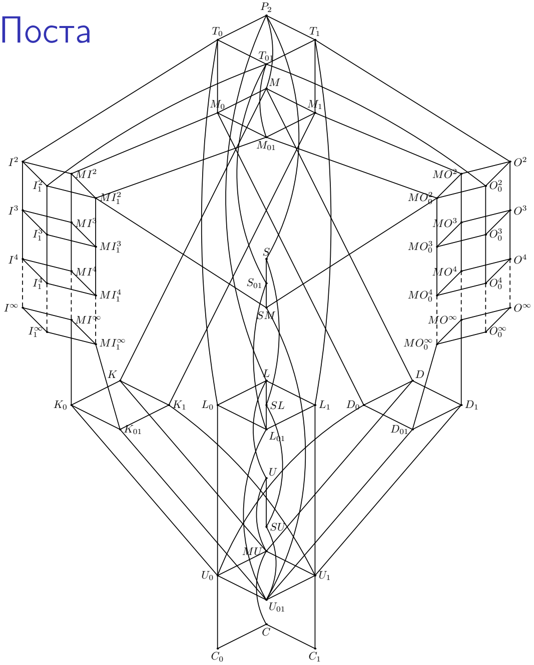
Каждый из перечисленных замкнутых классов порождается конечной системой своих функций.

Доказательство

- Все замкнутые классы и их базисы перечислены в указанных выше теоремах. Совокупность этих теорем доказывает, что других замкнутых классов в P_2 нет.

□

Диаграмма Поста



Функции k-значной логики

Определение

$E_k = \{0,\, 1,\, \ldots,\, k-1\}$. Функция k-значной логики — это функция вида

$$f\colon E_k^n \to E_k.$$

P_k — множество всех функций k-значной логики при фиксированом k.

Примеры функций

- Константы: $0,\, \ldots,\, k-1$.
- Сложение $x+y$ и умножение xy по модулю k.
- $\min(x,y)$, $\max(x,y)$.
- $J_\sigma(x) = \begin{cases} k-1, & x=\sigma, \\ 0, & \text{иначе,} \end{cases} \qquad j_\sigma(x) = \begin{cases} 1, & x=\sigma, \\ 0, & \text{иначе,} \end{cases}$
  $(\sigma \in \{0,\ldots,k-1\})$.

Функции k-значной логики

Примеры функций

- Отрицание Поста: $\overline{x} = x + 1$.
- Отрицание Лукасевича: $\sim x = (k-1) - x$.
- $-x = (k-1) \cdot x = \begin{cases} 0, & x = 0, \\ k - x, & \text{иначе.} \end{cases}$
- Усечённая разность: $x \dot{-} y = \begin{cases} x - y, & x \geqslant y, \\ 0, & x < y. \end{cases}$
- Импликация: $x \supset y = \sim(x \dot{-} y) = \begin{cases} k-1, & x < y, \\ (k-1) - (x - y), & x \geqslant y. \end{cases}$

Функции k-значной логики

Теорема (о первой форме)

Для любой функции $f\colon \{0,\ldots,k-1\}^n \to \{0,\ldots,k-1\}$ *верно*

$$f(\tilde{x}^n) = \max_{\sigma_1,\ldots,\sigma_n \in \{0,\ldots,k-1\}} \min(J_{\sigma_1}(x_1),\ldots,J_{\sigma_n}(x_n), f(\sigma_1,\ldots,\sigma_n)).$$

Теорема (о второй форме)

Для любой функции $f\colon \{0,\ldots,k-1\}^n \to \{0,\ldots,k-1\}$ *верно*

$$f(\tilde{x}^n) = \sum_{\sigma_1,\ldots,\sigma_n \in \{0,\ldots,k-1\}} j_{\sigma_1}(x_1)\ldots j_{\sigma_n}(x_n) f(\sigma_1,\ldots,\sigma_n).$$

Функции k-значной логики

Теорема (малая теорема Ферма)

Пусть k — простое число и a не делится на k. Тогда

$$a^{k-1} \equiv 1 \pmod{k}.$$

Функции j_σ

- Если k — простое число, то $j_\sigma(x) = j_0(x - \sigma) = 1 - (x - \sigma)^{k-1}$.
- Если k — составное число, то ни одна функция j_σ не представима полиномом по модулю k.

Поиск полиномиального представления при простом k

- Строим вторую форму f;
- Подставляем $j_\sigma(x) = 1 - (x - \sigma)^{k-1}$ и раскрываем скобки;
- Заменяем отрицательные коэффициенты: $-a \equiv k - a \pmod{k}$.

Функции k-значной логики

Утверждение

Система Россера-Туркетта

$$\{0,\ \ldots,\ k-1,\ J_0(x),\ \ldots,\ J_{k-1}(x),\ \max(x,y),\ \min(x,y)\}$$

полна в P_k.

Утверждение

Система

$$\{0,\ \ldots,\ k-1,\ j_0(x),\ \ldots,\ j_{k-1}(x),\ x+y,\ xy\}$$

полна в P_k.

Утверждение

Система $\{0,\ \ldots,\ k-1,\ x+y,\ xy\}$ *полна в* P_k *тогда и только тогда, когда* k *— простое число.*

Функции k-значной логики

Утверждение

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

Доказательство

- Из $\overline{x} = x+1$ получим $x+1,\ x+2,\ \ldots,\ x+k = x$.
- $k-1 = \max(x,\, x+1,\, \ldots,\, x+(k-1))$.
- Константы: $0 = (k-1)+1,\ 1 = 0+1,\ \ldots,\ k-2 = (k-3)+1$.
- $J_0(x) = \max(x,\, x+1,\, \ldots,\, x+(k-2))+1$.
- $J_\sigma(x) = J_0(x+(k-\sigma)),\ \sigma \in \{1, \ldots, k-1\}$.
- Обозначим $g_i(x) = \begin{cases} \sim x = k-1-i, & x = i, \\ 0, & \text{иначе}, \end{cases}\quad i \in \{0, \ldots, k-1\}$.
- $g_i(x) = \max(J_i(x),\, i)+(k-i),\ i \in \{0, \ldots, k-1\}$.
- $\sim x = \max(g_0(x), \ldots, g_{k-1}(x))$.

Функции k-значной логики

Доказательство (продолжение)

- Заметим, что $\sim\sim x = x$.
- Кроме того, $x < y$ тогда и только тогда, когда $\sim x > \sim y$.
- Поэтому $\max(\sim x, \sim y)$ равно $\sim\min(x, y)$.
- То есть $\min(x, y) = \sim\max(\sim x, \sim y)$.
- Мы получили все функции полной в P_k системы Россера-Туркетта. Значит, система $\{\overline{x}, \max(x, y)\}$ полна в P_k.

$\square$

Функции k-значной логики

Определение

Функция Вебба:

$$V_k(x,y) = \max(x,y) + 1\colon\ E_k^2 \to E_k,\ \ k \geqslant 2.$$

Утверждение

Система $\{V_k(x,y)\}$ *полна в* P_k.

Доказательство

- $\overline{x} = \max(x,x) + 1.$
- $\max(x,y) = \max(x,y) + 1 \underbrace{+ 1 + \ldots + 1}_{k-1 \text{ раз}}.$

$\square$

Лекция 8
Алгоритм распознавания полноты в P_k.
Теорема Кузнецова

Алгоритм распознавания полноты в P_k

Теорема (Яблонский)

Существует алгоритм, распознающий полноту конечной системы в P_k (функции на вход алгоритма подаются в виде векторов значений или формул над фиксированной конечной полной системой).

