Содержание

1 Билет 1 (Основные определения и функции алгебры логики)

Определение. Упорядоченный набор - функция, которая ставит в соответствие каждому элементу множества $\{1, \ldots, n\}$ элемент из множества $\{a_1, \ldots, a_n\}$: $1 \to a_1$, …, $n \to a_n$.

Декартовое произведение множеств $A_1 \times \ldots \times A_n = (a_1, \ldots, a_n) : a_i \in A_i$.

Определение. Пусть функция f определена на $A_1 \times \ldots \times A_n$, тогда f - n-местная функция.

Определение. Множество $B_n = E_2 \times \ldots \times E_2$, где $E_i = \{0, 1\}$, называется n-мерным булевым кубом.

Определение. Функция $f : B_n \to E_2$ называется функцией алгебры логики. Множество всех таких функций обозначим P_2.

Представление функции $f(x_1, \ldots, x_n)$ в виде таблицы, имеющей $n + 1$ столбец:

x_1	$\ldots$	x_{n-1}	x_n	f
0	$\ldots$	0	0	0
0	$\ldots$	0	0	1
0	$\ldots$	0	1	0
$\vdots$		$\vdots$	$\vdots$	$\vdots$
1	$\ldots$	1	1	1

Так как число различных первых n столбцов 2^n, так как в каждой ячейке одного столбца может быть либо 0, либо 1. $\Longrightarrow$ число функций будет 2^{2^n}, так как для каждого набора значение функции может быть либо 0, либо 1.

Определение. Переменная x_i называется существенной, если существуют наборы α_1, …, α_{i-1}, 1, α_{i+1}, …, α_n и α_1, …, α_{i-1}, 0, α_{i+1}, …, α_n, на которых функция принимает различные значения. В противном случае переменная x_i называется несущественной (фиктивной).

Определение. Пусть x_i - фиктивная переменная, тогда, если функция $f(x_1$, …, x_{i-1}, x_{i+1}, …, $x_n) = g(x_1$, …, x_{i-1}, 0, x_{i+1}, …, $x_n)$, то функция g называется полученной из f добавлением фиктивной переменной. Функция удаления фиктивной переменной определяется аналогично.

Определение. Функция называется симметрической, если при любых перестановках переменных $x_{i_1}, \ldots, x_{i_n}$ значение функции не меняется.

Элементарные функции в алгебре логики:

1. константы 0, 1
2. тождественный x
3. отрицание $\overline{x}$
4. конъюнкция $x \wedge y$
5. дизъюнкция $x \vee y$
6. имплекация $x \to y$
7. штрих Шеффера $x|y$
8. стрелка Пирса $x \downarrow y$
9. сложение по модулю 2
10. эквивалентность

2 Билет 2 (Основные определения алгебры логики, связанные с формулой)

Определение. Формула - слово в некотором алфавите A.

Определение. Алфавит - конечное или бесконечное множество.

Определение. Слово - произвольная функция, определённая на начальном отрезке натурального ряда и принимающая на нём значения из A.

Определение. Пусть F - множество функций алгебры логики, S - множество символов, обозначающих функции из F, тогда отображение $\Sigma : S \to F$ - сигнатура для F.

Определение. Пусть $X = \{x_1, \ldots\}$ - символы переменных.
База индукция: если x_i - символ переменной, то однобуквенное слово, состоящее из x_i - формула в сигнатуре Σ.
Пусть $s \in S$, $f = \Sigma(s)$ - функция от n переменных, Φ_1, …, Φ_n - формулы в сигнатуре Σ, тогда слово $s(\Phi_1$, …, $\Phi_n)$ - формула в сигнатуре Σ.

Определение. Пусть Φ - формула, $\tilde{x}$ - упорядоченный набор $(x_{i_1}, \ldots, x_{i_n})$, содержащий все переменные формулы Φ, $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ - двоичный набор.
База индукции: Φ - однобуквенное слово x_{i_j}, тогда $\Phi[\tilde{x}, \tilde{\alpha}] = \alpha_j$ - значение формулы на наборе $\tilde{\alpha}$.
Пусть Φ - $s(\Phi_1, \ldots, \Phi_n)$, $f = \Sigma(s)$, причём $\Phi_1[\tilde{x}, \tilde{\alpha}] = \beta_1$, …, $\Phi_n[\tilde{x}, \tilde{\alpha}] = \beta_n$, тогда $f(\beta_1, \ldots, \beta_n)$ - значение формулы Φ на наборе значений переменных.

Определение. Формулой, определяющей функцию f алгебры логики, определённой на B_n, называется формула Φ такая, что $\forall$ набора $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n) \in B_n$ $f(\tilde{\alpha}) = \Phi[\tilde{x}, \tilde{\alpha}]$.

Определение. Формулы в сигнатуре, представляющие собой переменные, называются вырожденными, остальные - невырожденными. Если функция определяется невырожденной формулой в сигнатуре $\Sigma : S \to F$, то она получена суперпозициями над F, где F - множество функций.

Определение. (Другое определение суперпозиции) Если одну функцию можно получить с помощью конечного числа применений следующих трёх операций, то данная функция называется функцией, полученной суперпозициями над F. Операции:

1. Операция подстановки переменных. Пусть $f(x_1, \ldots, x_n) \in P_2$, $g(x_1, \ldots, x_n)$ - функция, определённая на B_n, такая, что $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, где набор $(i_1, \ldots, i_n)$ - набор элементов $(1, \ldots, n)$ (они необязательно различны). Тогда g получена из f операцией подстановки переменных.

2. Операция подстановки функции в функцию. Пусть $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m)$, h определена на B_{n+m-1} и $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, тогда функция h получена из функций f и g операцией подстановки одной функции в другую.

3. Операция добавления или удаления фиктивных переменных. Пусть x_i - фиктивная переменная, тогда если функция $f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$, то функция g называется полученной из f добавлением фиктивной переменной. Функция удаления фиктивной переменной определяется аналогично.

3 Билет 3 (Основные тождества алгебры логики)

Определение. Формулы F_1 и F_2 называются эквивалентными, если они определяют равные функции относительно объединения их переменных. Функции называются равными, если их области определения равны и $\forall x \in D_f(x)$ $f(x) = g(x)$. Слово $F_1 = F_2$, если формулы F_1 и F_2 эквивалентны, называется тождеством.

Основные тождества:

1. Ассоциативность операций: $\wedge$, $\vee$, $\neg$, $\leftrightarrow$.
2. Дистрибутивности:
   (a) $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$
   (b) $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$
   (c) $(x + y) \cdot z = x \cdot z + y \cdot z$
3. Тождества для отрицания:
   (a) $\overline{\overline{x}} = x$
   (b) $\overline{x \wedge y} = \overline{x} \vee \overline{y}$
   (c) $\overline{x \vee y} = \overline{x} \wedge \overline{y}$
   (d) $x \cdot \overline{x} = 0$
   (e) $x \vee \overline{x} = 1$
   (f) $\overline{x \rightarrow y} = x \cdot \overline{y}$
4. Тождества для эдентичных операндов
5. Тождества с константным операндом

Определение. Функция g называется двойственной к f, если $g(x_1, \ldots, x_n) = \overline{f}(\overline{x_1}, \ldots, \overline{x_n})$. Обозначение $g = f^*$.

Определение. Если функция двойственна к самой себе, то она называется самодвойственной.

Теорема. *(принцип двойственности) Если Φ - формула в сигнатуре $\Sigma : S \rightarrow F$, определяющая некоторую функцию g, то эта формула в сигнатуре $\Sigma^* : S \rightarrow F^*$ определяет двойственную функцию g^*.*

Доказательство. База индукции: пусть x_i - символ переменной, тогда однобуквенное слово, состоящее из x_i - формула в сигатуре Σ, определяющая одноместную функцию g. Эта формула в сигнатуре Σ^* имеет вид $\overline{x_i}$, то есть она определяет функцию, двойственную к g.
Пусть $s \in S$, $f = \Sigma(s)$ - формула от n переменных, $\Phi_1, \ldots, \Phi_n$ - формулы в сигнатуре Σ, тогда слово $s(\Phi_1, \ldots, \Phi_n)$ - формула в сигнатуре Σ. В $\Sigma^*(s) = (\Sigma(s))^* = (\Sigma(s(\Phi_1, \ldots, \Phi_n)))^* = f^*$, то есть данная формула определяет в двойственной сигнатуре двойственнную функцию. □

4 Билет 4 (Совершенные д.н.ф. и к.н.ф)

Определение. Выражение $f(x_1, \ldots, x_n) = \bigvee\limits_{(\sigma_1,\ldots,\sigma_n): f(\sigma_1,\ldots,\sigma_n)=1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n} \cdot f(\sigma_1, \ldots, \sigma_n)$ называется совершенной дизъюнктивной нормальной формой. $x_i^{\sigma_i} = \begin{cases} x_i, \sigma_i = 1 \\ \overline{x}_i, \sigma_i = 0 \end{cases}$.

Теорема. *Для любой функции $f(x_1, \ldots, x_n)$ алгебры логики и $\forall m$ верно равенство:*
$f(x_1, \ldots, x_n) = \bigvee\limits_{(\sigma_1,\ldots,\sigma_m)\in B_m} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n)$.

Доказательство. Рассмотрим прозвольный набор $(\alpha_1, \ldots, \alpha_m)$, если $(\alpha_1, \ldots, \alpha_m) \neq (\sigma_1, \ldots, \sigma_m)$, то $\exists \alpha_i \neq \sigma_i \implies \alpha_i^{\sigma_i} = 0 \implies$ данное слагаемое будет равно нулю. Тогда единственным не нулевым членом будет $(\alpha_1^{\alpha_1} \cdot \ldots \cdot \alpha_m^{\alpha_m}) \cdot f(\alpha_1, \ldots, \alpha_m, x_{m+1}, \ldots, x_n) = f(x_1, \ldots, x_n)$. □

Теорема. *Любую функцию алгебры логики можно представить с помощью суперпозиций конъюнкции, дизъюнкции и отрицания.*

Доказательство. Так как любая функция алгебры логики, кроме тождественного нуля, реализуется совершенной д.н.ф., значит она представима суперпозициями конъюнкции, дизъюнкции и отрицания. Тождественный ноль можно представить так: $x \wedge \overline{x} = 0$. □

Теорема. *Любая функция алгебры логики, кроме тождественной единицы, представима в виде совершенной конъюнктивной нормальной формы.*

Доказательство. Так как любая функция алгебры логики, кроме тождественного нуля, представима в виде совершенной д.н.ф., тогда по принципу двойственности

$$f(x_1, \ldots, x_n) = \bigwedge_{(\sigma_1,\ldots,\sigma_n):f^*(\sigma_1,\ldots,\sigma_n)=1} x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n} \Longrightarrow$$
$$f(x_1, \ldots, x_n) = \bigwedge_{(\delta_1,\ldots,\delta_n):f(\delta_1,\ldots,\delta_n)=1} x_1^{\overline{\delta}_1} \vee \ldots \vee x_n^{\overline{\delta}_n}. \qquad \square$$

5 Билет 5 (Полные системы в алгебре логики)

Определение. Система функций называется полной в P_2, если через них выражаются все функции в P_2.

Примеры.

1. $\wedge$ и $\neg$
2. $\vee$ и $\neg$
3. $x|y$
4. $x \downarrow y$

Определение. Полиномы по модулю 2 вида: $\sum\limits_{\{i_1,\ldots,i_s\}\subseteq 1,\ldots,n} a_{i_1,\ldots,i_s} \cdot x_{i_1} \cdot \ldots \cdot x_{i_s}$ называются полиномами Жегалкина.

Теорема. *(Жегалкина)*
Любая функция алгебры логики представима полиномом Жегалкина, причём единственным образом.

Доказательство. Так как в каждом мономе полинома Жегалкина n перменных, каждая из которых может быть либо 0, либо 1, а коэффициент перед каждым мономом может принимать значение 0 или 1 $\Longrightarrow$ всего есть 2^{2^n} различных полиномов Жегалкина.
Пусть два различных полинома Жегалкина задают одну функцию, тогда мы получим ненулевой полином, задающий нулевую константу $\Longrightarrow$ противоречие $\Longrightarrow$ Любая функция алгебры логики представима полиномом Жегалкина, причём единственным образом. $\square$

6 Билет 6 (Замыкание множества и замкнутые классы)

Определение. Множество функций, которые можно пулучить из данного множества M функций алгебры логики, называется замыканием множества M и обозначается $[M]$.

Примеры. 1. $P_2 = [P_2]$

1, $x + y$ - множество линейных функций

Свойства. *1.* $M \subseteq [M]$

2. $[[M]] = [M]$

3. Если $M_1 \subseteq M_2$, *то* $[M_1] \subseteq [M_2]$

4. $[M_1] \cup [M_2] \subseteq [M_1 \cup M_2]$

Доказательство. 1. По определению замыкания.

2. Из первого следует, что $[M] \subseteq [[M]]$, а $[[M]] \subseteq [M]$, так как в противном случае существовала бы функция, которая не выражается суперпозициями функций из M, но выражается суперпозициями функций, которые выражаются суперпозициями функций из M, а значит, она выражается суперпозициями из $M \Longrightarrow$ противоречие.

3. Если функция получается суперепозициями из M_1, то её можно получить суперпозициями из M_2, так как все функции M_1 являются функциями M_2.

4. Пусть функция $f \in [M_1] \cup [M_2]$, тогда она получается суперпозициями из M_1 или из M_2, пусть для определённости она выражается суперпозициями из M_1, но тогда её можно получить суперпозициями из $M_1 \cup M_2$, то есть $f \in [M_1 \cup M_2]$

□

Определение. Класс функций M называется замкнутым, если $[M] = M$.

Примеры. 1. $P_2 = [P_2]$

2. $L = [L]$, L - множество линейных функций.

7 Билет 7 (Классы T_0 и T_1)

Определение. Функция f называется функцией, сохраняющей ноль, если на наборе из нулей она принимает значение 0.

Определение. Функция f называется функцией, сохраняющей единицу, если на наборе из единиц она принимает значение 1.

Класс функций, сохраняющих ноль, обозначим T_0, а класс функций, сохраняющих единицу, обозначим T_1.

Теорема. *Классы T_0 и T_1 замкнуты.*

Доказательство.

