МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени М. В. ЛОМОНОСОВА
Механико-математический факультет

Колпаков Р.М.
Теория дискретных функций

Конспект лекций первого курса первого потока 2014-2015

20 апреля 2015 г.

1 Булевы функции

1.1 Определение булевой функции.

Обозначим за E множество $\{0, 1\}$.

Определение. $f(x_1, \ldots, x_n) \in E$ — функция алгебры логики **(булева функция)**, где $x_i \in E\ \forall i = 1, \ldots, n$ — это отображение $f\colon E^n \to E$. Его можно проиллюстрировать таблицей возможных значений f на различных наборах переменных:

x_1	x_2	$\ldots$	x_{n-1}	x_n	$f(x_1, \ldots, x_n)$
0	0	$\ldots$	0	1	0 **или** 1
0	0	$\ldots$	1	1	0 **или** 1
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	1	$\ldots$	1	1	0 **или** 1

Определение. P_2 — множество всех булевых функций от произвольного конечного множества переменных. $P_2(n)$ — множество всех булевых функций от n переменных.

Определение. $E^n = \{(\sigma_1, \ldots, \sigma_n) |\ \sigma_i \in E;\ i = 1, \ldots, n\}$

Утверждение 1.1. $|P_2(n)| = 2^{2^n}$.

□ Очевидно. ■

1.2 Существенные и фиктивные переменные.

Определение. Пусть $f(x_1, \ldots, x_n)$ — булева функция. Тогда x_i называется **существенной** переменной для f, если $\exists \sigma_1, \sigma_2, \ldots \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n \in \{0, 1\}$:

$$f(\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, 0, \sigma_{i+1}, \ldots, \sigma_n) \neq f(\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, 1, \sigma_{i+1}, \ldots, \sigma_n).$$

В противном случае переменная называется **фиктивной** (пример придумать не очень сложно).

Определение. Пусть x_i — фиктивная переменная для f. Рассмотрим функцию

$$g(x_1, x_2, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)\colon g(\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n) =$$
$$= f(\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, 0, \sigma_{i+1}, \ldots, \sigma_n) = f(\sigma_1, \sigma_2, \ldots, \sigma_{i-1}, 1, \sigma_{i+1}, \ldots, \sigma_n).$$

Тогда говорят, что g **получена из** f **удалением фиктивной переменной** x_i.

Определение. Пусть $f(x_1, \ldots, x_n)$ — булева функция. Также, пусть имеется $y \neq x_1, \ldots, x_n$. Рассмотрим функцию $h(x_1, \ldots, x_n, y)$, $h(\sigma_1, \ldots, \sigma_n, \sigma) = f(\sigma_1, \ldots, \sigma_n)$. Тогда говорим, что h **получена из** f **добавлением фиктивной переменной** y.

Определение. Две булевы функции называются **равными**, если они могут быть получены друг из друга с помощью некоторого числа операций добавления или удаления фиктивных переменных.

1.3 Элементарные функции

1. От одной переменной:

x	0	x	$\bar{x}$	1
0	0	0	1	1
1	0	1	0	1

2. От двух переменных:

x	y	xy	$x \vee y$	$x \oplus y$	$x \sim y$	$x \to y$	$x \vert y$	$x \downarrow y$
0	0	0	0	0	1	1	1	1
0	1	0	1	1	0	1	1	0
1	0	0	1	1	0	0	1	0
1	1	1	1	0	1	1	0	0

3. От трех переменных (функция "медиана"):

x	y	z	$f(x,y,z)$
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

1.4 Формула над системой булевых функций.

$\Phi = \{f_1(x_1, x_2, \ldots, x_{n_1}); f_2(x_1, x_2, \ldots, x_{n_2}); \ldots; f_n(x_1, x_2, \ldots, x_{n_n})\} \subseteq P_2$ — некоторое множество булевых функций, таких что каждой булевой функции $f_i(x_1, x_2, \ldots, x_{n_i})$ сопоставляем функциональный символ f_i.

Определение. Формулой над Φ называется строка символов, состоящая из любых символов-переменных, обозначающих $f_1, \ldots, f_n$ и вспомогательных символов «(», «)», «,», определяемое индуктивным образом:

База индукции: символ любой переменной — правильная формула над Φ.

Индуктивное предположение: пусть $F_1, F_2, \ldots, F_{n_i}$ — некоторые формулы над Φ, тогда $f_i(F_1, F_2, \ldots, F_{n_i})$ — тоже формула над Φ.

Пример 4.1. $((\overline{x \vee y})\&(z \to y))$ — формула над $\{x \vee y; x\&y, x \to y, \overline{x}\}$

Конъюнкция имеет приоритет над дизъюнкцией.

Определение. Значения формулы на наборе значений переменных, входящих в формулу, определяется индуктивным образом.