Доказательство

- Пусть $Q = \{f_1, \ldots, f_s\} \subseteq P_k$ и функция f_i зависит от n_i переменных, $i = \overline{1, s}$.
- Пусть $[Q]^{(2)}$ — все функции из $[Q]$ от 2 переменных. Это множество конечно.
- $H_1 = \{f_i(x_{j_1}, \ldots, x_{j_{n_i}}) \mid j_1, \ldots, j_{n_i} \in \{1, 2\},\ i \in \{1, \ldots, s\}\}$.
- Пусть $H_j \subseteq [Q]^{(2)},\ j \geqslant 1$. $H_{j+1} = \{f_i(h_{j_1}(x_1, x_2), \ldots, h_{j_{n_i}}(x_1, x_2)) \mid h_{j_1}, \ldots, h_{j_{n_i}} \in H_j \cup \{I_1^2, I_2^2\},\ i \in \{1, \ldots, s\}\}$.
- Получаем последовательность $H_1 \subseteq H_2 \subseteq \ldots \subseteq [Q]^{(2)}$.

Алгоритм распознавания полноты в P_k

Доказательство (продолжение)

- Очевидно, что H_i — это множество функций, получающихся формулами над Q глубины не более i с подстановкой x_1, x_2 вместо всех переменных. Тогда $\bigcup\limits_{i=1}^{\infty} H_i = [Q]^{(2)}$.
- Поскольку множество $[Q]^{(2)}$ конечно, в какой-то момент окажется $H_r = H_{r+1}$. Тогда $H_r = \bigcup\limits_{i=1}^{\infty} H_i = [Q]^{(2)}$.
- Ясно, что система Q полна тогда и только тогда, когда $V_k \in [Q]^{(2)}$.
- Алгоритм проверки полноты системы:
  - Строим классы функций $H_1, H_2, \ldots$
  - Как только оказалось, что только что построенный класс H_i совпадает с H_{i-1}, останавливаем построение.
  - Если $V_k \in H_i$, выдаём, что система полна.
  - Если $V_k \notin H_i$, выдаём, что система не полна.

$\square$

Теорема Кузнецова о функциональной полноте

Определение

Пусть $F \subseteq P_k$. Тогда $F^{(m)}$ — это множество всех функций из F, зависящих от m переменных.

Определение

- Пусть $H = \{h_1(x_1, \ldots, x_m),\ \ldots,\ h_s(x_1, \ldots, x_m)\} \subseteq P_k$ — конечное множество функций от одного и того же числа переменных, а $f(x_1, \ldots, x_n) \in P_k$.
- f сохраняет множество H, если для любых $i_1, \ldots, i_n \in \{1, \ldots, s\}$ верно $f(h_{i_1}(x_1, \ldots, x_m), \ldots, h_{i_n}(x_1, \ldots, x_m)) \in H$.

Лемма

Пусть F — множество всех функций, сохраняющих множество H. Тогда F — замкнутый класс, содержащий все селекторные функции $I_i^n(x_1, \ldots, x_n) = x_i,\ i = \overline{1, n},\ n \in \mathbb{N}$.

Теорема Кузнецова о функциональной полноте

Доказательство

- Пусть $h_{j_1}, \ldots, h_{j_n} \in H$.
  $I_i^n(h_{j_1}(x_1, \ldots, x_m), \ldots, h_{j_n}(x_1, \ldots, x_m)) = h_{j_i}(x_1, \ldots, x_m) \in H$.
  Поэтому $I_i^n(h_{j_1}(x_1, \ldots, x_m), \ldots, h_{j_n}(x_1, \ldots, x_m))$ сохраняет H и принадлежит F.
- Пусть $f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n), \ldots, f_k(x_1, \ldots, x_n))$, $f_0, \ldots, f_k \in F$.
- Тогда при $i = \overline{1, k}$ для любых $h_{j_1}, \ldots, h_{j_n} \in H$ верно $f_i(h_{j_1}(x_1, \ldots, x_m), \ldots, h_{j_n}(x_1, \ldots, x_m)) = h_{l_i}(x_1, \ldots, x_m) \in H$.
- Тогда $f(h_{j_1}(x_1, \ldots, x_m), \ldots, h_{j_n}(x_1, \ldots, x_m)) = f_0(h_{l_1}(x_1, \ldots, x_m), \ldots, h_{l_k}(x_1, \ldots, x_m)) \in H$, то есть f сохраняет H. Значит, $f \in F$.
- Таким образом, $[F] = F$, то есть класс F замкнут.

$\square$

Теорема Кузнецова о функциональной полноте

Лемма

Пусть $H = [H]^{(m)}$, $I_1^m, \ldots, I_m^m \in H$. *Пусть* F *— множество всех функций, сохраняющих* H. *Тогда* $F^{(m)} = H$.

Доказательство

- Покажем, что $F^{(m)} \subseteq H$.
- Пусть $f(x_1, \ldots, x_m) \in F^{(m)}$.
- f сохраняет H, поэтому $f(x_1, \ldots, x_m) = f(I_1^m(x_1, \ldots, x_m), \ldots, I_m^m(x_1, \ldots, x_m)) \in H$.
- Теперь покажем, что $H \subseteq F^{(m)}$.
- Пусть $f \in H$. Тогда, поскольку $[H]^{(m)} \subseteq H$, верно, что f сохраняет H. Значит, $f \in F^{(m)}$.

□

Теорема Кузнецова о функциональной полноте

Теорема (Кузнецов)

Пусть $k \geqslant 2$. Тогда в P_k существует конечное число предполных классов. При этом любая система $Q \subseteq P_k$ полна в P_k тогда и только тогда, когда Q целиком не содержится ни в одном из предполных классов P_k.

Доказательство

- Рассмотрим все множества $H_1, \ldots, H_t \subseteq P_k^{(2)}$ такие, что
  1. $I_1^2,\ I_2^2 \in H_i$;
  2. $[H_i]^{(2)} = H_i \neq P_k^{(2)}$.
- Такие множества существуют, так как $\{I_1^2, I_2^2\}$ удовлетворяет этому условию. Поскольку $P_k^{(2)}$ конечно, число таких множеств H_i конечно.
- Обозначим через F_i' множество всех функций, сохраняющих $H_i,\ i = \overline{1, t}$.

Теорема Кузнецова о функциональной полноте

Доказательство (продолжение)

- По доказанным выше леммам каждое множество F_i' содержит все селекторные функции, $F_i' = [F_i']$.
  Кроме того, $F_i'^{(2)} = H_i \neq P_k^{(2)}$, поэтому $F_i' \neq P_k$.
- Удалим из набора $F_1', \ldots, F_t'$ дубликаты классов, а также каждый класс, который содержится в каком-либо другом классе этого набора (без дубликатов). Получим набор $F_1, \ldots, F_s,\ s \leqslant t$.
- По построению классы $F_1, \ldots, F_s$ замкнуты, различны, не вложены друг в друга и отличны от P_k.
- Покажем, что для любой системы $Q \subseteq P_k$ верно, что Q полна в P_k тогда и только тогда, когда $Q \not\subseteq F_i,\ i = \overline{1, s}$.
- Пусть Q полна в P_k. Если $Q \subseteq F_i$, то $[Q] \subseteq [F_i] = F_i \neq P_k$, что невозможно. Тогда $Q \not\subseteq F_i,\ i = \overline{1, s}$.

Теорема Кузнецова о функциональной полноте

Доказательство (продолжение)

- Пусть теперь $Q \not\subseteq F_i,\ i = \overline{1, s}$.
- Q полна в P_k тогда и только тогда, когда $Q \cup \{I_1^2, I_2^2\}$ полна в P_k: из любой формулы, построенной с использованием селекторных функций, можно исключить эти селекторные функции, заменив всю функцию на соответствующий аргумент.
- Поэтому нам достаточно доказать полноту $Q' = Q \cup \{I_1^2, I_2^2\}$.
- Предположим, что $[Q']^{(2)} \neq P_k^{(2)}$.
- Тогда множество $[Q']^{(2)}$ обладает свойствами:
    1. $I_1^2, I_2^2 \in [Q']^{(2)}$.
    2. $[[Q']^{(2)}]^{(2)} = [Q']^{(2)} \neq P_k^{(2)}$
- Обоснуем второй пункт. $[[Q']^{(2)}]^{(2)} \supseteq [Q']^{(2)}$, так как при замыкании множество не сужается. С другой стороны, $[[Q']^{(2)}]^{(2)} \subseteq [[Q']]^{(2)} = [Q']^{(2)}$.