1. Операция подстановки переменных:
   $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, если функция f сохраняла ноль, то и функция g будет сохранять ноль, если функция f сохраняла единицу, то и функция g будет сохранять единицу.

2. Операция подстановки одной функции в другую:
   $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, если функции f и h сохраняли ноль, то и функция g будет сохранять ноль, если функции f и g сохраняли единицу, то и функция h будет сохранять единицу.

3. Операция добавления или удаления фиктивной переменной, не влияет на способность функции сохранять ноль или сохранять единицу.

Следовательно суперпозициями мы не сможем получить функцию, не принадлежащую данному классу $\Longrightarrow$ классы T_0 и T_1 - замкнуты. $\square$

8 Билет 8 (Класс S и лемма, связанная с ним)

Класс самодвойственных функций обозначим S.

Теорема. *Класс S замкнут.*

Доказательство.

1. Операция подстановки переменных:
   Пусть $f(x_1, \ldots, x_n) \in S$, $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, тогда $\overline{g}(\overline{x}_1, \ldots, \overline{x}_n) = \overline{f}(\overline{x}_{i_1}, \ldots, \overline{x}_{i_n}) = f(x_{i_1}, \ldots, x_{i_n}) = g(x_1, \ldots, x_n) \Longrightarrow g$ - самодвойственная функция.

2. Операция подстановки функции в функцию:
   Пусть $f(x_1, \ldots, x_n) \in S$, $g(x_1, \ldots, x_m) \in S$, $h(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, тогда $\overline{h}(\overline{x}_1, \ldots, \overline{x}_n, \overline{x}_{n+1}, \ldots, \overline{x}_{m+n-1}) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_{n-1}, g(\overline{x}_n, \ldots, \overline{x}_{m+n-1})) = \overline{f}(\overline{x}_1, \ldots, \overline{x}_{n-1}, \overline{g}(x_n, \ldots, x_{m+n-1})) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{m+n-1})) = h(x_1, \ldots, x_n, x_{n+1}, \ldots, x_{m+n-1}) \Longrightarrow h$ - самодвойственная функция.

3. Операция добавления или удаления фиктивных переменных:
   Пусть $f(x_1, \ldots, x_n) \in S$, $g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) = f(x_1, \ldots, x_n) =$

$g(x_1, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n)$, тогда $\overline{g}(\overline{x}_1, \ldots, \overline{x}_{i-1}, 1, \overline{x}_{i+1}, \ldots, \overline{x}_n) = f(x_1, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n) \Longrightarrow g$ - самодвойственная функция.

$\square$

Теорема. *Если функция f не является самодвойственной, то с помощью неё и функции отрицания можно получить константу.*

Доказательство. Пусть $f(x_1, \ldots, x_n) \notin S$, тогда существует набор $(\alpha_1, \ldots, \alpha_n)$:

$$f(\alpha_1, \ldots, \alpha_n) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n).$$

Пусть $\varphi_i = x^{\alpha_i}$, $\varphi(x) = f(\varphi_1(x), \ldots, \varphi_n(x))$,

тогда $\varphi(0) = f(0^{\alpha_1}, \ldots, 0^{\alpha_n}) = f(\overline{\alpha}_1, \ldots, \overline{\alpha}_n) = f(\alpha_1, \ldots, \alpha_n) = f(1^{\alpha_1}, \ldots, 1^{\alpha_n}) = \varphi(1) \Longrightarrow$

$\Longrightarrow \varphi(x)$ - константа, полученная из несамодвойственной функции и отрицания.

$\square$

9 Билет 9 (Класс М и лемма, связанная с ним)

Определение. Пусть $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, $\tilde{\beta} = (\beta_1, \ldots, \beta_n)$ - двоичные наборы, тогда $\tilde{\alpha} \leqslant \tilde{\beta}$, если $\forall i = \overline{1, n}$ $\alpha_i \leqslant \beta_i$.

Определение. Функция алгебры логики называется монотонной, если $\forall$ двоичных наборов $\tilde{\alpha}$ и $\tilde{\beta}$ таких, что $\tilde{\alpha} \leqslant \tilde{\beta}$, $f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$.

Теорема. *Класс M монотонных функций - замкнут.*

Доказательство. 1. Операция подстановки переменных:
$g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, если функция f монотонна, то
$\forall \tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_n) : \tilde{\alpha} \leqslant \tilde{\beta}$, $f(\tilde{\alpha}) \leqslant f(\tilde{\beta}) \Longrightarrow \alpha_1 \leqslant \beta_1, \ldots, \alpha_n \leqslant \beta_n \Longrightarrow$
$\Longrightarrow \alpha_{i_1} \leqslant \beta_{i_1}, \ldots, \alpha_{i_n} \leqslant \beta_{i_n} \Longrightarrow f(\alpha_{i_1}, \ldots, \alpha_{i_n}) \leqslant f(\beta_{i_1}, \ldots, \beta_{i_n}) \Longrightarrow$
$\Longrightarrow g(\alpha_1, \ldots, \alpha_n) = f(\alpha_{i_1}, \ldots, \alpha_{i_n}) \leqslant f(\beta_{i_1}, \ldots, \beta_{i_n}) = g(\beta_{i_1}, \ldots, \beta_{i_n}) \Longrightarrow g$ - монотонна.

2. Операция подстановки одной функции в другую:
$f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m)$ - монотонные функции, $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, так как функции f и g монотонны,

$\forall\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{m+n-1})$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_{m+n-1}) : \tilde{\alpha} \leqslant \tilde{\beta}$, $f(\tilde{\alpha}) \leqslant f(\tilde{\beta})$ и $g(\alpha_n, \ldots, \alpha_{m+n-1}) = g(\beta_n, \ldots, \alpha_{m+n-1}) \Longrightarrow$
$(\alpha_1, \ldots, \alpha_{n-1}, g(\alpha_n, \ldots, \alpha_{m+n-1})) \leqslant (\beta_1, \ldots, \beta_{n-1}, g(\beta_n, \ldots, \beta_{n+m-1})) \Longrightarrow$
$h(\alpha_1, \ldots, \alpha_{m+n-1}) = f(\alpha_1, \ldots, \alpha_{n-1}, g(\alpha_n, \ldots, \alpha_{m+n-1})) \leqslant f(\beta_1, \ldots, \beta_{n-1}, g(\beta_n, \ldots, \beta_{n+m-1})) = h(\beta_1, \ldots, \beta_{m+n-1})$.

3. Операция добавления или удаления фиктивных переменных:
$f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$, так как f монотонна $\Longrightarrow \forall\tilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$ и $\tilde{\beta} = (\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_n) : \tilde{\alpha} \leqslant \tilde{\beta}$,
верно $f(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_n)$.
Тогда $\tilde{\alpha}$, с добавленной фиктивной переменной, $\leqslant \tilde{\beta}$, с добавленной фиктивной переменной $\Longrightarrow g(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n) \leqslant f(\beta_1, \ldots, \beta_{i-1}, \beta_{i+1}, \ldots, \beta_n) = g(\beta_1, \ldots, \beta_{i-1}, 0, \beta_{i+1}, \ldots, \beta_n)$.

Следовательно, суперпозициями мы не сможем получить функцию, не принадлежащую данному классу $\Longrightarrow$ класс M замкнут. $\square$

Теорема. *Если f - немонотонная функция, то из неё и констант можно получить отрицание.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ - немонотонная функция, тогда $\exists\tilde{\alpha}$ и $\tilde{\beta}$: $\tilde{\alpha} \leqslant \tilde{\beta}$ и $f(\tilde{\alpha}) = 1$, а $f(\tilde{\beta}) = 0$. Так как наборы различны, то $\exists\alpha_{i_1} = \ldots = \alpha_{i_k} = 0$ и $\beta_{i_1} = \ldots = \beta_{i_k} = 1$,
а $\forall j \in (1, \ldots, n) \setminus (i_1, \ldots, i_k)$ $\alpha_j = \beta_j$.
Пусть наборы $\tilde{\gamma}_0, \ldots, \tilde{\gamma}_k$ с номерами $(1, \ldots, n)\setminus(i_1, \ldots, i_k)$ совпадают с набором $\tilde{\alpha}$, набор γ_j на позициях с номерами $i_1, \ldots, i_j$ принимает значение 1, а на позициях $i_{j+1}, \ldots, i_k$ принимает значение 0, тогда $\tilde{\gamma}_0 = \tilde{\alpha}$, а $\tilde{\gamma}_k = \tilde{\beta} \Longrightarrow f(\tilde{\gamma}_0) = 1$, $f(\tilde{\gamma}_k) = 0 \Longrightarrow \exists\tilde{\gamma}_j : f(\tilde{\gamma}_j) = 0$, а $f(\tilde{\gamma}_{j-1}) = 1 \Longrightarrow$
$\Longrightarrow \tilde{\gamma}_{j-1} = (\delta_1, \ldots, \delta_{i_j-1}, 0, \delta_{i_j+1}, \ldots, \delta_n)$, $\tilde{\gamma}_j = (\delta_1, \ldots, \delta_{i_j-1}, 1, \delta_{i_j+1}, \ldots, \delta_n)$.
Тогда функция $\varphi(f(\delta_1, \ldots, \delta_{i_j-1}, x, \delta_{i_j+1}, \ldots, \delta_n))$, при $x = 0$ функция равна 1, а при $x = 1$, функция равна 0, то есть $\varphi = \overline{x}$, а так как она получена с помощью функции f и констант, значит, это искомая функция. $\square$

10 Билет 10 (Класс L и лемма, связанная с ним)

Определение. Функция f называется линейной, если она представима полиномом Жегалкина степени 1.

Теорема. *Класс L линейных функций замкнут.*

Доказательство. 1. Операция подстановки переменных:
$g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, если функция f линейна, то $\forall \tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ $f(\tilde{\alpha}) = c_0 + c_1\alpha_1 + \ldots + c_n\alpha_n$, тогда
$g(\alpha_1, \ldots, \alpha_n) = c_0 + c_1\alpha_{i_1} + \ldots + c_n\alpha_{i_n} \Longrightarrow g$ - линейная функция.

2. Операция подстановки одной функции в другую:
$f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m)$ - линейные функции, $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, так как функции f и g линейны, $\forall \tilde{\alpha} = (\alpha_1, \ldots, \alpha_{m+n-1})$ $f(\alpha_1, \ldots, \alpha_n) = c_0 + c_1\alpha_1 + \ldots + c_n\alpha_n$, $g(\alpha_1, \ldots, \alpha_m) = c'_0 + c'_1\alpha_1 + \ldots + c'_n\alpha_n \Longrightarrow$
$\Longrightarrow h(\alpha_1, \ldots, \alpha_{n+m-1}) = c_0 + c_1\alpha_1 + \ldots + c_{n-1}\alpha_{n-1} + c_n g(\alpha_n, \ldots, \alpha_{m+n-1}) =$
$= c_0 + c_1\alpha_1 + \ldots + c_{n-1}\alpha_{n-1} + c_n(c'_1\alpha_n + \ldots + c'_m\alpha_{m+n-1}) \Longrightarrow$ функция h является линейной.

3. Операция добавления или удаления фиктивных переменных:
$f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$, так как f линейна $\Longrightarrow \forall \tilde{\alpha} = (\alpha_1, \ldots, \alpha_{i-1}, \alpha_{i+1}, \ldots, \alpha_n)$ $f(\tilde{\alpha}) = c_0 + c_1\alpha_1 + \ldots + c_{i-1}\alpha_{i-1} + c_{i+1}\alpha_{i+1} + \ldots + c_n\alpha_n$, тогда очевидно, что $g(\alpha_1, \ldots, \alpha_{i-1}, 0, \alpha_{i+1}, \ldots, \alpha_n)$ тоже линейная функция.

Следовательно, суперпозициями мы не сможем получить функцию, не принадлежащую данному классу $\Longrightarrow$ класс L замкнут. □

Теорема. *Если функция f нелинейна, то из неё, констант и отрицания можно получить конъюнкцию.*

Доказательство. Пусть $f(x_1, \ldots, x_n)$ - нелинейная функция, тогда полином Жегалкина без ограничения общности имеет вид: $x_1x_2f_1(x_3, \ldots, x_n) + x_1f_2(x_3, \ldots, x_n) + x_2f_3(x_3, \ldots, x_n) + f_4(x_3, \ldots, x_n)$. Так как $f1$ не является тождественно нулевой функцией, существует набор $(\alpha_3, \ldots, \alpha_n) : f_1(\alpha_3, \ldots, \alpha_n) = 1$, тогда $f = x_1x_2 + \alpha x_1 + \beta x_2 + \gamma \Longrightarrow$
$\Longrightarrow f(x_1+\alpha, x_2+\beta) = (x_1+\alpha)(x_2+\beta)+\alpha(x_1+\alpha)+\beta(x_2+\beta)+\gamma = x_1x_2+\alpha\beta\gamma$, если $\alpha\beta\gamma = 1$, то возьмём $\overline{f}(x_1+\alpha, x_2+\beta) = x_1x_2$, так как данная функция получена из f с помощью констант и отрицания, значит, это искомая функция. □

11 Билет 11 (Теорема Поста)

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

Доказательство. $\Longrightarrow$ Если ситсема F функций алгебры логики полна, то $[F] = P_2$. Предположим, что $F \subseteq K$, где K - один из этих классов, тогда $[F] \subseteq [K] \neq P_2$ - противоречие.
$\Longleftarrow$ Пусть F не лежит ни в одном из этих классов, тогда $\exists f_1,\ f_2,\ f_3,\ f_4,\ f_5 : f_1 \notin T_0,\ f_2 \notin T_1,\ f_3 \notin S,\ f_4 \notin M,\ f_5 \notin L$.
Рассмотрим $f_1 \notin T_0$, тогда $f_1(0, \ldots, 0) = 1$. Есть два случая:

1. Пусть $f_1 \notin T_1$, тогда $\varphi(x) = f_1(x, \ldots, x) = \overline{x}$, то есть мы получили из f_1 функцию отрицания. Тогда по лемме о несамодвойственной функции из f_3 и $\overline{x}$ можно получить константы.