База индукции: если f — тривиальная, то все очевидно.

Индуктивное предположение: пусть $F_1, F_2, \ldots, F_n$ — формулы, для которых данное понятие уже определено.

$$F = f_i(F_1, F_2, \ldots, F_{n_i});$$

$x_1, \ldots, x_n$ — все переменные, содержащиеся в F;

$\Omega = (\sigma_1, \ldots, \sigma_n)$— набор значений $x_1, \ldots, x_n$;

Ω_j — поднабор значений из Ω для переменных, содержащихся в формуле F_j;

b_j — значение функции F_j на наборе Ω_j.

Тогда значение F на наборе Ω равно $f_i(b_1, \ldots, b_{ni})$.

Пусть F — формула над Φ, содержащая символы переменных $x_1, \ldots, x_n$. Тогда F реализует функцию $f(x_1, \ldots, x_n)$, т. ч. для любого набора $(\sigma_1, \ldots, \sigma_n)$ значений $x_1, \ldots, x_n$ значение $f(\sigma_1, \ldots, \sigma_n)$ равно значению формулы F на $\sigma_1, \ldots, \sigma_n$. f получается из Φ с помощью операции суперпозиции, если F реализуется некоторой нетривиальной формулой над Φ.

Определение. Две формулы F_1 и F_2 называются **эквивалентными**, если они реализуют одинаковые функции.

Пусть $* \in \{\vee, \&, \oplus, \sim\}$ — некоторая операция. Тогда $*$ имеет следующие

Свойства:

1. (*коммутативность*) $x * y = y * x$
2. (*ассоциативность*) $x * (y * z) = (x * y) * z$
3. (*дистрибутивность*)

$$x(y \vee z) = xy \vee xz$$
$$x(y \oplus z) = xy \oplus xz$$
$$x \vee (y \& z) = (x \vee y) \& (x \vee z)$$
$$x \vee (y \sim z) = (x \vee y) \sim (x \vee z)$$

4. (*поглощение*) $x \vee xy = x$
5. (*двойное отрицание*) $\overline{\overline{x}} = x$
6. (*закон де Моргана*)

$$\overline{x \vee y} = \overline{x} \& \overline{y}$$
$$\overline{x \& y} = \overline{x} \vee \overline{y}$$

7.

$$\begin{array}{rrrr} x\overline{x} = 0, & x \vee \overline{x} = 1, & x \oplus \overline{x} = 1, & x \sim \overline{x} = 0 \\ xx = x, & x \vee x = x, & x \oplus x = 0, & x \sim x = 1 \\ x\&1 = x, & x \vee 1 = 1, & x \oplus 1 = \overline{x}, & x \sim 1 = x \\ x\&0 = 0, & x \vee 0 = x, & x \oplus 0 = x, & x \sim 0 = \overline{x} \end{array}$$

2 Замыкания.

2.1 Определения.

Возьмем множество $F \subseteq P_2$.

Определение. Замыкание $[F]$ множества F — это множество всех булевых функций, получаемых из булевых функций множества F с помощью операций суперпозиции, удаления и добавления фиктивных переменных.

Определение. F — замкнуто, если $[F] = F$.

1. $[\{x \oplus y\}] = \{0, x, x_1 \oplus \ldots \oplus x_t (t \geqslant 2)\}$

2. P_2 — замкнуто.

Определение. $P_2(n)$ — все булевы функции, существенно зависящие от не более, чем n переменных.

1. $P_2(1)$ — замкнуто.

2. $P_2(2)$ — не замкнуто. ($xy \in P_2(2)$, $xyz \notin P_2(2)$)

2.2 Свойства замыкания.

1. $F \subseteq [F]$.

2. $F_1 \subseteq F_2 \Longrightarrow [F_1] \subseteq [F_2]$

3. $[[F]] = [F]$

   $\square$ 1) $[F] \subseteq [[F]]$ (по 1, 2)

   2)$[[F]] \subseteq [F]$.

   $f(x_1, \dots, x_n) \in [[F]] \Rightarrow \exists$ формула Φ, реализующая f. Пусть $f_1, \dots, f_s$ — все функциональные символы, содержащиеся в Φ. $f_1, \dots, f_s \in [F] \Rightarrow$ каждая функция f_i реализуется некоторой формулой Φ_i над $F : \Phi = f_i(F_1, \dots, F_{n_i})$.

   $\Phi_i(F_1, \dots, F_{n_i})$ — формула, полученная из Φ заменой $x_i \longmapsto F_i$. $\Phi_i(F_1, \dots, F_n)$.

   $\Phi_i(F_1, \dots, F_n)$.

   Так получим:

   Φ' — формулу над F, реализующую функцию $F \Rightarrow f \in [F] \Rightarrow [[F]] \subseteq [F]$. $\blacksquare$

4. $[F_1] \cap [F_2]$ — замкнуто.