Теорема Кузнецова о функциональной полноте

Доказательство (продолжение)

- Таким образом, $[Q']^{(2)} = H_i$, где $i \in \{1, \ldots, s\}$.
- Рассмотрим любую функцию $f \in [Q']$. Очевидно, f сохраняет $[Q']^{(2)} = H_i$, то есть $f \in F_i'$.
- Тогда $Q \subseteq [Q'] \subseteq F_i' \subseteq F_j$ при некотором j. Противоречие исходному предположению о Q.
- Противоречие пошло из предположения, что $P_k^{(2)} \neq [Q']^{(2)}$. Значит, $[Q']^{(2)} = P_k^{(2)}$, то есть $V_k \in [Q']^{(2)}$. Тогда система Q полна.

Теорема Кузнецова о функциональной полноте

Доказательство (продолжение)

- Осталось доказать, что $F_1, \ldots, F_s$ — это и есть все предполные классы в P_k.
- Пусть $f \notin F_i$. Тогда система $F_i \cup \{f\}$ целиком не содержится ни в одном из классов $F_1, \ldots, F_s$, а значит (по доказанному выше), она полна. Это значит, что классы $F_1, \ldots, F_s$ предполные.
- Пусть F — предполный класс, отличный от $F_1, \ldots, F_s$. F не полная система, значит (по доказанному выше) $F \subseteq F_i$ для некоторого i. Значит, F строго вложен в F_i. Но тогда для любой $f \in F_i \setminus F$ верно $[F \cup \{f\}] \subseteq F_i \neq P_k$. Получили противоречие.
- Это значит, что $F_1, \ldots, F_s$ — все предполные классы в P_k.

$\square$

Лекция 9
Критерий Яблонского: вспомогательные леммы и начало доказательства

Критерий Яблонского

Определение

Функция f называется существенной, если она существенно зависит по крайней мере от двух переменных.

Лемма (о трёх наборах)

Пусть $k \geqslant 3$ и $f(x_1, \ldots, x_n)$ — существенная функция с существенной переменной x_1, принимающая не менее 3 значений. Тогда существуют наборы вида

$$(a, a_2, \ldots, a_n),$$
$$(b, a_2, \ldots, a_n),$$
$$(a, c_2, \ldots, c_n),$$

на которых f принимает 3 различных значения.

Критерий Яблонского

Доказательство

- x_1 — существенная переменная, поэтому существуют $a_2, \dots, a_n \in E_k$ такие, что множество $\{f_0, \dots, f_{k-1}\}$, где $f_i = f(i, a_2, \dots, a_n)$, содержит не менее 2 различных значений.
- Пусть $\{f_0, \dots, f_{k-1}\}$ содержит не все значения f.
- Выбираем $a, c_2, \dots, c_n \in E_k$ такие, что $f(a, c_2, \dots, c_n) \notin \{f_0, \dots, f_{k-1}\}$.
- Тогда $f(a, a_2, \dots, a_n) \neq f(a, c_2, \dots, c_n)$.
- В $\{f_0, \dots, f_{k-1}\}$ не менее 2 различных значений. Выбираем b такое, что $f(b, a_2, \dots, a_n) \neq f(a, a_2, \dots, a_n)$.
- Так как $f(a, c_2, \dots, c_n) \notin \{f_0, \dots, f_{k-1}\}$, верно и $f(a, c_2, \dots, c_n) \neq f(b, a_2, \dots, a_n)$.
- Значит, на выбранных наборах f принимает 3 различных значения.

Критерий Яблонского

Доказательство (продолжение)

- Пусть теперь $\{f_0, \ldots, f_{k-1}\}$ содержит все значения f.
- Кроме x_1 у f есть другая существенная переменная. Не ограничивая общности, считаем, что это x_2.
- Тогда существуют значения $a, c_2', \ldots, c_n'$ такие, что $c_2' \neq a_2$ и $f(a, c_2', c_3', \ldots, c_n') \neq f(a, a_2, c_3', \ldots, c_n')$. Хотя бы одно из этих значений не совпадает с $f(a, a_2, \ldots, a_n)$.
- Выберем в качестве $(c_2, \ldots, c_n)$ значения $(c_2', c_3', \ldots, c_n')$ или $(a_2, c_3', \ldots, c_n')$ так, чтобы было $f(a, c_2, \ldots, c_n) \neq f(a, a_2, \ldots, a_n)$.
- Функция f принимает не менее 3 значений и все эти значения есть среди $\{f_0, \ldots, f_{k-1}\}$. Это значит, что существует b такое, что $f(b, a_2, \ldots, a_n)$ отличается от $f(a, a_2, \ldots, a_n)$ и $f(a, c_2, \ldots, c_n)$.
- На выбранных наборах f принимает 3 различных значения.

$\square$

Критерий Яблонского

Следствие (из леммы о трёх наборах)

Пусть $k \geqslant 3$ *и* $f(x_1, \ldots, x_n)$ *— существенная функция, принимающая* $l \geqslant 3$ *значений. Тогда существуют множества* $G_1, \ldots, G_n \subseteq E_k$ *такие, что* $1 \leqslant |G_1|, \ldots, |G_k| \leqslant l - 1$ *и на множестве* $G_1 \times \ldots \times G_n$ *функция* f *принимает все* l *значений.*

Доказательство

- Не ограничивая общности, считаем, что x_1 — существенная переменная.
- По лемме функция принимает 3 различных значения на наборах

$$
\begin{gathered}
(a, a_2, \ldots, a_n),\\
(b, a_2, \ldots, a_n),\\
(a, c_2, \ldots, c_n).
\end{gathered}
$$

Критерий Яблонского

Доказательство (продолжение)

- В каждой координате эти 3 набора содержат только по 2 различных значения.
- Дополняем эти наборы любыми $l-3$ наборами, на которых f принимает остальные значения.
- При $i=\overline{1,n}$ множество G_i — это множество значений, находящихся в i-й координате выбранных наборах. Ясно, что $1 \leqslant |G_i| \leqslant l-1$ и что все выбранные наборы принадлежат $G_1 \times \ldots \times G_n$.
- Таким образом, построенные множества удовлетворяют условию следствия.

□

Критерий Яблонского

Определение

Квадрат — это 4 набора из E_k^n вида

$$
\begin{gathered}
(a_1, \ldots, a_{i-1},\ a,\ a_{i+1}, \ldots, a_{j-1},\ c,\ a_{j+1}, \ldots, a_n),\\
(a_1, \ldots, a_{i-1},\ a,\ a_{i+1}, \ldots, a_{j-1},\ d,\ a_{j+1}, \ldots, a_n),\\
(a_1, \ldots, a_{i-1},\ b,\ a_{i+1}, \ldots, a_{j-1},\ c,\ a_{j+1}, \ldots, a_n),\\
(a_1, \ldots, a_{i-1},\ b,\ a_{i+1}, \ldots, a_{j-1},\ d,\ a_{j+1}, \ldots, a_n),
\end{gathered}
$$

где $a \neq b$, а $c \neq d$.

Лемма (о квадрате)

Пусть $k \geqslant 3$ и $f(x_1, \ldots, x_n)$ — существенная функция, принимающая не менее 3 значений. Тогда существует квадрат, на котором функция принимает не менее 2 значений, причём одно из них лишь в одной из точек квадрата.

Критерий Яблонского

Доказательство

- Не ограничивая общности, считаем, что x_1 — существенная переменная.
- По лемме о трёх наборах функция принимает 3 различных значения на наборах

$$(a, a_2, \ldots, a_n),$$
$$(b, a_2, \ldots, a_n),$$
$$(a, c_2, \ldots, c_n).$$

- Далее через $\tilde{a}_j$ будем обозначать набор $(a_j, \ldots, a_n)$.
- Очевидно, что $(a_2, \ldots, a_n) \neq (c_2, \ldots, c_n)$.
- Пусть i_1 — наименьшее число такое, что $a_{i_1} \neq c_{i_1}$. Не ограничивая общности считаем, что $i_1 = 2$.