2. Пусть $f_1 \in T_1$, тогда $\varphi(x) = f_1(x, \ldots, x) = 1$, то есть $\varphi(x)$ - константа 1. Рассмотрим $f_2 \notin T_1$, тогда $f_2(f_1(x, \ldots, x)) = 0$, то есть мы получили константу 0.

Тогда по лемме о немонотонной функции из f_4 и констант можно получить $\overline{x}$, а по лемме о нелинейной функции из f_5, $\overline{x}$ и констант можно получить $x \wedge y$, то есть мы получим полную систему $x \wedge y$, $\overline{x}$. $\square$

12 Билет 12 (Теорема о предполных классах)

Определение. Класс K функций алгебры логики называется предполным, если $[K] \neq P_2$ и если $f \in P_2 \setminus K$, то $[\{f\} \cup K] = P_2$.

Теорема. *В P_2 нет предполных классов, отличных от T_0, T_1, S, M, L.*

Доказательство. Пусть класс K - предполный класс, отличный от данных пяти классов. Этот класс замкнут, так как в противном случае можно было бы выбрать функцию $f : f \in [K]$ и $f \notin K$, тогда $[\{f\} \cup K] = [K]$, но так как класс K является предполным, то $[K] = P_2 \Longrightarrow$ противоречие с тем, что класс K не является полным.
Так как класс K замкнут, то он содержится в одном из классов T_0, T_1, S, M, L (обозначим этот класс Q), иначе по теореме Поста он был бы полным, а он по условию таким не является. Пусть класс K не совпадает с классом Q, тогда

$\exists f \in Q \setminus K \Longrightarrow [\{f\} \cup K] \subseteq [Q] \neq P_2$ - противоречие.
Пусть $f \in P_2 \setminus Q$, тогда если $[Q \cup \{f\}] = [Q'] \neq P_2$, то Q' содержится в одном из оставшихся классов, что невозможно, а значит, класс Q является предполным. □

13 Билет 13 (Теорема о конечной полной подсистеме полной системы в P_2)

Теорема. *В любой полной системе алгебры логики можно выделить полную подсистему, состоящую из 4 функций.*

Доказательство. Пусть система F полна, выберем в ней функции f_1, f_2, f_3, f_4, $f_5 : f_1 \notin T_0$, $f_2 \notin T_1$, $f_3 \notin S$, $f_4 \notin M$, $f_5 \notin L$, по теореме Поста система из этих функций полна. Если $f_1 \in T_1$, тогда $f_1 \notin S$, тогда функцию f_3 можно выбрать равной f_1, а если $f_1(1, \ldots, 1) = 0$, то $f_1 \notin M$, то есть f_4 можно выбрать равной $f_1 \Longrightarrow$ в обоих случаях мы получаем полную систему из четырёх функций. □

14 Билет 14 (Базис в P_k)

Определение. Пусть K - замкнутый класс, F - система функций данного класса, тогда F называется полной, если $[F] = K$.

Определение. Система функций некоторого класса K называется базисом, если она полна в K, но каждая её собствееная подсистема неполна в K.

Примеры. $\{0, 1, x_1 \cdot x_2, x_1 \vee x_2\}$ - базис в M

Теорема. *Каждый замкнутый класс функций алгебры логики имеет конечный базис. (Без доказательства)*

Теорема. *Число замкнутых классов в P_2 счётно. (Без доказательства)*

15 Билет 15 (Основные определения в P_k)

Определение. Отображение $f : E_k \times \ldots \times E_k \to E_k$ - функция k-значной логики.

Элементарные функции:

1. $\overline{x} = x + 1 (mod\ k)$

2. $\sim x = k - 1 - x$

3. $J_i(x) = \begin{matrix} k-1, \text{если} x = i \\ 0, \text{если} x \neq i \end{matrix}$

4. $j_i(x) = \begin{matrix} 1, \text{если} x = i \\ 0, \text{если} x \neq i \end{matrix}$

5. $min(x_1,\, x_2)$

6. $max(x_1,\, x_2)$

7. $x_1 \cdot x_2 (mod\ k)$

8. $x_1 + x_2 (mod\ k)$

Определение. Отображение $\Sigma : S \to F$, где S - множество символов, обозначуюющих функции из P_k, а F - множество функций в P_k, называется сигнатурой.

Определение. База индукции: пусть x_i - символ переменной, тогда однобуквенное слово, состоящее из x_i - формула в сигнатуре.
Пусть $s \in S$, $f = \Sigma(s)$ - функция от n переменных, Φ_1, …, Φ_n - формулы в сигнатуре Σ, тогда слово $s(\Phi_1, \ldots, \Phi_n)$ - формула в сигнатуре Σ.

Определение. Пусть Φ - формула, $\tilde{x} = (x_{i_1}, \ldots, x_{i_n})$ - упорядоченный набор, содержащий все переменные формулы Φ, $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$ - двоичный набор.
База индукции: Φ - однобуквенное слово x_{i_j}, тогда $\Phi[\tilde{x},\, \tilde{\alpha}] = \alpha_j$ - значение формулы на наборе.
Пусть $s \in S$, $f = \Sigma(s)$, Φ_1, …, Φ_n - формулы в сигнатуре. Обозначим $\Phi_1[\tilde{x}, \tilde{\alpha}] = \beta_1, \ldots, \Phi_n[\tilde{x},\, \tilde{\alpha}] = \beta_n$, тогда $f(\beta_1, \ldots, \beta_n)$ - значение формулы на наборе $\tilde{\alpha}$.

Определение. Операции:

1. Операция подстановки переменных. Пусть $f(x_1, \ldots, x_n) \in P_k$, $g(x_1, \ldots, x_n)$ - функция, определённая на B_n, такая, что $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, где набор $(i_1, \ldots, i_n)$ - набор элементов $(1, \ldots, n)$ (они необязательно различны). Тогда g получена из f операцией подстановки переменных.

2. Операция подстановки функции в функцию. Пусть $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_m)$, h определена на B_{n+m-1} и $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{n+m-1}))$, тогда функция h получена из функций f и g операцией подстановки одной функции в другую.

3. Операция добавления или удаления фиктивных переменных. Пусть x_i - фиктивная переменная, тогда если функция $f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n) = g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$, то функция g называется полученной из f добавлением фиктивной переменной. Функция удаления фиктивной переменной определяется аналогично.

16 Билет 16 (Простейшие тождества для функций и аналог совершенной д.н.ф. в P_k)

Тождества для функций в P_k:

1. операции $min(x_1, x_2)$, $max(x_1, x_2)$, $x_1 \cdot x_2 (mod\ k)$, $x_1 + x_2 (mod\ k)$ ассоциативны и коммутативны
2. $min(max(x_1, x_2), x_3) = max(min(x_1, x_3), min(x_2, x_3))$
3. $(x_1 + x_2) \cdot x_3 = (x_1 \cdot x_3) + (x_2 \cdot x_3)$
4. $\sim (\sim x) = x$
5. $\sim min(x_1, x_2) = max(\sim x_1, \sim x_2)$

Определение. Выражение $\bigvee\limits_{(\sigma_1, \ldots, \sigma_n) \in (E_k)^n} min(J_{\sigma_1}(x_1), \ldots, J_{\sigma_n}(x_n), f(\sigma_1, \ldots, \sigma_n))$ - аналог совершенной дизъюнктивной нормальной формы для P_k.

Теорема. *Любая функция, не являющаяся тождественно нулевой, имеет аналог совершенной д.н.ф.*

Доказательство. Рассмотрим произвольный набор $(\alpha_1, \ldots, \alpha_n)$, так как $J_{\sigma_i}(\alpha_j) = 0\ \forall j \neq i$, а для $j = i$ $J_{\sigma_i}(\alpha_i) = k - 1$, значит, все члены, кроме $\alpha_1 = \sigma_1, \ldots, \alpha_n = \sigma_n$, будут равны нулю, а значит, останется только $min(J_{\sigma_1}(\alpha_1), \ldots, J_{\sigma_n}(\alpha_n), f(\alpha_1, \ldots, \alpha_n)) = f(\alpha_1, \ldots, \alpha_n)$. □

17 Билет 17 (Полные системы в P_k)

Определение. Система F функций в P_k называется полной, если любая функция из P_k получается суперпозициями из F.

Примеры. 1. P_k

2. $\{0, 1, \ldots, k-1, J_0(x), \ldots, J_{k-1}(x), min(x_1, x_2), max(x_1, x_2)\}$

3. $max(x_1, x_2), \overline{x}$

4. $min(x_1, x_2), \overline{x}$

5. $\{0, 1, \ldots, k-1, j_0(x), \ldots, j_{k-1}(x), x_1 + x_2, x_1 \cdot x_2\}$

6. $V_k(x_1, x_2) = max(x_1, x_2) + 1(mod\ k)$

Докажем полноту каждой из систем.

Доказательство. 1. Так как в системе есть отрицание Поста, то из $\forall x$ можно получить $\{x, x+1, \ldots, x+k-1\}$ все эти числа различны по $(mod\ k) \Longrightarrow max(x, \ldots, x+k-1) = k-1$, тогда из константы $k-1$ можно получить все остальные константы, используя отрицание Поста.
Рассмотрим набор $\{x, \ldots, x+j-1, x+j+1, \ldots, x+k-1\}$, тогда функция $\varphi_j(x) = max(x, \ldots, x+j-1, x+j+1, \ldots, x+k-1) = \begin{cases} k-1, \text{ при} x+j \neq k-1 \\ k-2, \text{ при} x+j = k-1 \end{cases}$. Тогда функция $\psi_j(x) = max(x, \ldots, x+j-1, x+j+1, \ldots, x+k-1) + 1$ (это можно сделать благодаря отрицанию Поста) $\Longrightarrow \psi_j(x) = \begin{cases} 0, \text{ при} x+j \neq k-1 \\ k-1, \text{ при} x+j = k-1 \end{cases}$. То есть мы получили все константы, $J_i(x)\ \forall i$, а значит, получили полную систему из примера 2.

2. Аналогично с предыдущим пунктом, с помощью отрицания Поста можно получить все константы, а значит, можем получить отрицание Лукашевича, а по одному из тождеств, $\sim min(x_1, x_2) = max(\sim x_1, \sim x_2)$, то есть мы получили полную систему из предыдущего пункта.

3. Из $V_k(x_1, x_2)$ получим отрицание Поста: $V_k(x, x) = x + 1 = \overline{x} \Longrightarrow$ можно получить $x + i\ \forall i$, тогда $max(x_1, x_2) = V_k(x_1, x_2) + k - 1$, то есть мы получили полную систему $\{max(x_1, x_2), \overline{x}\}$.

□

18 Билет 18 (Замыкание и замкнутые классы в P_k)

Определение. Замыканием множества F в P_k называется множество всех функций, которые можно получить суперпозициями из F.

Определение. Если $[F] = F$, то множество F называется замкнутым.

Определение. Пусть $Q \subseteq E_k$. Множество функций $T_Q : \forall \alpha_1, \ldots, \alpha_n \in Q\ f(\alpha_1, \ldots, \alpha_n) \in Q$, называется функцией, сохраняющей множество Q.

Примеры. 1. P_k

2. T_Q

Теорема. *Класс T_Q замкнут.*

Доказательство. 1. Операция подстановки переменных:
Пусть функция $f(x_1, \ldots, x_n)$ сохраняет множество Q, тогда $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$ тоже будет сохранять множество Q, так как при перестановке одинаковых переменных ничего не поменяется.

2. Операция подстановки функции в функцию:
Пусть функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_m)$ сохраняют множесво Q, тогда $h(x_1, \ldots, x_{m+n-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{m+n-1}))$, так как функция g сохраняет множество $Q \Longrightarrow$ все переменные f принимают одно и то же значение, а значит, и функция h будет сохранять множество Q.

3. Операция добавления или удаления фиктивных переменных:
Очевидно.

□

19 Билет 19 (Последовательность Кузнецова и алгоритм, связанный с ней)

Определение. Определим глубину формулы через индукцию по определению формулы в сигнатуре:
База индукции: пусть x_i - символ переменной, тогда глубина формулы x_i равна 0.
Пусть $s \in S$, $f = \Sigma(s)$, $\Phi_1, \ldots, \Phi_n$ - формулы в сигнатуре, причём m - наибольшая из глубин этих формул, тогда глубина формулы $s(\Phi_1, \ldots, \Phi_n)$ равна $m + 1$.

Теорема. *Существует алгоритм, распознающий полноту конечных систем функций в P_k. Он заключается в построении последовательности Кузнецова и проверке вхождения в её предел функции Вебба.*

Доказательство. Пусть $F \subseteq P_k$ - конечное множество функций в P_k, $\Sigma : S \to F$ - сигнатура. Рассмотрим последовательность G_1, G_2, $\ldots$ такую, что G_i - множество функций, определяемых невырожденными формулами в сигнатуре Σ, содержащими только переменные x_1, x_2 и имеющими глубину, меньшую i. Данную последовательность назовём последовательностью Кузнецова. Так как все формулы в соответствующем множестве G_i имеют глубину, меньшую $i \Longrightarrow \varnothing \subseteq G_1 \subseteq \ldots$. Так как число функций в P_k от двух переменных равно k^{k^2} $\Longrightarrow |G_i| \leqslant k^{k^2} \Longrightarrow$ последовательность Кузнецова стабилизируется на некотором шаге $G_m = G$, G называется пределом последовательности Кузнецова. Свяжем с каждой функцией из G_i некоторую формулу Φ'_j, содержащую только переменные x_1, x_2 и имеющую глубину, меньшую i. Рассмотрим функцию $f \in G_{i+1} \setminus G_i$, она определяется формулой $\Phi = s(\Phi_1, \ldots, \Phi_n)$, где формулы Φ_1, $\ldots$, Φ_n либо являются переменными, либо определяют некоторые функции в G_i, но эти функции мы уже определили формулами Φ'_j, тогда елси заменить в формуле Φ формулы Φ_j на Φ'_j, то мы получим формулу Φ', определяющую ту же самую функцию $f \Longrightarrow$ для получения из G_i G_{i+1} достаточно рассмотреть все формулы Ф'= $s(\Phi'_1, \ldots, \Phi'_n)$. Значит данную последовательность имеет смысл проверять до первого совпадения G_i и G_{i+1}.