   $\square$ Возьмем $f \in [[F_1] \cap [F_2]]$: f реализуется формулой Φ над $[F_1] \cap [F_2]$. Пусть $f_1, \dots f_s$ — все функциональные символы из Φ. $\forall i\, f_i$ реализуется и формулой Φ_1 над F_1 и формулой Φ_2 над $F_2 \Rightarrow f \in [F_1] \cap [F_2]$. $\blacksquare$

5. $[F_1] \cup [F_2]$ не обязательно замкнуто.

2.3 СДНФ и СКНФ.

Пусть F — замкнутое множество, и $F_1 \subseteq F$.

Определение. F_1 называется полным в F, если $[F_1] = F$.

Определение. F_1 называется полным, если $[F_1] = P_2$.

Пример 3.1. P_2 — полное множество.

Утверждение 2.1. *$f(x_1, \dots, x_n)$ — булева функция.*
Тогда: $f(x_1, \dots, x_n) = (\overline{x_1} \,\&\, f(0, x_2, \dots, x_n)) \vee (x_1 \,\&\, f(1, x_2, \dots, x_n))$

$\square$ Пусть $\sigma = (\sigma_1, \dots, \sigma_n)$ — набор значений переменных $x_1, \dots, x_n$.

1. $\sigma_1 = 0$.

   $$\overline{\sigma_1} \,\&\, f(0, \sigma_2, \dots, \sigma_n) \vee \sigma_1 \,\&\, f(1, \sigma_2, \dots, \sigma_n) = \\ = 1 \,\&\, f(0, \sigma_2, \dots, \sigma_n) \vee 0 \,\&\, f(1, \sigma_2, \dots, \sigma_n) = \\ = f(0, \sigma_2, \dots, \sigma_n) = f(\sigma_1, \dots, \sigma_n)$$

2. $\sigma_1 = 1$.

   $$0 \,\&\, f(0, \sigma_2, \dots, \sigma_n) \vee 1 \,\&\, f(1, \sigma_2, \dots, \sigma_n) = \\ = f(1, \sigma_2, \dots, \sigma_n) = f(\sigma_1, \dots, \sigma_n)$$

■

$f(x_1,\dots,x_n) = (\overline{x_1} \,\&\, f(0,x_2,\dots,x_n)) \vee (x_1 \,\&\, f(1,x_2,\dots,x_n)) =$
$= \overline{x_1} \,\&\, (\overline{x_2} \,\&\, f(0,0,\dots,x_n)) \vee (x_2 \,\&\, f(0,1,\dots,x_n)) \vee$
$\vee (x_1 \,\&\, (\overline{x_2} \,\&\, f(1,0,\dots,x_n)) \vee (x_1 \,\&\, f(1,1,\dots,x_n))) =$
$= \overline{x_1 x_2} f(0,0,\dots,x_n) \vee \overline{x_1} x_2 f(0,1,\dots,x_n) \vee x_1 \overline{x_2} f(1,0,\dots,x_n) \vee x_1 x_2 f(1,1,\dots,x_n)$

Определение. $x_\sigma = \begin{cases} x, \text{ если } \sigma = 1 \\ \overline{x}, \text{ если } \sigma = 0 \end{cases}$

Итак, $f(x_1,\dots,x_n)$ можно переписать в виде $\bigvee\limits_{\sigma_1,\sigma_2 \in E} f(\sigma_1,\sigma_2,x_3,\dots,x_n)$.

Мы также можем аналогично разложить f по k переменным:
$f(x_1,\dots,x_n) = \bigvee\limits_{(\sigma_1,\dots,\sigma_k) \in E^k} f(\sigma_1,\dots,\sigma_k,\dots,x_n)$

При $k = n$ получаем: $f(x_1,\dots,x_n) = \bigvee\limits_{(\sigma_1,\dots,\sigma_n) \in E^n} x_1^{\sigma_1} \dots x_n^{\sigma_n} f(\sigma_1,\dots,\sigma_n) =$
$= \bigvee\limits_{\substack{(\sigma_1,\dots,\sigma_n) \in E^n \\ f(\sigma_1,\dots,\sigma_n)=1}} x_1^{\sigma_1} \dots x_n^{\sigma_n}$

Определение. Форма представления функции в виде
$f(x_1,\dots,x_n) = \bigvee\limits_{\substack{(\sigma_1,\dots,\sigma_n) \in E^n \\ f(\sigma_1,\dots,\sigma_n)=1}} x_1^{\sigma_1} \dots x_n^{\sigma_n}$ называется
Совершенной дизъюнктивной нормальной формой (СДНФ).