Критерий Яблонского

Доказательство (продолжение)

- Рассмотрим квадрат

$$
\begin{aligned}
&(a, a_2, \tilde{a}_3), \quad (a, c_2, \tilde{a}_3),\\
&(b, a_2, \tilde{a}_3), \quad (b, c_2, \tilde{a}_3).
\end{aligned}
$$

- Пусть $A = f(a, a_2, \tilde{a}_3)$, $B = f(b, a_2, \tilde{a}_3)$. В левой части квадрата f принимает различные значения A и B. Если одно из них только в одной точке, то теорема доказана.
- В противном случае $\{f(a, c_2, \tilde{a}_3), f(b, c_2, \tilde{a}_3)\} = \{A, B\}$. Кроме того, $(a, c_2, \tilde{a}_3) \neq (a, c_2, c_3, \ldots, c_n)$ (иначе, так как $f(a, c_2, c_3, \ldots, c_n) \notin \{A, B\}$, в квадрате было бы 3 разных значения f).
- Пусть i_2 — наименьшее число, большее i_1, такое, что $a_{i_2} \neq c_{i_2}$. Не ограничивая общности считаем, что $i_2 = 3$.

Критерий Яблонского

Доказательство (продолжение)

- Рассмотрим квадрат

$$
\begin{array}{cc}
(a, c_2, a_3, \tilde{a}_4), & (a, c_2, c_3, \tilde{a}_4), \\
(b, c_2, a_3, \tilde{a}_4), & (b, c_2, c_3, \tilde{a}_4).
\end{array}
$$

- В левой части квадрата f принимает различные значения A и B. Если одно из них только в одной точке, то теорема доказана.
- В противном случае $\{f(a, c_2, c_3, \tilde{a}_4),\ f(b, c_2, c_3, \tilde{a}_4)\} = \{A, B\}$. Кроме того, $(a, c_2, c_3, \tilde{a}_4) \neq (a, c_2, c_3, \ldots, c_n)$ (иначе, так как $f(a, c_2, c_3, \ldots, c_n) \notin \{A, B\}$, в квадрате было бы 3 разных значения f).
- Продолжаем аналогично, на каждом шаге заменяя очередную координату a_i у пары наборов на c_i.

Критерий Яблонского

Доказательство (продолжение)

- Каждый раз либо получим искомый квадрат, либо на новой паре наборов функция будет принимать значения A и B, при этом никакой набор очередной пары не будет совпадать с $(a, c_2, \ldots, c_n)$.
- В результате, если искомый квадрат не будет найден раньше, мы придём к квадрату

$$
\begin{array}{cc}
(a, c_2, \ldots, c_{n-1}, a_n), & (a, c_2, \ldots, c_{n-1}, c_n), \\
(b, c_2, \ldots, c_{n-1}, a_n), & (b, c_2, \ldots, c_{n-1}, c_n).
\end{array}
$$

- Имеем $\{f(a, c_2, \ldots, c_{n-1}, a_n), f(b, c_2, \ldots, c_{n-1}, a_n)\} = \{A, B\}$ и $f(a, c_2, \ldots, c_{n-1}, c_n) \notin \{A, B\}$. Квадрат содержит 3 различных значения, а значит одно из них только в одной точке квадрата.

$\square$

Критерий Яблонского

Теорема (критерий Слупецкого–Яблонского)

Пусть $k \geqslant 3$, $Q \subseteq P_k$ и Q содержит все функции одной переменной, принимающие не более $k-1$ значения. Тогда Q полон в P_k тогда и только тогда, когда Q содержит существенную функцию, принимающую все k значений.

Доказательство

- Пусть в Q нет существенной функции, принимающей все k значений.
- Суперпозиция принимает только значения, которые принимает «внешняя» функция суперпозиции. Кроме того, при подстановке функции, принимающей не все k значений, в любую одноместную функцию, получится функция, принимающая не все k значений.
- Тогда и $[Q]$ не может содержать существенной функции, принимающей все k значений, и $[Q] \neq P_k$.

Критерий Яблонского

Доказательство (продолжение)

- Пусть $f(x_1, \dots, x_n) \in Q$ — существенная функция, принимающая все k значений.
- По лемме о квадрате существует квадрат, на котором f принимает не менее 2 значений, причём одно из них — лишь в одной точке квадрата.
- Не ограничивая общности, считаем, что это квадрат

$$\begin{aligned} &(a,\ c,\ a_3, \dots, a_n), \quad (a,\ d,\ a_3, \dots, a_n), \\ &(b,\ c,\ a_3, \dots, a_n), \quad (b,\ d,\ a_3, \dots, a_n). \end{aligned}$$

- Пусть $e = f(a, c, a_3, \dots, a_n)$ — значение, принимаемое на этом квадрате только в одной точке (для достижения этого достаточно поменять местами обозначения a и b и/или обозначения c и d).

Критерий Яблонского

Доказательство (продолжение)

- Все константы принимают только 1 значение и принадлежат Q.
- Построим $g'(x) = \begin{cases} 0, & x = e, \\ 1, & x \neq e \end{cases} \in Q \ \ (2 \leqslant k-1$ значения).
- Теперь $g(x_1, x_2) = g'(f(x_1, x_2, a_3, \ldots, a_n)) \in [Q]$.
- Легко видеть, что $g(a,c) = 0, \ g(a,d) = g(b,c) = g(b,d) = 1$.
- Пусть $g_1(x_1) = \begin{cases} a, & x_1 = 0, \\ b, & x_1 \neq 0, \end{cases} \quad g_2(x_2) = \begin{cases} c, & x_2 = 0, \\ d, & x_2 \neq 0 \end{cases}$
- Ясно, что $g_1, g_2 \in Q$, а оператор $(g_1(x_1),\ g_2(x_2))$ отображает $\{0,1\}^2$ в $\{a,b\} \times \{c,d\}$, причём $(0,0)$ переходит в (a,c).
- Тогда функция $x_1 \vee_{01} x_2 = g(g_1(x_1),\ g_2(x_2)) \in [Q]$, $\vee_{01}$ совпадает с дизъюнкцией на $\{0,1\}^2$.
- $j_0(x) \in Q$, $j_0(x)$ совпадает с отрицанием на $\{0,1\}$.

Критерий Яблонского

Доказательство (продолжение)

- Функция $x_1 \,\&_{01}\, x_2 = j_0(j_0(x_1) \vee_{01} j_0(x_2)) \in [Q]$. $\&_{01}$ совпадает с конъюнкцией (или, иначе говоря, с умножением) на $\{0,1\}^2$.
- Пусть $d(x_1, \ldots, x_r)$ — произвольная функция из P_k, принимающая только значения $0, 1$. По теореме о второй форме

$$d(x_1, \ldots, x_r) = \sum_{\sigma_1, \ldots, \sigma_r \in E_k} j_{\sigma_1}(x_1) \ldots j_{\sigma_r}(x_r) d(\sigma_1, \ldots, \sigma_r).$$

- В этой сумме все множители и слагаемые могут быть равны только 0 или 1. Кроме того, в сумме может быть не более одного ненулевого слагаемого. Поэтому

$$d(x_1, \ldots, x_r) = \bigvee_{\sigma_1, \ldots, \sigma_r \in E_k}{}_{01} \; j_{\sigma_1}(x_1) \&_{01} \ldots \&_{01} j_{\sigma_r}(x_r) \&_{01} d(\sigma_1, \ldots, \sigma_r).$$

Критерий Яблонского

Доказательство (продолжение)

- Функции j_σ принимают 2 значения и принадлежат Q. Поэтому любая функция $d \in P_k$, принимающая только значения $0, 1$, принадлежит $[Q]$.
- Пусть $d(x_1, \ldots, x_r) \in P_k$, d принимает только два значения p и q.
- $l(x) = \begin{cases} p, & x = 0, \\ q & \text{иначе}, \end{cases}$ $\quad l'(x) = \begin{cases} 0, & x = p, \\ 1 & \text{иначе}. \end{cases}$ Ясно, что $l, l' \in Q$.
- Функция $d_0(x_1, \ldots, x_r) = l'(d(x_1, \ldots, x_r)) \in [Q]$, так как d_0 принимает только значения 0 и 1.
- Тогда $d(x_1, \ldots, x_r) = l(d_0(x_1, \ldots, x_r)) \in [Q]$.
- Итак, любая функция $d \in P_k$, принимающая не более 2 значений, принадлежит $[Q]$.