Лемма. *Система функций в P_k полна тогда и только тогда, когда в предел последовательности входит функция Вебба.*

Доказательство. $\underline{\Longleftarrow}$ Пусть $V_k(x_1, x_2) \in G$, тогда функция Вебба получается суперпозициями из функций данной системы $\Longrightarrow$ эта система полна.
$\underline{\Longrightarrow}$ Пусть система функций F полна, тогда функция Вебба определяется некоторой формулой в сигнатуре Σ, существенно зависящей от двух переменных и имеющей глубину, меньшую i, то есть $V_k \in G_i$, переобозначим переменные так, чтобы существенными стали только переменные x_1, x_2, а все остальные несущественные переменные заменим на x_1, тогда эта формула определяет функцию из G_{i+1} (так как она получена из формул, сопоставленных функциям из G_i) $\Longrightarrow V_k \in G_{i+1} \Longrightarrow V_k \in G$. □

□

20 Билет 20 (Теорема о существовании конечной полной подсистемы в полной системе в k-значной логике)

Теорема. *Из любой полной системы функций в P_k можно выделить конечную полную подсистему.*

Доказательство. Пусть F - полная система в P_k, тогда суперпозициями из F можно получить функцию Вебба, то есть полную подсистему, а так как она получается суперпозициями из конечного числа функций, значит, подсистема из этих функций конечна и полна. $\square$

21 Билет 21 (Селекторные функции, класс функций, сохраняющих множество K, его замкнутость)

Определение. Функции $g_i^p(x_1, \ldots, x_p) = x_i$, где $i = \overline{1, p}$, называются селекторными функциями.

Определение. Пусть K - множество функций $h(x_1, \ldots, x_p)$, зависящих от p переменных и содержащих все селекторные функции от p переменных. Если для любых функций $h_1(x_1, \ldots, x_p), \ldots, h_n(x_1, \ldots, x_p)$ функция $f(h_1, \ldots, h_n) \in K$, то скажем, что функция f сохраняет множество K.

Рассмотрим класс функций в алгебре логики, сохраняющих множество $K = \{x, \overline{x}\}$, то есть в K входят функции $\{x^\sigma\}$, где $\sigma = \{0, 1\}$. Тогда функция f сохраняет K, если $f(x_1^{\sigma_1}, \ldots, x_n^{\sigma_n}) = x^\sigma$, то есть

$$\begin{cases} f(1^{\sigma_1}, \ldots, 1^{\sigma_n}) = 1^\sigma = \sigma = f(\sigma_1, \ldots, \sigma_n) \\ f(0^{\sigma_1}, \ldots, 0^{\sigma_n}) = 0^\sigma = \overline{\sigma} = f(\overline{\sigma}_1, \ldots, \overline{\sigma}_n) \end{cases}$$

$\Longrightarrow f(\sigma_1, \ldots, \sigma_n) = \overline{f(\overline{\sigma}_1 \ldots \overline{\sigma}_n)}$, то есть мы получили класс S самодвойственных функций.

Определение. Множество всех функций, сохраняющих множество K, называется классом сохранения множества K. Данный класс обозначим $U(K)$.

Теорема. *Класс $U(K)$ замкнут.*

Доказательство. 1. Опреация подстановки переменных:
Пусть функция f сохраняет множество K, тогда функция $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, $f(h_1(x_1, \ldots, x_p), \ldots, h_n(x_1, \ldots, x_p)) \in K$ $\forall h_1, \ldots, h_n \in K$, а значит, $f(h_{i_1}(x_1, \ldots, x_p), \ldots, h_{i_n}(x_1, \ldots, x_p)) \in K \implies g$ сохраняет множество K.

2. Операция подстановки функции в функцию:
Аналогично с предыдущим пунктом.

3. Операция добавления или удаления фиктивных переменных:
Пусть $f(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ сохраняет множество K, $g(x_1, \ldots, x_{i-1}, 0, x_{i+1}, \ldots, x_n)$ получена из f добавлением фиктивной переменной, тогда g будет сохранять множество K, так как при подстановке функций $h_j(x_1, \ldots, x_p)$ в функцию g мы получим $g(h_1(x_1, \ldots, x_p), \ldots, h_{i-1}(x_1, \ldots, x_p), 0, h_{i+1}(x_1, \ldots, x_p), \ldots, h_n(x_1, \ldots, x_p)) = f(h_1(x_1, \ldots, x_p), \ldots, h_{i-1}(x_1, \ldots, x_p), h_{i+1}(x_1, \ldots, x_p), \ldots, h_n(x_1, \ldots, x_p)) \in K$.

Значит, суперпозициями мы не сможем получить функцию, не сохраняющую множество K. □

22 Билет 22 (Лемма о неполноте системы F, если $F \subseteq U(K)$ и $V_k \notin U(K)$)

Теорема. *Класс функций $U(K)$ не является полным, если множество K не содержит функцию Вебба.*

Доказательство. Пусть F - множество функций, сохраняющих множество K, содержащее все селекторные функции и не содержащее функцию Вебба, Σ - сигнатура для F, тогда рассмотрим последовательность Кузнецова G_1, G_2, ... и докажем по индукции, что $G \subseteq K$.
База индукции: $\varnothing \subseteq K$.
Пусть $G_i \subseteq K$, докажем для G_{i+1}. Рассмотрим функцию $h \in G_{i+1} \setminus G_i$, она задаётся формулой $s(A_1, \ldots, A_n)$, где $\Sigma(s) \in F$, A_j либо является функцией из G_i, глубина которой меньше i, либо является переменной x_1, либо является переменной x_2. В первом случае A_j задаёт некоторую функцию $h_j(x_1, x_2) \in G_i$, во втором случае $h_j(x_1, x_2) = g_1^2(x_1, x_2)$, в третьем случае $h_j(x_1, x_2) = g_2^2(x_1, x_2)$. Так как $G_i \subseteq K$, значит, $\forall j$ $A_j \in K$, а значит, $G_{i+1} \subseteq K$. А так как K не содержит функцию Вебба, по критерию K неполно. □

23 Билет 23 (Существование для неполной системы F множества K такого, что $V_k \notin K$ и $F \subseteq U(K)$)

Теорема. *Если система функций F в k-значной логике не является полной, то в P_k существует множество K функций от двух переменных, содержащее обе селекторные функции и не содержащее функцию Вебба, такое, что $F \subseteq U(K)$.*

Доказательство. Пусть F - система функций в k-значной логике, Σ - сигнатура для F. Рассмотрим последовательность Кузнецова $G_1, G_2, \ldots$. Пусть $G_m = G_{m+1}$, так как F неполна $\Longrightarrow V_k \notin F$. Пусть $K = G_m \cup \{g_1^2, g_2^2\}$. Так как V_k не является селекторной функцией и $V_k \notin G_m \Longrightarrow V_k \notin K$. Пусть $f(x_1, \ldots, x_n) \in F$, $h_1, \ldots, h_n \in K$. Рассмотрим $f(h_1(x_1, x_2), \ldots, h_n(x_1, x_2))$. Пусть s - символ для f в сигнатуре Σ. Если $h_j(x_1, x_2) \in G_m$, то эта функция определяется в сигнатуре Σ формулой A_j, глубина которой меньше m, если $h_j(x_1, x_2) = g_1^2(x_1, x_2)$, то возьмём в качестве A_j x_1, если $h_j(x_1, x_2) = g_2^2(x_1, x_2)$, то возьмём в качестве A_j x_2. Тогда функция $f(h_1(x_1, x_2), \ldots, h_n(x_1, x_2))$ определяется формулой $s(A_1, \ldots, A_n)$, глубина которой меньше $m + 1$, значит, функция реализующая эту формулу, $h(x_1, x_2) \in G_{m+1} = G_m \subseteq K \Longrightarrow h \in K \Longrightarrow F$ сохраняет множество K и $F \subseteq U(K)$. □

24 Билет 24 (Теорема Кузнецова о предполных классах в k-значной логике)

Теорема. *В P_k можно построить замкнутые классы $M_1, \ldots, M_s$ такие, что ни один из них не содержится в других и произвольная система $F \subseteq P_k$ полна тогда и только тогда, когда F не содержится ни в одном из этих классов.*

Доказательство. Рассмотрим все классы $N_1, \ldots, N_q$ вида $U(K)$, где K - множество функций от двух переменных, содержащее обе селекторные функции и не содержащее функцию Вебба. По лемме 1 они замкнуты. Пусть $F \subseteq P_k$ неполна, тогда по лемме 3 существует класс N_i такой, что $F \subseteq N_i$, тогда по лемме 2, множество F неполно $\Longrightarrow$ полнота системы эквивалентна невключению её ни в один из классов $N_1, \ldots, N_q$, удалив из них те, которые содержатся в других, получим искомую систему классов $M_1, \ldots, M_s$. □

25 Билет 25 (Лемма о трёх наборах)

Определение. Функция $f \in P_k$ называется существенной, если она имеет больше одной существенной переменной.

Теорема. *Пусть $f(x_1, \ldots, x_n)$ - существенная функция, принимающая l значений, где $l \geqslant 3$, и пусть x_1 - её существенная переменная, тогда существуют наборы $(\alpha, \alpha_2, \ldots, \alpha_n)$, $(\beta, \alpha_2, \ldots, \alpha_n)$, $(\alpha, \gamma_2, \ldots, \gamma_n)$, на которых она принимает три различных значения.*

Доказательство. Так как переменная x_1 является существенной, существуют значения $\alpha_2, \ldots, \alpha_n$ такие, что в следующем списке S: $f(0, \alpha_2, \ldots, \alpha_n)$, $f(1, \alpha_2, \ldots, \alpha_n)$, $\ldots$, $f(k-1, \alpha_2, \ldots, \alpha_n)$ - есть более одного значения. Рассмотрим два случая:

1. В S меньше чем l значений, тогда найдём набор, на котором функция f принимает значение, не встречающееся в S, обозначим этот набор $(\alpha, \gamma_2, \ldots \gamma_n)$. $f(\alpha, \gamma_2, \ldots \gamma_n) \neq f(\alpha, \alpha_2, \ldots \alpha_n)$, так как $f(\alpha, \gamma_2, \ldots \gamma_n) \notin S$, $f(\alpha, \gamma_2, \ldots \gamma_n) \neq f(\beta, \alpha_2, \ldots \alpha_n)$, где набор $(\beta, \alpha_2, \ldots \alpha_n) \neq f(\alpha, \alpha_2, \ldots \alpha_n)$.

2. В S ровно l значений, тогда существует такое α, что $f(\alpha, x_2, \ldots x_n)$ - не константа $\Longrightarrow \exists(\alpha, \alpha_2, \ldots \alpha_n) \neq (\alpha, \gamma_2, \ldots \gamma_n)$. Так как $l \geqslant 3$ $\exists\beta$ такое, что $(\beta, \alpha_2, \ldots \alpha_n) \neq (\alpha, \alpha_2, \ldots \alpha_n) \neq (\alpha, \gamma_2, \ldots \gamma_n)$.

□

26 Билет 26 (Лемма о подмножестве $G_1 \times \ldots \times G_n$, на котором функция принимает хотя бы l значений)

Теорема. *Если $f(x_1, \ldots, x_n)$ - существенная функция в P_k, принимающая хотя бы l значений, где $l \geqslant 3$, тогда существуют подмножества $G_1, \ldots, G_n$ множества E_k такие, что $1 \leqslant |G_1| \leqslant l-1, \ldots, 1 \leqslant |G_n| \leqslant l-1$, причём на множестве $G_1 \times \ldots \times G_n$ функция принимает хотя бы l значений.*

Доказательство. Без ограничения общности будем считать, что x_1 - существенная переменная. По лемме о трёх наборах существуют наборы $(\alpha, \alpha_2, \ldots \alpha_n)$, $(\beta, \alpha_2, \ldots \alpha_n)$, $(\alpha, \gamma_2, \ldots \gamma_n)$, на которых функция принимает три различных значения. Пусть остальные $l-3$ значения функция принимает на наборах $\delta_i = (\delta_{i1},$

$\ldots\ \delta_{in})$, тогда в качестве G_1 выберем набор $(\alpha,\ \beta,\ \delta_{11},\ \ldots\ \delta_{l-3,1})$, в качестве G_2, ..., G_n выберем наборы $(\alpha_2,\ \gamma_2,\ \delta_{12},\ \ldots\ \delta_{l-3,2})$, ..., $(\alpha_n,\ \gamma_n,\ \delta_{1n},\ \ldots\ \delta_{l-3,n})$. Каждое из G_j непусто и в каждом не больше $l-1$ элемента, а значит, мы получили искомые множества. $\square$

27 Билет 27 (Лемма о квадрате)

Определение. Четвёрка наборов $\{(\alpha_1,\ \ldots,\ \alpha_{i-1},\ x,\ \alpha_{i+1},\ \ldots,\ \alpha_{j-1},\ y,\ \alpha_{j+1},\ \ldots,\ \alpha_n) | x \in \{p_1,\ p_2\},\ y \in \{q_1,\ q_2\}\}$ называется квадратом в P_k.