Лекция 10
Окончание доказательства критерия Яблонского. Теорема Янова, теорема Мучника. Число замкнутых классов в P_k. Классы функций, сохраняющих предикаты

Критерий Яблонского

Теорема (критерий Слупецкого–Яблонского)

Пусть $k \geqslant 3$, $Q \subseteq P_k$ и Q содержит все функции одной переменной, принимающие не более $k-1$ значения. Тогда Q полон в P_k тогда и только тогда, когда Q содержит существенную функцию, принимающую все k значений.

Доказательство (продолжение)

- $\Leftarrow$. Ранее было доказано, что любая функция $d \in P_k$, принимающая не более 2 значений, принадлежит $[Q]$.
- Используя индукцию по v докажем, что $[Q]$ содержит все функции из P_k, принимающие не более v значений при $v = \overline{2, k}$.

Критерий Яблонского

Доказательство (продолжение)

- Для $v = 2$ доказано ранее. Пусть $[Q]$ содержит все функции, принимающие не более $v - 1 \geqslant 2$ значений.
- Шаг индукции. По следствию из леммы о трёх наборах существует v наборов $(a_1^1, \ldots, a_n^1)$, $\ldots$, $(a_1^v, \ldots, a_n^v)$, на которых f принимает v различных значений, причём множество $\{a_i^1, \ldots, a_i^v\}$ содержит не более $v - 1$ значений при $i = \overline{1, n}$.
- Обозначим $b_j = f(a_1^j, \ldots, a_n^j)$, $j = \overline{1, v}$.
- Пусть $h(x_1, \ldots, x_r) \in P_k$, h принимает только значения $b_1, \ldots, b_v$.
- Пусть $g_i(x_1, \ldots, x_r) = a_i^j$ при $h(x_1, \ldots, x_r) = b_j$, $j = \overline{1, v}$, $i = \overline{1, n}$. Эти n функций полностью задаются указанным соотношением. Каждая из них принимает не более $v - 1$ значений, поэтому по предположению индукции они принадлежат $[Q]$.

Критерий Яблонского

Доказательство (продолжение)

- Нетрудно видеть, что
  $h(x_1, \dots, x_r) = f(g_1(x_1, \dots, x_r), \dots, g_n(x_1, \dots, x_r)) \in [Q]$.
- Если $v = k$, получили $[Q] = P_k$. Пусть $v < k$.
- Пусть $h_1(x_1, \dots, x_r) \in P_k$, h_1 принимает не более v значений $e_1, \dots, e_v$ (в отличие от прошлого случая эти значения произвольны и не связаны с f).
- $l(x) = \begin{cases} e_i, & x = b_i,\ i = \overline{1, v}, \\ e_1 & \text{иначе}, \end{cases} \qquad l'(x) = \begin{cases} b_i, & x = e_i,\ i = \overline{1, v}, \\ b_1 & \text{иначе}. \end{cases}$
  Ясно, что $l, l' \in Q$.
- Функция $h(x_1, \dots, x_r) = l'(h_1(x_1, \dots, x_r)) \in [Q]$, так как h принимает только значения $b_1, \dots, b_v$.
- Тогда $h_1(x_1, \dots, x_r) = l(h(x_1, \dots, x_r)) \in [Q]$.

Критерий Яблонского

Доказательство (продолжение)

- Итак, любая функция $h_1 \in P_k$, принимающая не более v значений, принадлежит $[Q]$. Шаг индукции обоснован.
- Таким образом, $[Q] = P_k$.

$\square$

Теорема Янова

Теорема (Янов)

Пусть $k \geqslant 3$. Тогда в P_k существует замкнутый класс, не имеющий базиса.

Доказательство

- Пусть
$$f_0(x) = 0,\ \ f_n(x_1, \ldots, x_n) = \begin{cases} 1, & x_1 = \ldots = x_n = 2, \\ 0 & \text{иначе}, \end{cases} \quad n = \overline{1, \infty},$$
$$F = \{f_n \mid n = \overline{0, \infty}\}_c.$$
- Ни одна функция f_n не принимает значение 2. Поэтому любая функция, реализуемая формулой над F с использованием более одного функционального символа (и без подстановок на места фиктивных переменных), является константой 0.
- Таким образом, F — замкнутый класс.

Теорема Янова

Доказательство (продолжение)

- Нетрудно видеть, что из любой функции f_n можно получить все функции f_m, $m < n$ с помощью отождествления переменных.
- Пусть $B \subseteq F$ — базис F.
- Пусть $f_m, f_n \in B$ при $m < n$. Тогда $f_m \in [f_n]$ и B не базис.
- Это значит, что $B = \{f_n\}$ для некоторого $n \in \mathbb{N}$. Но тогда $[B] = \{f_0, f_1, \ldots, f_n\}_c \neq F$.
- Полученное противоречие означает, что у класса F нет базиса.

$\square$

Теорема Мучника

Теорема (Мучник)

Пусть $k \geqslant 3$. Тогда в P_k существует замкнутый класс со счётным базисом.

Доказательство

- Пусть $g_n(x_1, \ldots, x_n) =$
  $$= \begin{cases} 1, & (\exists i)(x_i = 1 \,\&\, x_1 = \ldots = x_{i-1} = x_{i+1} = \ldots = x_n = 2), \\ 0 & \text{иначе}, \end{cases}$$
  $n = \overline{2, \infty}$,
  $F = [\{g_i \mid i = \overline{2, \infty}\}]$ — замкнутый класс.
- Докажем, что $B = \{g_i \mid i = \overline{2, \infty}\}$ — базис в F. Ясно, что система B полна в F.
- Покажем, что ни одну из функций B нельзя выразить через другие.

Теорема Мучника

Доказательство (продолжение)

- Пусть $g_m = \Phi(g_2, \ldots, g_{m-1}, g_{m+1}, \ldots, g_l)$ и g_n — внешняя функция формулы Φ.
- Пусть в g_n подставлены две или более формул, не являющиеся переменными: $g_m(x_1, \ldots, x_m) = g_n(\ldots, \Phi_1, \ldots, \Phi_2, \ldots)$.
- Поскольку функции, реализуемые Φ_1, Φ_2, не принимают значения 2, получаем $g_m(x_1, \ldots, x_m) \equiv 0$, что невозможно.
- Пусть в g_n подставлена ровно одна формула Φ', не являющаяся переменной. Поскольку $n \geqslant 2$, в g_n подставлена хотя бы одна переменная $x_p,\ p \in \{1, \ldots, m\}$:
  $g_m(x_1, \ldots, x_m) = g_n(\ldots, \Phi', \ldots, x_p, \ldots)$
- Рассмотрим набор $\bar{a} = (2, \ldots, 2, 1, 2, \ldots, 2)$, единица стоит в позиции p. Ясно, что $g_m(\bar{a}) = 1$.

Теорема Мучника

Доказательство (продолжение)

- Функция, реализуемая Φ', принимает на $\bar{a}$ значение $b \neq 2$, а $x_p(\bar{a}) = 1$.
- Тогда $g_m(\bar{a}) = g_n(\ldots, b, \ldots, 1, \ldots) = 0$.
  Но $g_m(\bar{a}) = 1$, поэтому такое невозможно.
- Пусть в g_n подставлены только переменные. Тогда, очевидно, $m < n$ и хотя бы одна переменная x_p подставлена хотя бы 2 раза: $g_m(x_1, \ldots, x_m) = g_n(\ldots, x_p, \ldots, x_p, \ldots)$
- Рассмотрим набор $\bar{a} = (2, \ldots, 2, 1, 2, \ldots, 2)$, единица стоит в позиции p. Ясно, что $g_m(\bar{a}) = 1$.
- При этом $x_p(\bar{a}) = 1$, а $g_m(\bar{a}) = g_n(\ldots, 1, \ldots, 1, \ldots) = 0$.
  Но $g_m(\bar{a}) = 1$, поэтому такое невозможно.
- Таким образом, B — счётный базис F.