Теорема. *Пусть $f(x_1,\ \ldots,\ x_n)$ - существенная функция в P_k, принимающая l значений, причём $l \geqslant 3$. Тогда существует квадрат, на котором f принимает некоторое своё значение ровно в одной точке.*

Доказательство. Без ограничения общности будем считать, что x_1 - существенная переменная, тогда по лемме о трёх наборах существуют наборы $(\alpha,\ \alpha_2,\ \ldots,\ \alpha_n)$, $(\beta,\ \alpha_2,\ \ldots,\ \alpha_n)$, $(\alpha,\ \gamma_2,\ \ldots,\ \gamma_n)$, на которых функция принимает три различных значения. Рассмотрим последовательность пар:

$$P_1 = \{(\alpha, \alpha_2, \ldots, \alpha_n), (\beta, \alpha_2, \ldots, \alpha_n)\}$$
$$P_2 = \{(\alpha, \gamma_2, \alpha_3, \ldots, \alpha_n), (\beta, \gamma_2, \alpha_3, \ldots, \alpha_n)\}$$
$$\vdots$$
$$P_i = \{(\alpha, \gamma_2, \ldots, \gamma_i, \alpha_{i+1}, \ldots, \alpha_n), (\beta, \gamma_2, \ldots, \gamma_i, \alpha_{i+1}, \ldots, \alpha_n)\}$$
$$\vdots$$
$$P_n = \{(\alpha, \gamma_2, \ldots, \gamma_n), (\beta, \gamma_2, \ldots, \gamma_n)\}$$

На наборах пары P_1 функция принимает значения a и b, на первом наборе пары P_n функция принимает значение, отличное от a и b, а на втором наборе она может принимать одно из значений либо a, либо b, но не оба. Значит, существуют пары P_i и P_{i+1} такие, что на наборах пары P_i функция приниает оба значения a и b, а на наборах пары P_{i+1} функция не принимает одно из этих значений. Заметим, что наборы из пар P_i и P_{i+1} образуют квадрат в P_k, причём одно из значений a и b, которое функция не принимает на наборах пары P_{i+1}, и будет искомым значением, которое функция принимает ровно в одной точкче. $\square$

28 Билет 28 (Теорема Слупецкого, теорема Яблонского, теорема Мартина)

Теорема. *Пусть F - система функций в P_k, где $k \geqslant 3$, содержащая все функции одной переменной. Тогда для полноты F необходимо и достаточно, чтобы* *она содержала существенную функцию, принимающую все k значений.*

Доказательство. $\Longrightarrow$ Пусть F не содержит функцию, принимающую все k значений, тогда проверим, сможем ли мы получить суперпозициями из F функцию, принимающую все k значений:

1. Операция подстановки переменных:
   Пусть $f \in F$ и $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, тогда, если f является существенной и не принимает все k значений, то и g будет существенной функцией, не принимающей все k значений. Если f не является существенной, то есть f имеет единственную существенную переменную x_j, но тогда и функция g будет иметь единственную существенную переменную x_{i_j}.

2. Операция подстановки функции в функцию:
   Пусть $f,\ g \in F$ и $h(x_1, \ldots, x_{m+n-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{m+n-1}))$, тогда если функции f и g являются существенными и не принимают все k значений, то и h их не принимает. Если функция f принимает все k значений и не является существенной, то она имеет одну существенную переменную x_j. Если $j \neq n$, то она будет единственной сущесвенной переменной у функции h. Пусть $j = n$, тогда если функция g не принимает все k значений, то и функция не будет принимать все k значений. Если g принимает все k значений, то она не является существенной, а значит, содержит ровно одну существенную переменную $\Longrightarrow$ h тоже содержит ровно одну существенную перемнную, то есть функция h не является сущетвенной.

3. Операция добавления или удаления несущественных переменных:
   Если функция не была существенной, то при добавлении несущественной переменной, она не может стать существенной. Если функция была существенной и не принимала все k значений, то при добавлении фиктивной переменной, количество принимаемых ею значений не изменится, так как она от этой переменной существенно не зависит.

Значит, суперпозициями мы не сможем получить существенную функцию, принимающую все k значений, то есть система F неполна.
$\Longleftarrow$ Пусть F имеет существенную функцию $f(x_1, \ldots, x_n)$, принимающую все k значений, тогда по лемме о квадрате существует квадрат $\{(\alpha_1, \ldots, \alpha_{i-1}, x, \alpha_{i+1}, \ldots, \alpha_{j-1}, y, \alpha_{j+1}, \ldots, \alpha_n) | x \in \{p_1, p_2\},\ y \in \{q_1, q_2\}\}$, на котором функция f принимает некоторое своё значение a ровно в одной точке. $\varphi_0(x) =$

$\begin{cases} 0, & \text{при } x = a \\ 1, & \text{при } x \neq a \end{cases}$ Так как φ_0 зависит от одной переменной, то $\varphi_0 \in F$. Пусть функция g имеет вид: $g(x_1,\ x_2) = \varphi_0(f(\{(\alpha_1,\ \ldots,\ \alpha_{i-1},\ x_1,\ \alpha_{i+1},\ \ldots,\ \alpha_{j-1},\ x_2,\ \alpha_{j+1},\ \ldots,\ \alpha_n))$. Так как функция g на квадрате $\{(p_1,\ q_1),\ (p_1,\ q_2),\ (p_2,\ q_1),\ (p_2,\ q_2)\}$ принимает значения 0 и 1, причём 0 она принимает ровно в одной точке. Без ограничения общности будем считать, что $g(p_1,\ q_1) = 0$, а в остальных точках квадрата функция принимает значение 1.

База индукции: пусть $\varphi_1(x) = \begin{cases} p_1, & \text{при } x = 0 \\ p_2, & \text{при } x \neq 0 \end{cases}$, а $\varphi_2(x) = \begin{cases} q_1, & \text{при } x = 0 \\ q_2, & \text{при } x \neq 0 \end{cases}$, обе этих функции зависят от одной переменной. Пусть $g'(x_1,\ x_2) = g(\varphi_1(x_1),\ \varphi_2(x_2)) = \begin{cases} 0, & \text{при } x_1 = x_2 = 0 \\ 1, & \text{иначе} \end{cases}$, тогда эта функция совпадает с дизъюнкцией, если её аргументы ограничить множеством $\{0,\ 1\}$, обозначим эту функцию $x_1 \vee_{01} x_2$. Так как функция $j_i(x) = \begin{cases} 1, & \text{при } x = i \\ 0, & \text{при } x \neq i \end{cases}$ зависит от одной переменной $\Longrightarrow j_i(x) \in F$, причём $j_0(x) = \overline{x}$, если ограничить x на множество $\{0,\ 1\}$. Пусть $g''(x_1,\ x_2) = j_0(j_0(x_1) \vee_{01} j_0(x_2))$, она совпадает с конъюнкцией, если её ограничить на множество $\{0,\ 1\} \times \{0,\ 1\}$. Данную функцию обозначим $x_1 \wedge_{01} x_2$. Пусть $h(x_1,\ \ldots,\ x_n) \in P_k$, которая принимает только значения 0 и 1. Тогда благодаря совершенной д.н.ф. имеем:

$$h(x_1, \ldots, x_n) = \bigvee_{\sigma_1, \ldots, \sigma_n} j_{\sigma_1}(x_1) \wedge_{01} \ldots \wedge_{01} j_{\sigma_n}(x_n) \wedge_{01} h(\sigma_1, \ldots, \sigma_n).$$

Так как константы $h(\sigma_1, \ldots, \sigma_n)$ принадлежат F, то данная функция получена суперпозициями над F. Если функция $h(x_1,\ \ldots,\ x_n)$ - функция из P_k, принимающая только какие-то два значения a и b, то рассмотрим функцию $h'(x_1,\ \ldots,\ x_n) = \begin{cases} 0, & \text{если } h(x_1, \ldots, x_n) = a \\ 1, & \text{иначе} \end{cases}$ и функцию $\psi(x) = \begin{cases} a, & \text{если } x = 0 \\ b, & \text{иначе} \end{cases}$, тогда $h(x_1,\ \ldots,\ x_n) = \psi(h'(x_1,\ \ldots,\ x_n)) \Longrightarrow$ любая функция из P_k, принимающая не более двух значений, получается суперпозициями над F.

Шаг индукции: пусть все функции k-значной логики, принимающие не более чем $l - 1$ значение, получаются суперпозициями над F, докажем, что любая функция, принимающая l значений, тоже будет получаться суперпозициями над F. Рассмотрим существенную функцию $f(x_1,\ \ldots,\ x_n)$, принимающую все k значений, тогда по лемме 2 существуют подмножества $G_1,\ \ldots,\ G_n$ множества E_k такие, что $1 \geqslant |G_1| \geqslant l - 1,\ \ldots,\ 1 \geqslant |G_n| \geqslant l - 1$, причём на множестве

$G_1 \times \ldots \times G_n$ функция принимает хотя бы l значений. Обозначим эти l значений $a_1, \ldots, a_n$ и рассмотрим наборы из $G_1 \times \ldots \times G_n$, на которых f принимает эти l значений:

$$a_1 = f(a_{11}, ..., a_{1n})$$
$$\vdots$$
$$a_l = f(a_{l1}, ..., a_{ln})$$

Пусть функция $h(x_1, \ldots, x_m)$ принимает только значения $a_1, \ldots, a_l$, тогда рассмотрим произвольный набор $(\alpha_1, \ldots, \alpha_m)$ значений переменных $x_1, \ldots, x_m$. На этом наборе функция h принимает некоторое значение a_i. Зададим функции $\psi_1(\alpha_1, \ldots, \alpha_m), \ldots, \psi_n(\alpha_1, \ldots, \alpha_m)$, равные $a_{i1}, \ldots, a_{in}$. Тогда $f(\psi_1(\alpha_1, \ldots, \alpha_m), \ldots, \psi_n(\alpha_1, \ldots, \alpha_m)) = f(a_{i1}, \ldots, a_{in}) = a_i \Longrightarrow$ значения функций $\psi_1, \ldots, \psi_n$ определены для всех значений их аргументов, при этом $h(x_1, \ldots, x_m) \equiv f(\psi_1(x_1, \ldots, x_m), \ldots, \psi_n(x_1, \ldots, x_m))$ по построению. А так как все функции ψ_i принимают только значения из множества $\{a_{1i}, \ldots, a_{li}\}$, которые принадлежат множеству $G_i \Longrightarrow$ данные функции принимают не более чем $l-1$ значение, а по предположению индукции эти функции получаются суперпозициями над F, а значит, и функция h получается суперпозициями над F. То есть мы получили, что любая функция из P_k, принимающая только значения $a_1, \ldots, a_l$, получается суперпозициями над F. Если $l = k$, то все функции из P_k получаются суперпозициями над F.

Пусть $l < k$, тогда рассмотрим произвольную функцию $h \in P_k$, принимающую не более чем l значений. Пусть эти значения принадлежат списку $b_1, \ldots, b_l$. Рассмотрим $h' = \begin{cases} a_i, & \text{на некотором набооре} \\ b_i, & \text{на остальных наборах} \end{cases}$ и функцию

$$\psi = \begin{cases} b_i, & \text{если значение функции } h' = a_i \\ 0, & \text{на остальных наборах} \end{cases}$$

$\Longrightarrow h(x_1, \ldots, x_m) = \psi(h'(x_1, \ldots, x_m))$, а так как h' и ψ получаются суперпозициями над F, значит, функция h тоже. Значит, если $l = k$, то система F полна. $\square$

Теорема. *Пусть система F k-значной логики, где $k \geqslant 3$, содержит все функции одной переменной, принимающие не более $k-1$ значения, тогда для её полноты необходимо и достаточно, чтобы она содержала существенную функцию, принимающую все k значений.*

Доказательство. Данная теорема следует из доказательства теоремы Слупецкого, так как в этом доказательстве для докакзательства случая $l = k$ использовались не все одноместные функции, а только те функции, которые принимают не более чем $k-1$ значение. $\square$

Теорема. *Функция $f(x_1, \ldots, x_n) \in P_k$ образует полную систему (является шефферовой) тогда и только тогда, когда она содержит все функции одной переменной, принимающие не более чем $k-1$ значение.*

Доказательство. $\underline{\Longrightarrow}$ Следует из теоремы Яблонского.
$\underline{\Longleftarrow}$ Пусть f порождает все функции одной переменной, принимающие не более чем $k-1$ значение, в частности она порождает все константы $\Longrightarrow$ f принимает все k значений. Предположим, что f не является существенной, тогда она имеет ровно одну существенную переменную. Класс данных функций обозначим $M(k)$

1. Операция подстановки переменных:
   Пусть $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, тогда если f имела единственную существенную переменную x_j, то g также будет иметь единственную существенную переменную x_{i_j}. Если f принимала все k значений, то, варьируя значение переменной, получим все k значений, но тогда $g \in M(k)$.

2. Операция подстановки функции в функцию:
   Пусть $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{m+n-1}))$. Если f имеют единственную существенную переменную x_i, где $i < n$, то и h имеет единственную существенную переменную x_i и, варьируя значение переменной x_i получим все k значений. Если единственной существенной переменной f является переменная x_n, то рассморим единственную существенную переменную функции $g \Longrightarrow$ она является единственной существенной переменной и для h, аналогично, варьируя значения данной переменной, получим все k значений функции g, а значит, и функции h.

3. Операция добавления или удаления фиктивных переменных:
   Добавление или удаление фиктивных переменных не повлияет на количество существенных переменных и число значений, которые принимает функция.

$\Longrightarrow$ из функции f можно получить суперпозициями только одноместные функции, принимающие все k значений, то есть нельзя получить константу $\Longrightarrow$ f является существенной, тогда по теореме Яблонского она образует полную систему. $\square$

29 Билет 29 (Теорема Янова)

Теорема. *В* $\forall k \geqslant 3$ *в* P_k *существует замкнутый класс, не имеющий базиса.*

Доказательство. Рассмотрим последовательность функций

$$f_0 = 0, \ldots, f_i(x_1, \ldots, x_i) = \begin{cases} 1, & \text{если } x_1 = x_2 = \ldots = x_i = 2 \\ 0, & \text{иначе} \end{cases}$$

. Пусть M - замыкание множества $\{f_0, \ldots\}$, тогда рассмотрим операции суперпозиции на множестве M.

1. Операция подстановки переменных:
   Пусть $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$, тогда, если f получалась из некоторой функции f_j добавлением фиктивной переменной, то и g получалась из некоторой функции f_m, где $n \leqslant i$, добавлением фиктивной переменной.

2. Операция добавления функции в функцию:
   Пусть функции f и g получаются из некоторых функций f_i добавлением фиктивных переменных и $h(x_1, \ldots, x_{n+m-1}) = f(x_1, \ldots, x_{n-1}, g(x_n, \ldots, x_{m+n-1}))$, тогда функция h тождественно равна 0, так как g не принимает значение 2, то есть h получается добавлением фиктивных переменных к ыункции f_0.

3. Операция добавления или удаления фиктивных переменных:
   Очевидно.

Предположим, что данный класс имеет базис, тогда:

1. Если в базисе B есть хотябы две различные функции, которые получаются из f_i и f_j соотвественно, тогда одна из этих функций получается из другой сначала отождествлением некоторых переменных, а затем добавлением фиктивных переменных $\Longrightarrow$ это не базис.