$\square$

Теорема Мучника

Следствие

Пусть $k \geqslant 3$. Тогда в P_k существует континуум замкнутых классов.

Доказательство

- Рассматриваем функции g_i, $i = \overline{2, \infty}$ из доказательства теоремы Мучника.
- Рассмотрим произвольную возрастающую последовательность $\alpha = (i_1, i_2, \ldots)$, $i_1 \geqslant 2$. Свяжем с ней класс $F_\alpha = [\{g_{i_1}, g_{i_2}, \ldots\}]$.
- Поскольку ни одну функцию g_i нельзя выразить через другие, разным последовательностям соответствуют разные классы.
- Всего различных последовательностей такого вида столько же, сколько последовательностей вида $(i_1 - 2,\ i_2 - i_1,\ i_3 - i_2,\ \ldots)$, то есть столько же, сколько и счётных последовательностей произвольных чисел из $\mathbb{N}_0$. Это число континуально.

□

Сохранение функцией предиката

Определение

Пусть $k \geqslant 2$.

- Предикат на множестве E_k — это отображение вида
$$\rho\colon E_k^m \to \{\mathbf{true}, \mathbf{false}\}.$$
- Набор $(a_1, \ldots, a_m)$ удовлетворяет предикату $\rho(x_1, \ldots, x_m)$, если $\rho(a_1, \ldots, a_m) = \mathbf{true}$.
- Пусть $(a_{11}, \ldots, a_{m1}), \ldots, (a_{1s}, \ldots, a_{ms})$ — все наборы из E_k^m, удовлетворяющие предикату ρ. Тогда, выписывая их в виде столбцов, получим матрицу предиката ρ:
$$X_\rho = \begin{pmatrix} a_{11} & \ldots & a_{1s} \\ \vdots & \ddots & \vdots \\ a_{m1} & \ldots & a_{ms} \end{pmatrix}.$$

Сохранение функцией предиката

Применение функции к набору векторов

Пусть $f(x_1, \dots, x_n) \in P_k$ и $\bar{a}_1, \dots, \bar{a}_n \in E_k^m$. Тогда через $f(\bar{a}_1, \dots, \bar{a}_n)$ обозначим результат поразрядного применения f к указанным векторам.

Определение

Пусть $f(x_1, \dots, x_n) \in P_k$. f сохраняет предикат $\rho(x_1, \dots, x_m)$, если для любых наборов

$$(a_{11}, \dots, a_{m1}),\ \dots,\ (a_{1n}, \dots, a_{mn}),$$

удовлетворяющих ρ, набор

$$f(a_{11}, \dots, a_{1n}),\ \dots,\ f(a_{m1}, \dots, a_{mn})$$

тоже удовлетворяет ρ.

Сохранение функцией предиката

Определение (равносильное)

Пусть $f(x_1, \dots, x_n) \in P_k$. f сохраняет предикат $\rho(x_1, \dots, x_m)$, если для любого набора столбцов матрицы X_ρ

$$\begin{pmatrix} a_{11} & & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & & a_{mn} \end{pmatrix}$$

столбец

$$f\begin{pmatrix} a_{11} & & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{m1} & & a_{mn} \end{pmatrix} = \begin{pmatrix} f(a_{11}, \dots, a_{1n}) \\ \vdots \\ f(a_{m1}, \dots, a_{mn}) \end{pmatrix}$$

тоже является столбцом X_ρ.

Сохранение функцией предиката

Определение

Пусть ρ — предикат на E_k. $\mathrm{Pol}(\rho)$ — это множество всех функций из P_k, сохраняющих предикат ρ.

Утверждение

Для любого предиката $\rho(x_1, \dots, x_m)$ множество $\mathrm{Pol}(\rho)$ содержит все селекторные функции $I_k^n(x_1, \dots, x_n) = x_k,\ k \in \{1, \dots, n\},\ n \in \mathbb{N}$.

Доказательство

- Рассмотрим любые столбцы $\bar{a}_1, \dots, \bar{a}_n$ матрицы X_ρ.
- Тогда $I_k^n(\bar{a}_1, \dots, \bar{a}_n) = \bar{a}_k$ — столбец X_ρ.

$\square$

Сохранение функцией предиката

Утверждение

Для любого предиката $\rho(x_1, \ldots, x_m)$ *множество* $\mathrm{Pol}(\rho)$ *является замкнутым классом.*

Доказательство

- Поскольку селекторные функции принадлежат $\mathrm{Pol}(\rho)$, достаточно доказать, что для любых функций
  $f_0(x_1, \ldots, x_l),\ f_1(x_1, \ldots, x_n),\ \ldots,\ f_l(x_1, \ldots, x_n) \in \mathrm{Pol}(\rho)$
  функция
  $f(x_1, \ldots, x_n) = f_0(f_1(x_1, \ldots, x_n),\ \ldots,\ f_l(x_1, \ldots, x_n)) \in \mathrm{Pol}(\rho)$.
- Пусть $\bar{a}_1, \ldots, \bar{a}_n$ — столбцы X_ρ. Тогда
  $\bar{b}_i = f_i(\bar{a}_1, \ldots, \bar{a}_n),\ i = \overline{1, l}$ — столбцы X_ρ.
- Тогда $f(\bar{a}_1, \ldots, \bar{a}_n) = f_0(\bar{b}_1, \ldots, \bar{b}_l)$ — столбец X_ρ.

$\square$

Сохранение функцией предиката

Примеры

- Рассматриваем функции из P_2.
- Рассмотрим предикат $(x = 0)$ (матрица (0)). Функция сохраняет этот предикат, если на нулевом наборе она выдаёт 0. $\mathrm{Pol}((x = 0)) = T_0$.
- Рассмотрим предикат $(x = 1)$ (матрица (1)). Функция сохраняет этот предикат, если на единичном наборе она выдаёт 1. $\mathrm{Pol}((x = 1)) = T_1$.
- Рассмотрим предикат $(x = \overline{y})$ (матрица $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$). Функция сохраняет этот предикат, если на противоположных наборах она принимает противоположные значения. $\mathrm{Pol}((x = \overline{y})) = S$.

- Мы будем описывать предполные классы в P_k как классы, сохраняющие предикаты определённого вида.

Лекция 11
Предполные классы в P_k: предикаты $\mathbf{P}, \mathbf{O}, \mathbf{L}, \mathbf{E}, \mathbf{C}, \mathbf{B}$.
Класс Слупецкого

Предикаты типа $\mathbf{P}$

Типы предполных предикатов

- Предикаты, определяющие все предполные классы P_k, разбиваются на шесть семейств $\mathbf{P}, \mathbf{O}, \mathbf{L}, \mathbf{E}, \mathbf{C}, \mathbf{B}$.

Предикаты типа $\mathbf{P}$

- $k \geqslant 2$. Рассмотрим произвольное взаимно-однозначное соответствие $E_k \leftrightarrow E_k$ (перестановку) π.
- Предикат $(\pi(x_1) = x_2)$ называется графиком перестановки.
- Функция сохраняет предикат $(\pi(x_1) = x_2)$ тогда и только тогда, когда $\pi(f(x_1, \ldots, x_n)) = f(\pi(x_1), \ldots, \pi(x_n))$. Эти функции называются самосопряжёнными относительно перестановки π.
- $\mathbf{P}$ — это класс всех предикатов вида $(\pi(x_1) = x_2)$, где перестановка π разлагается в произведение циклов одной и той же простой длины.