2. Если в базисе имеется единственная функция, получаемая из некоторой функции f_i добавлением фиктивных переменных, тогда из неё суперпозициями можно получить только функции f_j, где $j \leqslant i$, а значит, нельзя получить функцию f_{i+1}.

$\square$

30 Билет 30 (Теорема Мучника)

Теорема. *$\forall k \geqslant 3$, в P_k существует замкнутый класс, имеющий счётный базис.*

Доказательство. Рассмотрим систему функий $f_i(x_1, \ldots, x_i) =$

$$= \begin{cases} 1, & \text{если в наборе есть ровно одна единица, а все остальные элементы равны 2} \\ 0, & \text{иначе} \end{cases}$$

$i = 2, 3, \ldots$, обозначим M множество $\{f_2, f_3, \ldots\}$.
Предположим, что какая-то функция f_m выражается через остальные функции и рассмотрим сигнатуру Σ в $\{f_2, f_3, \ldots, f_{m-1}, f_{m+1}, \ldots\}$, тогда существует невырожденная формула Φ, определяющая относительно переменных $x_1, \ldots, x_m$ функцию f_m. Все фиктивные переменные формулы Φ заменим на x_1, что не изменит функции, реализуемые формулой. По определению Φ имеет вид $s(B_1, \ldots, B_r)$, где s - символ сигнатуры, а B_i - либо переменная, либо невырожденная формула в сигнатуре. Рассмотрим произвольный набор $(\alpha_1, \ldots, \alpha_m)$ значений переменных $(x_1, \ldots, x_m)$. Обозначим β_i значение формулы B_i на этом наборе, тогда $f_m(\alpha_1, \ldots, \alpha_m) = f_r(\beta_1, \ldots, \beta_r)$. Рассмотрим 3 случая:

1. Среди формул B_i есть не менее двух невырожденных, тогда не менее двух значений β_i, равных 0 или 1. Значит, функция f_r обращается в ноль на любом наборе $\Longrightarrow$ функция f_m является тождественным нулём - противоречие.

2. Среди формул B_i есть ровно одна невырожденная, её обозначим B_j, тогда есть функция $B_{j'}$, являющаяся переменной, обозначим её x_q, так как $r \geqslant 2$. Пусть $\alpha_q = 1$, $\alpha_1 = \ldots = \alpha_{q-1} = \alpha_{q+1} = \ldots = \alpha_m = 2$, тогда $f_m(\alpha_1, \ldots, \alpha_m) = 1$, но так как $\beta_{j'} = 1$ и β_j равно либо 0, либо 1, то $f_r(\beta_1, \ldots, \beta_r) = 0$, а значит, и $f_m = 0$ - противоречие.

3. Все формулы являются переменными, тогда $r > m$ так как все переменные функции f_m являются существенными $\Longrightarrow \exists i$ и $j : i \neq j$ и B_i и B_j - одна и та же переменная, обозначим её x_q. Пусть $\alpha_q = 1$, $\alpha_1 = \ldots = \alpha_{q-1} = \alpha_{q+1} = \ldots = \alpha_m = 2$, тогда $f_m(\alpha_1, \ldots, \alpha_m) = 1$, но $\beta_i = \beta_j = 1$, а значит, $f_r(\beta_1, \ldots, \beta_r) = 0 = f_m$ - противоречие.

Таким образом мы получили, что $\forall f_m$ не выражается через остальные функции, а так как система $\{f_2, f_3, \ldots\}$ полна в M, имеем, что эти функции образуют базис в M. $\square$

31 Билет 31 (Теорема о представлении функций k-значной логики полиномами)

Теорема. *Система полиномов по модулю k полна в P_k тогда и только тогда, когда k - простое число.*

Доказательство. Рассотрим функцию $f(x_1, \ldots, x_n) = \sum\limits_{\sigma_1, \ldots, \sigma_n} j_{\sigma_1}(x_1) \cdot \ldots \cdot j_{\sigma_n}(x_n) \cdot f(\sigma_1, \ldots, \sigma_n) (mod\ k)$ (аналог совершенной д.н.ф.).
$j_\sigma(x) = j_0(x - \sigma) \Longrightarrow$ функцию $j_\sigma(x)$ представима полиномом по модулю k тогда и только тогда, когда функция j_0 представима полтномом по модулю k. Тогда рассмотрим два случая:

1. k - простое число, тогда по малой теореме Ферма $x^{k-1} \equiv 1 (mod\ k)$ $\forall x = \overline{1, k-1} \Longrightarrow j_0(x) = 1 - x^{k-1} (mod\ k)$, то есть $j_0(x)$ представима полиномом по модулю k, а значит, система полиномов полна.

2. k - составное число, тогда $k = k_1 \cdot k_2$, где $k_1 \geqslant k_2 > 1$ - натуральные числа. Предположим, что $j_0(x) = b_0 + b_1 + \ldots + b_s x^s (mod\ k)$, тогда $j_0(0) = b_0 (mod\ k) = 1$, $j_0(k_1) = 1 + b_1 k_1 + \ldots + b_s k_1^s (mod\ k) = k_1 k_2 n \Longrightarrow 1 = k_1(k_2 n - b_1 - b_2 k_1 - \ldots - b_s k_1^{s-1}) \Longrightarrow k_1 = 1$ - противоречие.

□

32 Билет 32 (Основные определения, связанные с конечным автоматом)

Определение. Конечный абстрактный детерминированный автомат - объект $V = (A, Q, B, \varphi, \psi)$, где A, Q, B - конечные множества; $\varphi : Q \times A \to$; $\psi : Q \times A \to B$. Множества A, Q, B называются входным алфавитом, алфавитом состояний и выходным алфавитом соответственно.

Способы задания:

1. С помощью таблицы со строками $a_1, \ldots, a_m$ и столбцами $q_1, \ldots, q_n$, где на пересечении i-ой строки и j-ого столбца находится элемент $(\varphi(q_j, a_i), \psi(q_j, a_i))$.

2. С помощью диграммы мура: (см. рисунок 8 лекции на странице 3)

3. С помощью системы уравнений k-значной логики.

Определение. Слово в алфавите A - входное слово, в алфавите B - выходное слово, в алфавите Q - слово состояний.

Обозначения: Λ - пустое слово, $|\alpha|$ - длина слова α, X^* - множество слов в алфавите X, $\alpha]_l$ - начало слова α, имеющее длину l.

Определение. База индукции: $\varphi(q, \Lambda) = q$
Пусть $\varphi(q, \alpha)$ - состояние автомата, появляющееся при подаче на вход слова α, a - буква алфавита, тогда $\varphi(q, \alpha a) = \varphi(\varphi(q, \alpha), a)$ - состояние автомата при подаче на вход слова αa.
Так как для функции ψ нужен, чтобы был хотя бы какой-нибудь символ на вход $\Longrightarrow$ сразу перейти к шагу индукции. Пусть $\psi(q, \alpha)$ - значение выходного символа при подаче на вход слова α, a - буква алфавита, тогда $\psi(q, \alpha a) = \psi(\psi(q, \alpha), a)$ - выходной символ при подаче на вход слова αa.

Свойства. *1.* $\varphi(q, \alpha_1\alpha_2) = \varphi(\varphi(q, \alpha_1), \alpha_2)$

2. $\psi(q, \alpha_1\alpha_2) = \psi(\varphi(q, \alpha_1), \alpha_2)$

3. $\overline{\psi}(q, \alpha_1\alpha_2) = \overline{\psi}(q, \alpha_1)\overline{\psi}(\varphi(q, \alpha_1), \alpha_2)$

33 Билет 33 (Инициальный конечный автомат и функции, реализуемые им)

Определение. Инициальный конечный автомат - объект $V_{q_1} = (A, Q, B, \varphi, \psi, q_1)$, где A, Q, B - конечные множества, $\varphi : Q \times A \to Q$, $\psi : Q \times A \to B$, $q_1 \in Q$.

Определение. Конечно-автоматная функция - функция, заданная инициальным конечным автоматом. Она задана на A^* и определена равенством $f(\alpha) = \overline{\psi}(q_1, \alpha)$.

i-ую букву слова α обозначим $\alpha(i)$, так как слово является функцией, определённой на отрезке натурального ряда.

Определение. Канонические уравнения - это соотношения вида:

$$\kappa(1) = q_1$$
$$\kappa(t+1) = \varphi(\kappa(t), \alpha(t))$$
$$\beta(t) = \psi(\kappa(t), \alpha(t))$$

где слово $\kappa = \overline{\varphi}(q_1, \alpha)$, слово $\beta = \overline{\psi}(q_1, \alpha)$, $\kappa = \kappa(1) \dots \kappa(s+1)$, $\beta = \beta(1) \dots \beta(s)$, $\alpha = \alpha(1) \dots \alpha(s)$.

34 Билет 34 (Преобразование бесконечных и периодических последовательностей)

Определение. Пусть $V_q(A,\ Q, B,\ \varphi,\ \psi,\ q_1)$ - инициальный конечный автомат, $\alpha = \alpha(1)\alpha(2)\ldots$ - бесконечная последовательность символов алфавита A. Множество таких последовательностей обозначим A^∞. Скажем, что инициальный конечный автомат V_q преобразует входную последовательность α в выходную последовательность β, где $\beta = \overline{\psi}(q, \alpha)$, а i-ый элемент последовательности β имеет вид: $\beta(i) = \psi(q,\ \alpha(1),\ \ldots,\ \alpha(i))$.

Определение. Последовательность $\alpha = \alpha(1)\alpha(2)\ldots \in A^\infty$ называется периодической, если $\exists \tau$ и $\tau' : \forall i \geqslant \tau' + 1 \Longrightarrow \alpha(i) = \alpha(i+\tau)$. τ' - длина предпериода, τ - длина периода.

Теорема. *Конечный инициальный автомат $V_{q_1}(A,\ Q,\ B,\ \varphi,\ \psi,\ q_1)$, имеющий n состояний, прелбразует любую периодическую последовательность $\alpha \in A^\infty$, имеющую наименьшую длину периода τ, в периодическую последовательность с наименьшей длиной периода вида $\theta \cdot m$, где $\theta | \tau$, $m \in \{1,\ \ldots,\ n\}$. Если $|A| \geqslant 3$ и $|B| \geqslant 2$, то каждое такое значение вида $\theta \cdot m$ достигается при некотором автомате V_q и соответствующей последовательности α.*

Доказательство. Пусть $V_{q_1}(A,\ Q,\ B,\ \varphi,\ \psi,\ q_1)$, $|Q| = n$, α - периодическая последовательность с предпериодом τ' и периодом τ, тогда $\forall i \geqslant \tau' + 1 \Longrightarrow \alpha(i) = \alpha(i+\tau)$. Обозначим $\alpha_1 = \alpha(1)\ldots\alpha(\tau')$, $\alpha_2 = \alpha(\tau'+1)\ldots\alpha(\tau'+\tau)$, тогда α имеет вид: $\alpha_1\alpha_2\alpha_2\ldots$. Так как число состояний автомата равно n, то в последовательности $\varphi(q_1, \alpha_1\alpha_2)$, $\varphi(q_1, \alpha_1\alpha_2\alpha_2)$, $\ldots$, $\varphi(q_1, \alpha_1\alpha_2^{n+1})$ есть два одинаковых значения, то есть $\exists i_1,\ i_2 : 1 \leqslant i_1 \leq i_2 \leqslant n+1$ и $\varphi(q_1, \alpha_1\alpha_2^{i_1}) = \varphi(q_1, \alpha_1\alpha_2^{i_2})$. Пусть $q = \varphi(q_1, \alpha_1\alpha_2^{i_1})$, $\alpha_3 = \alpha_2^{i_2 - i_1}$, тогда из предыдущего уравнения и первого свойства функции φ имеем $q = \varphi(q, \alpha_3) \Longrightarrow$ автомат будет возвращаться в состояние q, а выходная последовательность, с некоторого момента, будет образована повторяющимися словами $\overline{\psi}(q, \alpha_3) \Longrightarrow \overline{\psi}(q_1, \alpha_3)$ - периодическая последовательность с периодом, равным длине слова α_3, которая равна $(i_2 - i_1)\tau$ $\Longrightarrow$ минимальная длина периода является делителем числа $(i_2 - i_1)\tau$ и имеет вид: $\theta \cdot m$, где $m | (i_2 - i_1)$, а $\theta | \tau$, а так как $i_2 - i_1 \in \{1, \ldots, n\}$.
Пусть $A = \{a_1, \ldots, a_k\}$, $k \geqslant 3$ и $B = \{b_1, \ldots, b_p\}$ $p \geqslant 2$. τ - произвольное натуральное число, θ - его делитель, $m \in \{1, \ldots, n\}$. Определим инициальный автомат V_{q_1} диаграммой Мура (см. рисунок 8 лекции на странице 7).
Если первая входная буква отлична от a_1, то до состояния q_{n-m} будем получать

b_1, а в состоянии q_{n-m} получим либо b_1, либо b_2 в зависимости от последней буквы входного алфавита.
Пусть первой входной буквой является буква a_1, тогда если следующая входная буква отлична от a_{k-1} и a_k, то автомат не изменяет своего состояния, иначе - сдвигается по циклу и выходной буквой будет b_1, если автомат не переходит в состояние q_{n-m+1}, где выходным словом будет b_2.
Рассмотрим слова $\alpha_1 = a_1^{\theta-1}a_{k-1}$, $\alpha_2 = a_1^{\theta-1}a_k$, $\alpha_3 = \alpha_1^{\frac{\tau}{\theta}-1}\alpha_2$. Пусть $\theta > 1$, возьмём периодичесую последовательность $\alpha = \alpha_3\alpha_3\ldots$, тогда в каждом слове α_3 буква a_k встретиться ровно один раз $\Longrightarrow$ наименьшая длина периода будет равна длине слова α_3, что равно $\theta \cdot (\frac{\tau}{\theta} - 1 + 1) = \tau$. Так как $\theta > 1$, то слово α_3 начинается с $a_1 \Longrightarrow$ пока на вход поступает a_1 состояние меняться не будет, это будет происходить $\theta - 1$ раз, а при подаче последней буквы слова α_1 или α_2 автомат перейдёт в новое состояние. До перехода в состояние q_{n-m+1} на выходе будем получать b_1, а при переходе в это состояние на выходе получим b_2. Однократное прохождение цикла происходит за время, равное $\theta \cdot m$, где m - число состояний цикла $\Longrightarrow$ выходная последовательность будет образована периодически повторяющимися фрагментами $b_1^{\theta \cdot m-1}b_2$, а её период равен $\theta \cdot m$.
Пусть $\theta = 1 \Longrightarrow$ число состояний не меньше длины наименьшего периода, тогда изменем вышеуказанную диаграмму Мура так: если первая буква входного слово равна a_{k-1} или a_k, то из состояния q_1 переходим в состояние q_{n-m+1}, иначе - в состояние q_2, остальное аналогично. $\square$

35 Билет 35 (Неотличимость автоматов и изоморфизм между ними)

Определение. Пусть $V = (A, Q, B, \varphi, \psi)$ и $V' = (A, Q', B, \varphi', \psi')$ - конечные автоматы. Если $\forall \alpha \in A^*$ $\overline{\psi}(q, \alpha) = \overline{\psi'}(q', \alpha)$, где $q \in Q$ и $q' \in Q'$, то состояния q и q' называются неотличимыми, иначе - отличимыми.