Предикаты типа $\mathbf{P}$

Предикаты типа $\mathbf{P}$: примеры

- Запись $(12)(3)(456)$ в виде произведения трёх циклов задаёт перестановку, переводящую $1 \to 2 \to 1, \quad 3 \to 3, \quad 4 \to 5 \to 6 \to 4$. Эта перестановка не является произведением циклов одной и той же простой длины.
- Перестановка $(12)(34)(56)$ является произведением циклов одной и той же простой длины 2.
- $k = 2$. Существует две перестановки: тождественная $(0)(1)$ (циклы имеют длину 1 — не простую) и перестановка (01). График (01) — $(x_1 = \overline{x}_2)$. Она задаёт класс S.
- При $k = 3$ существуют две перестановки нужного вида: $\pi_1 = (012)$ и $\pi_2 = (021)$. Их графики это $(x_1 + 1 = x_2)$ и $(x_1 + 2 = x_2)$.
- Так как $\pi_2 = \pi_1^{-1}$, предикат $x_1 = \pi_2(x_2)$ совпадает с $\pi_1(x_1) = x_2$, и эти перестановки задают один и тот же замкнутый класс.

Предикаты типа $\mathbf{O}$

Предикаты типа $\mathbf{O}$

- $k \geqslant 2$. Предикат $x_1 \leqslant_\rho x_2$ — это частичный порядок на E_k, если
  1) $x \leqslant_\rho x, \quad x \in E_k$;
  2) $x \leqslant_\rho y,\ y \leqslant_\rho z \ \rightarrow\ x \leqslant_\rho z, \quad x, y, z \in E_k$;
  3) $x \leqslant_\rho y,\ y \leqslant_\rho x \ \rightarrow\ x = y, \quad x, y \in E_k$.
- Частичный порядок допускает, что некоторые элементы могут быть несравнимы. Если все элементы сравнимы, то такой порядок называется линейным.
- Классы функций, сохраняющих частичные порядки, называются классами монотонных функций.
- Частичный порядок ограничен, если существует наибольший элемент (x такой, что $(\forall y)(y \leqslant_\rho x)$) и наименьший элемент ($x$ такой, что $(\forall y)(x \leqslant_\rho y)$).
- $\mathbf{O}$ — это класс всех ограниченных частичных порядков.

Предикаты типа $\mathbf{O}$

Предикаты типа $\mathbf{O}$: примеры

- При $k = 2$ существует два ограниченных частичных порядка: $0 \leqslant 1$ и $1 \leqslant 0$ (оба порядка линейные). Они задают один и тот же класс монотонных функций.
- При $k = 3$ существует три класса монотонных функций, задаваемых линейными порядками $0 \leqslant 1 \leqslant 2$, $1 \leqslant 2 \leqslant 0$ и $2 \leqslant 0 \leqslant 1$. Эти классы различаются содержанием функций
$$f_1(x,y) = \begin{cases} 1, & x = y = 0, \\ 2, & \text{иначе} \end{cases} \quad \text{и} \quad f_2(x,y) = \begin{cases} 2, & x = y = 1, \\ 0, & \text{иначе.} \end{cases}$$
Есть три других ограниченных порядка, которые являются обращениями данных, поэтому задают те же классы монотонных функций.
- При $k \geqslant 4$ существует нелинейный ограниченный частичный порядок: $0 \leqslant 1 \leqslant 3$, $0 \leqslant 2 \leqslant 3$, 1 и 2 не сравнимы, $3 \leqslant \ldots \leqslant k-1$.

Предикаты типа $\mathbf{L}$

Предикаты типа $\mathbf{L}$

- Предикаты данного типа существуют только при $k = p^l$, p — простое число, $l \in \mathbb{N}$.
- При $k = p^l$ на E_k можно определить бинарную операцию $+$ так, что $(E_k, +)$ образует абелеву p-группу периода p.
- $(E_k, +)$ является группой, если
  - Ассоциативность: $(a + b) + c = a + (b + c), \quad a, b, c \in E_k$;
  - Существует $\theta \in E_k$ такое, что $a + \theta = a, \quad a \in E_k$;
  - Для любого $a \in E_k$ существует $-a \in E_k$ такой, что $a + (-a) = \theta$.
- $(E_k, +)$ является p-группой, если это группа порядка p^l при некотором $l \in \mathbb{N}$, то есть это группа и $|E_k| = p^l$.
- Группа является абелевой, если $+$ коммутативен, то есть $a + b = b + a, \quad a, b \in E_k$.

Предикаты типа $\mathbf{L}$

Предикаты типа $\mathbf{L}$

- Порядком элемента $a \in E_k$ называется наименьшее t такое, что $\underbrace{a + \ldots + a}_{t} = \theta$.
- Периодом группы называется наименьшее общее кратное порядков элементов группы. Любая конечная группа имеет период, который делит порядок группы.
- Известно, что при $k = p^l$ существует конечное поле $(E_k; +, \times)$. Соответствующие таким полям группы $(E_k; +)$ и являются абелевыми p-группами периода p.
- $\mathbf{L}$ — это класс предикатов вида $(x_1 + x_2 = x_3 + x_4)$ для всех возможных операций $+$, образующих абелеву p-группу периода p.
- Классы функций, сохраняющие предикаты из $\mathbf{L}$, называются классами квазилинейных функций.

Предикаты типа $\mathbf{L}$

Предикаты типа $\mathbf{L}$

- Свойство квазилинейной функции:
  $f(a_1+b_1,\ \ldots,\ a_n+b_n) = f(a_1,\ldots,a_n) + f(b_1,\ldots,b_n) - f(\theta,\ldots,\theta)$.
- Общий вид квазилинейной функции (для данного конечного поля):

$$f(x_1,\ldots,x_n) = a_0 + \sum_{i=1}^{n}\sum_{j=0}^{l-1} a_{ij}x_i^{p^j}.$$

Предикаты типа $\mathbf{L}$: примеры

- При $k=2$ матрица предиката $(x_1+x_2=x_3+x_4)$ имеет вид

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

Предикаты типа $\mathbf{L}$

Предикаты типа $\mathbf{L}$: примеры

- При $k = 2$ предикат $(x_1 + x_2 = x_3 + x_4)$ задаёт класс L линейных функций (оба способа задать операцию $+$ дают один и тот же класс).
- Аналогично при простом k задаётся класс линейных по модулю k функций:
$$f(x_1, \ldots, x_n) = a_0 + \sum_{i=1}^{n} a_i x_i.$$
- При $k = p^l,\ l \geqslant 2$ нет предполного класса линейных по модулю k функций, но могут быть классы квазилинейных функций с более специфически определённой операцией сложения.

Предикаты типа $\mathbf{L}$

Предикаты типа $\mathbf{L}$: примеры

- При $k = 4 = 2^2$ обычное сложение по модулю 4 не образует группу периода 2.
- Вместо него можно взять операцию покоординатного сложения двоичных записей чисел по модулю 2:

$$x + 0 = x, \quad x + x = 0, \quad 1 + 2 = 3, \quad 1 + 3 = 2.$$

$+$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Предикаты типа $\mathbf{E}$

Предикаты типа $\mathbf{E}$

- $k \geqslant 3$. Отношение $\sim_\rho$ — отношение эквивалентности на E_k, если
  - $a \sim_\rho a, \quad a \in E_k$;
  - $a \sim_\rho b \ \rightarrow \ b \sim_\rho a, \quad a, b \in E_k$;
  - $a \sim_\rho b, \ b \sim_\rho c \ \rightarrow \ a \sim_\rho c, \quad a, b, c \in E_k$.
- Отношение эквивалентности задаёт разбиение E_k на классы эквивалентных элементов.
- Отношение эквивалентности на E_k нетривиально, если существуют хотя бы два неэквивалентных элемента из E_k и хотя бы два неравных эквивалентных элемента из E_k.
- $\mathbf{E}$ — класс нетривиальных отношений эквивалентности на E_k.
- Класс функций, сохраняющих отношение эквивалентности, называется классом функций, сохраняющим разбиение (на соответствующие классы эквивалентности).