Определение. Если любые два состояния автомата отличимы друг от друга, то такой автомат называется автоматом приведённого вида.

Определение. Если для любого состояния q автомата V существует неотличимое от него состояние q' автомата V', и это верно, если поменять местами авоматы V и V', то такие автоматы назовём неотличимыми.

Определение. Пусть $V = (A, Q, B, \varphi, \psi)$ и $V' = (A, Q', B, \psi', \varphi')$ - конечные автоматы. Если существует взаимно однозначное отображение $\xi : Q \to Q'$ такое, что

1. $\xi(\varphi(q,a)) = \varphi'(\xi(q),a)$

2. $\psi(q,a) = \psi'(\xi(q),a)$ $(\forall q \in Q,\, a \in A)$

то такие автоматы назовём изоморфными.

Теорема. *Для любого конечного автомата V существует единственный с точностью до изоморфизма конечный автомат приведённого вида, неотличимый от V.*

Доказательство. Пусть $V = (A,\, Q,\, B,\, \varphi,\, \psi)$ - конечный автомат. Рассмотрим разиение множества Q на классы $Q_1,\, \ldots,\, Q_n$ попарно отличимых состояний, $q,\, q' \in Q_i$, $i \in \{1,\, \ldots,\, n\}$, $a \in A$. Если $\varphi(q,a) \in Q_j$, $\varphi(q',a) \in Q_{j'}$, $j \neq j'$, то $\exists \alpha,\, a \in A^* : \overline{\psi}(\varphi(q,a),\alpha) \neq \overline{\psi}(\varphi(q',a)\alpha) \Longrightarrow \overline{\psi}(q,a\alpha) = \psi(q,a)\overline{\psi}(\varphi(q,a),\alpha) \neq \psi(q',a)\overline{\psi}(\varphi(q',a),\alpha) = \overline{\psi}(q',a\alpha) \Longrightarrow$ состояния q и q' отличимы - противоречие $\Longrightarrow Q_j = \varphi'(Q_i,a)$. Значит, $\forall q$ и $q' \in Q_i$ $\psi(q,a) = \psi(q',a) = b \Longrightarrow b = \psi'(Q_i,a)$. В результате имеем функции $\varphi' : \{Q_1,\, \ldots,\, Q_n\} \times A \to \{Q_1, \ldots, Q_n\}$ и $\psi' : \{Q_1, \ldots, Q_n\} \times A \to B$. Рассмотрим автомат $V' = (A,\, \{Q_1,\, \ldots,\, Q_n\},\, B,\, \varphi',\, \psi')$, из определения функций φ' и ψ' имеем $\forall q \in Q_i$ и $\alpha \in A^*$ $\varphi(q,\alpha) \in \varphi'(Q_i,\alpha)$, $\overline{\psi}(q,\alpha) = \overline{\psi'}(Q_i,\alpha) \Longrightarrow$ автоматы V и V' неотличимы. Пусть $i \neq j$, $i,\, j \in \{1, \ldots, n\}$, $q \in Q_i$, $q' \in Q_j$, так как Q_i и Q_j отличимы, существует слово $\alpha \in A^* : \overline{\psi}(q,\alpha) \neq \overline{\psi}(q',\alpha)$, тогда $\overline{\psi'}(Q_i,\alpha) \neq \overline{\psi'}(Q_j,\alpha) \Longrightarrow$ автомат V' является конечным автоматом приведённого вида.

Пусть $V'' = (A,\, Q'',\, B,\, \varphi'',\, \psi'')$ - автомат приведённого вида, $Q'' = \{q''_1, \ldots, q''_m\}$. Каждое q''_i неотличимо от некоторого состояния автомата V, а значит, и от некоторого состояния автомата V', а так как $q''_1,\, \ldots,\, q''_m$ попарно отличимы, то попарно отличимых $Q_1,\, \ldots,\, Q_n$ не меньше $m \Longrightarrow n \geqslant m$. Пусть $q \in Q_i$, тогда q неотличимо от некоторого состояния автомата V, а значит, и некоторого состояния автомата V'', а так как состояния $Q_1,\, \ldots,\, Q_n$ попарно отличимы, то число отличимых состояний в Q'' не меньше $n \Longrightarrow n = m$. Рассмотрим отображение ξ состояния Q_i автомата V' в соответствующее ему неотличимое состояние автомата V''. Это отображение взаимно однозначно, так как каждому состоянию Q_i автомата V' соответствует единственное неотличимое состояние автомата V''. Так как Q_i и $\xi(Q_i)$ неотличимы, то $\forall a \in A$ состояния $\varphi'(Q_i,a)$ и $\varphi''(\xi(Q_i),a)$ неотличимы $\Longrightarrow \xi(\varphi'(Q_i,a)) = \varphi''(\xi(Q_i),a)$. Так как состояния Q_i и $\xi(Q_i)$ неотличимы $\Longrightarrow \forall a \in A$ $\overline{\psi'}(\{Q_1,\ldots,Q_n\},a) = \overline{\psi''}(\xi(Q''),a) \Longrightarrow \psi'(Q_i,a) = \psi''(\xi(Q_i),a)$ $\forall Q_i$ и $a \in A$. Значит, по определению автоматы V' и V'' изоморфны. □

36 Билет 36 (Теорема Мура для одного конечного автомата)

Теорема. *Если два состояния автомата $V = (A,\ Q,\ B,\ \varphi,\ \psi)$ отличимы, то существует различающее их слово длины $|Q| - 1$, причём эта оценка не улучшаема.*

Доказательство. Пусть $V = (A, Q, B, \varphi, \psi)$ - конечный автомат, состояния q_1 и q_2 отличимы. Рассмотрим отношение ρ_k неотличимости состояний на множестве Q: $q\rho_k q' \Leftrightarrow \forall\alpha \in A^k\ \overline{\psi}(q,\alpha) = \overline{\psi}(q',\alpha)$. Отношение ρ_k - отношение эквивалентности, так как оно рефлексивно, симметрично и транзитивно. Множество классов эквивалентности обозначим R_k. Так как состояния q_1, q_2 отличимы, то существует непустое различающее их слово α наименьшей длины, оно представимо в виде $\alpha' a$, где $\alpha' \in A^*$, $a \in A$. Так как α - слово наименьшей длины, различающее состояния q_1 и $q_2 \Longrightarrow$ эти состояния отличаются последней буквой $\psi(\varphi(q_1,\alpha'),a) \neq \psi(\varphi(q_2,\alpha'),a) \Longrightarrow \varphi(q_1,\alpha') \neq \varphi(q_2,\alpha') \Longrightarrow$ состояния q_1 и q_2 принадлежат различным классам отношения $\rho_1 \Longrightarrow |R_1| \geqslant 2$.

$|R_k| \leqslant |R_{k+1}|$ так как все классы эквивалентности, содержащиеся в R_k, содержатся в R_{k+1}. Рассмотрим разбиение R_∞ множества Q на классы попарно неотличимых состояний. Пусть $R_k = R_{k+1}$ и $R_k \neq R_\infty$, тогда $\exists q$ и $q' \in M$, $M \in R_k$, которые отличимы. Выберем q, q', M так, чтобы различающее эти состояния слово α имело наименьшую длину $\Longrightarrow$ длина слова α не меньше 2, так как $M \in R_k$ и $k \geqslant 1$, тогда α имеет вид: $a\alpha'$, где $\alpha' \in A^*$, $a \in A$. Рассмотрим состояния $\tilde{q} = \varphi(q,a)$, $\widehat{q} = \varphi(q',a)$. Слово α' различает состояния $\tilde{q}$ и $\widehat{q}$, так как $\psi(\varphi(q,a),\alpha') = \psi(q,a\alpha') \neq \psi(q',a\alpha') = \psi(\varphi(q',a),\alpha')$. Длина слова α' меньше длины слова α, а так как α - слово наименьшей длины, то состояния $\tilde{q}$ и $\widehat{q}$ принадлежат различным классам в R_k. Пусть $\tilde{q} \in M_1$, $\widehat{q} \in M_2$, M_1, $M_2 \in R_k$, тогда рассмотрим слово α'', имеющее длину k и различающее состояния $\tilde{q}$ и $\widehat{q} \Leftrightarrow \overline{\psi}(\tilde{q},\alpha'') \neq \overline{\psi}(\widehat{q},\alpha'')$. Рассмотрим слово $\alpha''' = a\alpha''$, тогда $\overline{\psi}(q,\alpha''') = \psi(q,a)\overline{\psi}(\varphi(q,a),\alpha'') = \psi(q,a)\overline{\psi}(\tilde{q},\alpha'') \neq \psi(q',a)\overline{\psi}(\widehat{q},\alpha'') = \psi(q',a)\overline{\psi}(\varphi(q',a),\alpha'') = \overline{\psi}(q',\alpha''') \Longrightarrow$ слово α''' различает состояния q и $q' \Longrightarrow$ эти состояния лежат в разных классах R_{k+1} - противоречие.

Рассмотрим последовательность $|R_1|, |R_2|, \ldots$, она монотонно неубывает, и каждый её член не превосходит $|Q| \Longrightarrow \exists R_k : |R_k| = |R_{k+1}| = R_\infty \Longrightarrow 2 \leqslant |R_1| < \ldots < |R_k| \leqslant |Q|$.

База индукции: $|R_1| \geqslant 1 + 1$.

Пусть верно для $i = j - 1$, то есть $|R_{j-1}| \geqslant j - 1 + 1 = j$. Так как $|R_{j-1}| < |R_j|$,

то $|R_j| \geqslant |R_{j-1}| + 1 \geqslant j + 1$.
$\Longrightarrow |Q| \geqslant |R_k| \geqslant k + 1 \Longrightarrow k \leqslant |Q| - 1 \Longrightarrow$ любые два отличимые состояния автомата различимы словом длины $|Q| - 1$.
Докажем, что есть автомат, для которого данную оценку нельзя улучшить. Рассмотрим автомат $V = (A,\, Q,\, B,\, \varphi,\, \psi)$, $A = B = \{0, 1\}$, $Q = \{q_1,\, \ldots,\, q_n\}$, который из любого состояния q_i, кроме q_1 и q_n, при подаче на вход 0 переходит в состояние q_{i+1}, при подаче на вход 1, переходит в состояние q_{i-1}, а выходной буквой будет 0. Из состояния q_1 при любом входном символе автомат переходит в состояние q_2, а выходным символом является 1. Из состояния q_n при подаче на вход 0 автомат остаётся в этом состоянии, а при подаче на вход 1 автомат переходит в состояние q_{n-1}, выходным символом в обоих случаях является 0.
Чтобы отличить состояния q_{n-1} и q_n переведём состояние q_{n-1} в состояние q_1, что можно сделать, если подать на вход $n - 2$ единицы, причём длина такого слова минимальна, тогда для отличия этих состояний остаётся подать на вход любой символ и получить на выходе 1 для q_{n-1} и 0 для q_n. Длина данного слова равна $n - 1$ и она минимальна. □

37 Билет 37 (Теорема Мура для двух конечных автоматов)

Теорема. *Пусть $V = (A,\, Q,\, B,\, \varphi,\, \psi)$ и $V' = (A,\, Q',\, B,\, \varphi',\, \psi')$ - конечные автоматы, состояние q_1 автомата V отличимо от состояния q_2 автомата V', тогда существует различающее эти два состояния слово, имеющее длину $|Q| + |Q'| - 1$, причём, вообще говоря, эта оценка неулучшаема.*

Доказательство. Пусть $V = (A, Q, B, \varphi, \psi)$ и $V' = (A, Q', B, \varphi', \psi')$ - конечные автоматы, состояние q_1 автомата V отличимо от состояния q_2 автомата V'. Если Q и Q'пересекаются, то переобозначим состояния второго автомата так, чтобы они не пересекались, так что без ограничения общности будем считать, что $Q \cap Q' = \varnothing$. Рассмотрим автомат $V'' = (A, Q \cup Q', B, \varphi'', \psi'')$, $\varphi''(q, a) = \varphi(q, a)$, $\psi''(q, a) = \psi(q, a)\ \forall q \in Q$, $\varphi''(q, a) = \varphi'(q, a)$, $\psi''(q, a) = \psi'(q, a)\ \forall q \in Q'$. Состояния q_1 и q_2 являются отличимыми состояниями автомата V'', тогда по теореме Мура для одного автомата существует различающее их слово, длина которого равна $|Q \cup Q'| - 1 = |Q| + |Q'| - 1$.
Докажем, что сущестуют автоматы, для которых эту оценку нельзя улучшить. Рассмотрим автомат $V = (A,\, Q,\, B,\, \varphi,\, \psi)$, $A = B = \{0, 1\}$, $Q = \{q_1,\, \ldots,\, q_n\}$, который из любого состояния q_i, кроме q_1 и q_n, при подаче на вход 0 переходит