Предикаты типа $\mathbf{E}$

Предикаты типа $\mathbf{E}$: пример

- Пусть $k = 3$, отношение эквивалентности имеет классы эквивалентности $\{0\}$ и $\{1, 2\}$. Тогда его матрица:

$$\begin{pmatrix} 0 & 1 & 1 & 2 & 2 \\ 0 & 1 & 2 & 1 & 2 \end{pmatrix}.$$

- Все вектора длины n над E_3 можно разбить на классы эквивалентности: эквивалентными считаем вектора с одинаковыми наборами нулевых координат.
- Функции, сохраняющие указанное разбиение, для каждого класса эквивалентности векторов либо принимают значение 0 на всех векторах класса, либо не принимают значения 0 ни на одном векторе класса.

Предикаты типа $\mathbf{C}$

Предикаты типа $\mathbf{C}$

- $k \geqslant 2$. Предикат $\rho(x, y)$ называется рефлексивным, если $\rho(x, x)$ тождественно истинно.
- Обозначим $\tau_m(x_1, \ldots, x_m) = \bigvee\limits_{\substack{i,j=\overline{1,m} \\ i<j}} (x_i = x_j), \quad m \geqslant 2$. Этот предикат истинен, если хотя бы два из поданных значений равны.
- Предикат $\rho(x_1, \ldots, x_m)$ называется вполне рефлексивным, если $m = 1$ или $\tau(x_1, \ldots, x_m) \to \rho(x_1, \ldots, x_m)$ является тождественной истиной. Иными словами, предикат вполне рефлексивен, если он может быть ложен, только когда все поданные значения различны.
- Предикат $\rho(x_1, \ldots, x_m)$ называется вполне симметричным, если его значение не изменяется при любой перестановке переменных.

Предикаты типа $\mathbf{C}$

Предикаты типа $\mathbf{C}$

- Предикат $\rho(x_1, \ldots, x_m)$ называется центральным, если ρ не тождественно истинный и
  1) ρ вполне рефлексивен;
  2) ρ вполне симметричен;
  3) Существует C (центр предиката) — собственное подмножество E_k такое, что если среди элементов $a_1, \ldots, a_m \in E_k$ существует элемент $a_i \in C$, то $\rho(a_1, \ldots, a_m)$ истинно.
- $\mathbf{C}$ — класс центральных предикатов.
- Пусть C — собственное подмножество E_k. Тогда одноместный предикат $(x \in C)$ является центральным.
- Класс $\mathrm{Pol}((x \in C))$ называется классом функций, сохраняющих множество C.

Предикаты типа $\mathbf{C}$

Предикаты типа $\mathbf{C}$: примеры

- При $k = 2$: T_0 — класс функций, сохраняющих множество $\{0\}$. T_1 — класс функций, сохраняющих множество $\{1\}$.
- При $k = 3$ существует 6 аналогичных классов, сохраняющих множества.
- При $k = 3$ существуют также 3 класса, сохраняющие двухместные предикаты с центрами $\{0\}$, $\{1\}$, $\{2\}$. Эти предикаты имеют вид

$$\rho_0(x, y) \equiv ((x = y) \vee (x = 0) \vee (y = 0)),$$
$$\rho_1(x, y) \equiv ((x = y) \vee (x = 1) \vee (y = 1)),$$
$$\rho_2(x, y) \equiv ((x = y) \vee (x = 2) \vee (y = 2)).$$

- При $k \geqslant 4$ существует множество классов подобного вида.

Предикаты типа $\mathbf{B}$

Предикаты типа $\mathbf{B}$

- $k \geqslant 3$. Пусть $h \geqslant 3$ (необязательно простое), $l \in \mathbb{N}$ и $k \geqslant h^l$.
- Любой элемент $a \in E_{h^l}$ можно единственным образом представить в виде

$$a = a^{(0)} + a^{(1)}h + \ldots + a^{(l-1)}h^{l-1},$$

  где $a^{(0)}, \ldots, a^{(l-1)} \in E_h$. Будем записывать это представление в виде $a = (a^{(0)}, \ldots, a^{(l-1)})$.
- В этом представлении числа $a^{(0)}, \ldots, a^{(l-1)}$ являются цифрами числа $a \in \{0, \ldots, h^l - 1\}$ в системе счисления с основанием h.

Предикаты типа $\mathbf{B}$

Предикаты типа $\mathbf{B}$

- Пусть $\rho(x_1, \ldots, x_m)$ — предикат на E_h. l-й декартовой степенью предиката ρ называем предикат $\rho^l(x_1, \ldots, x_m)$ на E_{h^l} такой, что если

$$a_1 = (a_1^{(0)}, a_1^{(1)}, \ldots, a_1^{(l-1)}),\ \ldots,\ a_m = (a_m^{(0)}, a_m^{(1)}, \ldots, a_m^{(l-1)}),$$

то

$$\rho^l(a_1, \ldots, a_m) \equiv \rho(a_1^{(0)}, \ldots, a_m^{(0)})\ \&\ \ldots\ \&\ \rho(a_1^{(l-1)}, \ldots, a_m^{(l-1)}).$$

- Пусть $\sigma(x_1, \ldots, x_m)$ — предикат на множестве E_{h^l} и $q\colon E_k \to E_{h^l}$. Предикат $\rho(x_1, \ldots, x_m)$ на E_k называется полным прообразом предиката σ при отображении q, если

$$\rho(x_1, \ldots, x_m) \equiv \sigma(q(x_1), \ldots, q(x_m)).$$

Предикаты типа $\mathbf{B}$

Предикаты типа $\mathbf{B}$

- Напомним: $\tau_m(x_1,\ldots,x_m) = \bigvee\limits_{\substack{i,j=\overline{1,m}\\ i<j}} (x_i = x_j), \quad m \geqslant 2$. Этот предикат истинен, если хотя бы два из поданных значений равны.
- $\mathbf{B}$ — это класс всех полных прообразов $\tau_h^l(q(x_1),\ldots,q(x_h))$ предикатов вида $\tau_h^l(x_1,\ldots,x_h)$ при произвольных сюръективных отображених $q\colon E_k \to E_{h^l}$ и при произвольных $h \geqslant 3,\ l \geqslant 1,\ h^l \leqslant k$.
- Произвольный предикат из $\mathbf{B}$ получается следующим образом:
  - Выбираем произвольные h, l: $h \geqslant 3,\ l \geqslant 1,\ h^l \leqslant k$;
  - Выбираем произвольное сюръективное $q\colon E_k \to E_{h^l}$;
  - Берём предикат $\tau_h(x_1,\ldots,x_h)$ на E_h;
  - Берём его l-ю декартову степень: $\tau_h^l(x_1,\ldots,x_h)$ (это предикат на E_{h^l});
  - Берём полный прообраз полученного предиката при отображении q: $\tau_h^l(q(x_1),\ldots,q(x_h))$ (это предикат на E_k).

Предикаты типа $\mathbf{B}$

Предикаты типа $\mathbf{B}$: примеры

- При $k \geqslant 3$ предикат $\tau_k(x_1, \ldots, x_k) \in \mathbf{B}$ (при $h = k$, $l = 1$, q — тождественная функция). Этот предикат задаёт класс Слупецкого: класс всех функций, принимающих не все k значений, и всех функций одной переменной:
  - Если в наборе было 2 одинаковых значения, то после воздействия функции одной переменной эти значения останутся одинаковыми.
  - Если функция принимает не все k значений, то на любых k наборах она выдаст хотя бы 2 одинаковых значения.
  - Если функция существенна и принимает все k значений, то по следствию из леммы о трёх наборах она переводит некоторые столбцы матрицы предиката τ_k в столбец с k различными значениями.

Литература

1. Марченков С. С. Функциональные системы. — М.: МАКС Пресс, 2012. — 47 с. Файл на `mk.cs.msu.ru`
2. Марченков С. С. Избранные главы дискретной математики. — М.: Физматлит, 2023. — 192 с.
3. Марченков С. С. Избранные главы дискретной математики. — М.: МАКС Пресс, 2015. — 136 с. Файл на `mk.cs.msu.ru`