в состояние q_{i+1}, при подаче на вход 1 переходит в состояние q_{i-1}, а выходной буквой будет 0. Из состояния q_1 при любом входном символе автомат переходит в состояние q_2, а выходным символом является 1. Из состояния q_n при подаче на вход 0 автомат остаётся в этом состоянии, а при подаче на вход 1 автомат переходит в состояние q_{n-1}, выходным символом в обоих случаях является 0.
Рассмотрим автомат $V' = (A, Q', B, \varphi', \psi')$, $A = B = \{0, 1\}$, $Q' = \{q_1', \ldots, q_m'\}$ и $n \leqslant m$, который из любого состояния q_i, $1 < i < n+1$, при подаче на вход 0 переходит в состояние q_{i+1}, при подаче на вход 1, переходит в состояние q_{i-1}, а выходной буквой будет 0. Для любого состояния q_i, где $n+1 \leqslant i < m$, при подаче на вход 0 автомат переходит в состояние q_{i+1}, а при подаче на вход 1 автомат переходит в состояние q_{n-1}, в обоих случаях выходной буквой является 0. Из состояния q_1 при любом входном символе автомат переходит в состояние q_2, а выходным символом является 1. Из состояния q_m при подаче на вход любого символа автомат остаётся в этом состоянии, выходным символом в обоих случаях является 0.
Каждому состоянию q_i' автомата V', где $i \leqslant n$ сопоставим состояние q_i автомата V, а для каждого состояния q_i', где $m \geq i \geq n$, сопоставим состояние q_n автомата V. Если состояние автомата V сопоставлено состоянию автомата V', то такие состояния будем называть соответствующими. Так как при подаче некоторого входного слова соответствующие состояния переходят в соответствующие состояния, за исключением того момента, когда второй автомат переходит в состояние $q_m' \Longrightarrow$ если состояния q_1 и q_1' отличимы, то существует слово α, отличающее эти два состояния $\Longrightarrow$ некоторая начальная часть α' слова α переводит второй автомат в состояние q_m', а минимальная длина такого слова равна $m-1$. Данное слово переведёт первый автомат в состояние q_n, а значит, для того чтобы получить на выходе первого автомата 1, так как значение на выходе второго автомата равно нулю и меняться не будет, достаточно перевести первый автомат в состояние q_1, что можно сделать с помощью слова, наименьшая длина которого равна $n-1$, и остаётся лишь подать на вход любой символ, чтобы перевести первый автомат из состояния q_1 в состояние q_2 и получить на выходе единицу. Следовательно, наименьшая длина отличающего слова равна $m-1+n-1+1 = n+m-1$. □

38 Билет 38 (События в конечном алфавите)

Определение. Пусть $V_q = (A, Q, B, \varphi, \psi, q)$ - инициальный конечный автомат, $B' \subseteq B$, множество $M = \{\alpha | \alpha \in A^* \setminus \{\Lambda\}, \psi(q, \alpha) \in B'\}$ называется представимым в инициальном конечном автомате V_q с помощью подмножества B' выходных символов.

Определение. Подмножества множества $A^* \setminus \{\Lambda\}$ называются событиями в алфавите A.

Определение. Если существует инициальный конечный автомат V_q, представляющий событие M посредством некоторого подмножества B', то событие M называется представимым.

Определение. Произведение событий $M_1 \cdot M_2$ - множество всех слов вида: $\alpha_1\alpha_2$, где $\alpha_1 \in M_1$, $\alpha_2 \in M_2$.

Определение. Итерация события M ($< M >$) - множество слов вида: $\alpha_1 \ldots \alpha_k$, где $\alpha_1, \ldots, \alpha_k \in M$, $k \geqslant 1$.

Свойства. *1.* $\varnothing \cdot M = M \cdot \varnothing = \varnothing$

2. $< \varnothing > = \varnothing$

3. $< M > = M \cdot < M > \cup M$

4. $M \cdot < M > = < M > \cdot M$

Определение. Событие $M \subseteq A^*$ называется регулярным, если его можно получить из событий $\varnothing$, $\{a\} \in A$ с помощью конечного числа применения операции объединения событий, умножения событий и итерации события.

39 Билет 39 (Лемма о решении уравнений)

Теорема. *Соотношение* $X = XC \cup D$ *выполняется для событий* C, D, X *тогда и только тогда, когда* $X = D < C > \cup D$.

Доказательство. $\underline{\Longleftarrow}$ $X = D < C > \cup D$, тогда $XC \cup D = (D < C > \cup D)C \cup D = D(< C > C \cup C) \cup D = D(C < C > \cup C) \cup D = D < C > \cup D = X$.
$\underline{\Longrightarrow}$ Пусть $X = XC \cup D$ и $X \nsubseteq D < C > \cup D$, тогда рассмотрим кратчайшее слово $\alpha \in X \setminus (D < C > \cup D) \Longrightarrow \alpha \in XC \cup D$ и $\alpha \notin D \Longrightarrow \alpha \in XC \Longrightarrow \alpha = \alpha_1\alpha_2$, где $\alpha_1 \in X$, $\alpha_2 \in C$. Так как $\alpha \in X \setminus (D < C > \cup D)$ - слово минимальной длины, то $\alpha_1 \in (D < C > \cup D) \Longrightarrow \alpha_1\alpha_2 \in (D < C > \cup D)C \Longrightarrow \alpha \in (D < C > \cup D)C$, причём $(D < C > \cup D)C = D < C > C \cup DC = D(< C > C \cup C) = D(C < C > \cup C) = D < C >$ - противоречие.
Пусть $D < C > \cup D \nsubseteq X$, тогда рассмотрим слово α минимальной длины такое,

что $\alpha \in (D < C > \cup D) \setminus X$. Так как $X = XC \cup D$, то $\alpha \notin (XC \cup D) \Longrightarrow \alpha \notin D$ и $\alpha \notin XC \Longrightarrow \alpha \in D < C >$. Так как $D < C >= D(C < C > \cup C) = (D < C > \cup D)C$, то $\alpha = \alpha_1\alpha_2$, где $\alpha_1 \in (D < C > \cup D)$, $\alpha_2 \in C \Longrightarrow \alpha_1 \in X$, так как $\alpha \notin X$ - слово минимальной длины $\Longrightarrow \alpha_1\alpha_2 \in XC \Longrightarrow \alpha \in XC$, а значит, $\alpha \in XC \cup D = X$ - противоречие.
То есть $D < C > \cup D \subseteq X$ и $X \subseteq (D < C > \cup D)$, значит, $X = D < C > \cup D$. □

40 Билет 40 (Лемма о регулярных событиях, удовлетворяющих системе уравнений с регулярными коэффициентами)

Теорема. *Пусть события R_{ij} являются регулярными, тогда события $X_1, \dots, X_n$, которые удовлетворяют системе уравнений:*

$$\begin{cases} X_1 = X_1R_{11} \cup \ldots \cup X_nR_{n1} \cup R_{01} \\ \vdots \\ X_n = X_1R_{1n} \cup \ldots \cup X_nR_{nn} \cup R_{0n} \end{cases}$$

являются регулярными.

Доказательство. База индукции: $n = 1$ $X_1 = X_1R_{11} \cup R_{01}$, тогда по лемме $X_1 = R_{01} < R_{11} \cup R_{01}$, то есть событие X_1 получено из регулярных событий с помощью операций умножения, объединения и итерации, а значит, событие X_1 является регулярным.
Пусть события $X_1, \dots, X_{n-1}$ являются регулярными, рассмотрим последнее уравнение $X_n = X_1R_{1n} \cup \ldots \cup R_{nn}X_n \cup R0n$. Решим это уравнение относительно X_n, тогда получим

$$X_n = (X_1R_{1n} \cup \ldots \cup X_{n-1}R_{n-1,n} \cup R_{0n}) < R_{nn} > \cup X_1R_{11} \cup \ldots \cup X_{n-1}R_{n-1,n} \cup R_{0n} =$$

$$= X_1(R_{1n} < R_{nn} > \cup R_{1n}) \cup \ldots \cup X_{n-1}(R_{n-1,n} < R_{nn} > \cup R_{n-1,n}) \cup R_{0n} < R_{nn} > \cup R_{0n}$$

. Подставим X_n в систему из $n-1$ уравнения и получим:

$$\begin{cases} X_1 = X_1(R_{11} \cup R_{n1}(R_{1n} < R_{nn} > \cup R_{1n})) \cup \ldots \cup X_{n-1}(R_{n-1,1} \cup R_{1n}(R_{n-1,n} < R_{nn} > \cup R_{n-1,n})) \cup R_{n1}(R_{0n} < R_{nn} > \cup R_{0n}) \cup R_{01} \\ \vdots \\ X_{n-1} = X_1(R_{1n-1} \cup R_{nn-1}(R_{1n} < R_{nn} > \cup R_{1n})) \cup \ldots \cup X_{n-1}(R_{n-1,n-1} \cup R_{n-1n}(R_{n-1n} < R_{nn} > \cup R_{n-1n})) \cup R_{n,n-1}(R_{0n} < Rnn > \cup R_{0n}) \cup R_{0n-1} \end{cases}$$

Так как коэффициенты перед $X_1, \dots, X_{n-1}$ - регулярные события, то можно применить предположение индукции, что события $X_1, \dots, X_{n-1}$ являются регулярными, если удовлетворяют системе уравнений такого вида. А значит, событие X_n также является регулярным событием, так как оно получено из регулярных событий с помощью операций умножения, объединения и итерации. □

41 Билет 41 (Лемма о регулярности представимых событий)

Теорема. *Каждое событие, представимое в конечном автомате, является регулярным.*

Доказательство. Пусть $V_{q_1} = (A,\ Q,\ B,\ \varphi,\ \psi,\ q_1)$ - инициальный конечный автомат, $B' \subseteq B$, M - событие, представимое в V_{q_1} посредством B': $M = \{\alpha | \alpha \in A^* \backslash \{\Lambda\},\ \psi(q_1, \alpha) \in B'\}$. Пусть $\{q_1,\ \ldots,\ q_n\}$ - состояния автомата V_{q_1}. Рассмотрим множества M_i непустых входных слов, переводящих автомат из состояния q_1 в состояние q_i, то есть $M_i = \{\alpha | \alpha \in A^* \setminus \{\Lambda\},\ \varphi(q_1, \alpha) = q_i\}$. Рассмотрим множества $M_i' = \{a | a \in A,\ \psi(q_i, a) \in B'\}$, тогда $M = M_1 M_1' \cup \ldots \cup M_n M_n' \cup M_1'$, так как, если слово α имеет длину 1, то $M = M_1'$, если это слово имеет длину, большую единицы, то $\alpha = \alpha' a$, то есть $M_i M_i' = \{\alpha' a | \alpha' \in A^* \setminus \{\Lambda\},\ a \in A,\ \psi(\varphi(q_1, \alpha'), a) = \psi(q_1, \alpha' a) \in B'\}$, то есть $M_i M_i' \subseteq M$. Пусть $M_i' = \{a_1,\ \ldots,\ a_s\}$, где $a_j \in A\ \forall j = \overline{1, s}$, $s \geqslant 0$, при $s = 0$ $M_i' = \varnothing$, при $s > 0$ $M_i' = \{a_1\} \cup \ldots \cup \{a_s\}$, то есть события $M_1',\ \ldots,\ M_n'$ являются регулярными по определению. Обозначим $R_{ij} = \{a | a \in A,\ \varphi(q_i, a) = q_j\}$, эти события являются регулярными, так как $R_{ij} = \{a_1,\ \ldots,\ a_k\}$, если $k = 0$, то $R_{ij} = \varnothing$, если $k > 0$, то $R_{ij} = \{a_1\} \cup \ldots \cup \{a_k\}$. Выполнены следующие соотношения:

$$\begin{cases} M_1 = M_1 R_{11} \cup \ldots \cup M_n R_{n1} \cup R_{11} \\ \vdots \\ M_n = M_1 R_{1n} \cup \ldots \cup M_n R_{nn} \cup R_{1n} \end{cases}$$

По лемме о системе уравнений события $M_1,\ \ldots,\ M_n$ являются регулярными $\Longrightarrow$ событие $M = M_1 M_1' \cup \ldots \cup M_n M_n' \cup M_1'$ является регулярным по определению. □

42 Билет 42 (Обобщённые источники, лемма о событии, определяемом обобщённым источником)

Определение. Обобщённым осточником в алфавите A называется ориентированный граф G, у которого выделены начальная вершина v и конечная вершина $w \neq v$, причём каждому ребру приписано либо пустое слово, либо символ из алфавита A.

Определение. Путь в обобщённом источнике - последовательность π чередующихся вершин и рёбер v_1, ρ_1, ..., v_n, ρ_n, v_{n+1}, ребро ρ_i ведёт от вершины v_i к вершине v_{i+1}. π - путь от вершины v_1 к вершине v_{n+1}.

Определение. Событие, определяемое обобщённым источником G с начальной вершиной v и конечной вершиной w называется множество $|G| = \{\alpha | \alpha \in A^* \setminus \{\Lambda\}, w \in \theta(v, \alpha)\}$, где $\theta(v, \alpha)$ - множество всех вершин v' : $\exists$ путь π от v к v', соответствующий слову α, то есть $[\pi] = \alpha$, то есть пути соответствует слово $a_1 \dots a_n$, где a_i отметка ребра a_i.

Теорема. *Если событие R регулярно, то существует обобщённый источник G такой, что $|G| = R$.*

Доказательство. База индукции: $R = \varnothing$, тогда возьмём источник из двух вершин v и w и без рёбер.
Если $R = \{a\}$, то возьмём источник из двух вершин v и w, соединённых ребром a.
Если $R = R_1 \cup R_2$, то по предположению индукции существуют источники G_1 и G_2 такие, что $|G_1| = R_1$ и $|G_2| = R_2$. В качестве источника G выберем источник, состоящий из источников G_1 и G_2, вершин v, v_1, v_2, w_1, w_2, w и рёбер, которые соответствуют пустым словам и соединяют вершины v с v_1, w_1 с w, v с v_2 и w_2 с w.
Если $R = R_1 \cdot R_2$, $R_1 = |G_1|$, $R_2 = |G_2|$, то возьмём в качестве источника G источник, состоящий из источников G_1 и G_2, вершин $v_1 = v$, w_1, v_2, $w_2 = w$ и ребра, соответтствующего пустому слову и соединяющего вершины w_1 и v_2.
Если $R =< R_1 >$, $|G_1| = R_1$, то в качестве источника G выберем источник, состоящий из источника G_1 и ребра, соответствующего пустуму словуи соединяющего конечную и начальную вершины источника G_1. $\square$