Определение. Пусть $f(x_1,\dots,x_n) \neq 1$ — булева функция.
$\overline{x} \neq 0 \Rightarrow \overline{f(x_1,\dots,x_n)} = \bigvee\limits_{\substack{(\sigma_1,\dots,\sigma_n) \in E^n \\ \overline{f}(\sigma_1,\dots,\sigma_n)=1}} \overline{x_1^{\sigma_1} \dots x_n^{\sigma_n}} =$
$= \mathop{\&}\limits_{\substack{(\sigma_1,\dots,\sigma_n) \in E^n \\ f(\sigma_1,\dots,\sigma_n)=0}} \overline{x_1^{\sigma_1}} \vee \dots \vee \overline{x_n^{\sigma_n}} = \mathop{\&}\limits_{\substack{(\sigma_1,\dots,\sigma_n) \in E^n \\ f(\sigma_1,\dots,\sigma_n)=0}} x_1^{\overline{\sigma_1}} \vee \dots \vee x_n^{\overline{\sigma_n}}$ — это так называемая
Совершенная конъюктивная нормальная форма (СКНФ).

Утверждение 2.2. *$\{x \& y, x \vee y, \bar{x}\}$ — полное множество.*

□ Если $f \neq 0$, то СДНФ — формула над $\{x \& y, x \vee y, \bar{x}\}$ Если $f = 0$, то $f = \overline{x} \& x \Rightarrow$ любая функция реализуется формулой над $\{x \& y, x \vee y, \bar{x}\}$. ■

Лемма 2.3 (О сводимости полных множеств). *$F, F' \subseteq P_2$, F — полное множество, и любая функция из F может быть реализована формулой над $F' \Rightarrow F'$ — полное множество.*

□ $\forall$ функция из F может быть реализована формулой над $F' \Rightarrow F \subseteq [F'] \Rightarrow [F] \subseteq [[F']] = [F']$.
F — полное $\Rightarrow [F] = P_2, [F] \subseteq [F'] \Rightarrow P_2 \subseteq [F'] \Rightarrow F'$ — полное. ■

2.4 Ещё примеры полных множеств функций.

Утверждение 2.4. *$\{x \& y,\ \bar{x}\}$ — полное множество.*

□ $\{x \vee y,\ x \& y,\ \bar{x}\}$ — полное множество. Учитывая, что $x \vee y = \overline{\bar{x} \& \bar{y}}$, то по лемме о сводимости получаем нужное. ■

Утверждение 2.5. *$\{x \vee y,\ \bar{x}\}$ — полное множество.*

□ $\{x \& y,\ \bar{x}\}$ — полное множество. Учитывая, что: $x \& y = \overline{\bar{x} \vee \bar{y}}$, то по лемме о сводимости получаем нужное. ■

Утверждение 2.6. *$\{x \oplus y,\ x \& y,\ 1\}$ — полное множество.*

□ $\bar{x} = x \oplus 1$. Получаем нужное по лемме о сводимости и утверждению 2. ■

Утверждение 2.7. *$\{x|y\}$ — полное множество.*

□ $x|y = \bar{x} \vee \bar{y} = \overline{x\&y}$;
$\bar{x} = x|x$;
$x\&y = \overline{x|y} = (x|y)|(x|y)$;
$\{x\&y, \bar{x}\}$ — полное по лемме о сводимости, значит $\{x|y\}$ — полное. ■

Следствие 2.1. *Из любого полного множества можно выделить конечное полное подмножество.*

□ $F \subseteq P_2$ — полное множество. $\Rightarrow$ существует формула Φ над F, реализующая $x|y$. Пусть $\{f_1, \ldots, f_s\}$ — множество всех символов функций, содержащихся в Φ.Φ — формула над $\{f_1, \ldots, f_s\} \Rightarrow$ $x|y$ содержится в замыкании. $\{x|y\}$ — полное. $\Rightarrow$ по лемме о сводимости $\{f_1, \ldots, f_s\} \subseteq F$ — полное. ■

2.5 Полином Жегалкина.

Пусть $f(x_1, \ldots, x_n)$ — булева функция.

Определение. *Полиномом Жегалкина* функции f называется полином P с коэффициентами в $\{0, 1\}$ от переменных $x_1, \ldots, x_n$ степени не выше n, такой что $f(x_1, \ldots, x_n) = P(x_1, \ldots, x_n)$.

Утверждение 2.8. *Полином Жегалкина существует для любой функции* $f(x_1, \ldots, x_n)$.

□ $$f(x_1, \ldots, x_n) = \bigvee_{f(\sigma_1 \ldots \sigma_n)=1} x^{\sigma_1} \ldots x^{\sigma_n} = \bigoplus_{f(\sigma_1, \ldots, \sigma_n)=1} x^{\sigma_1} \ldots x^{\sigma_n} =$$

$$= \bigoplus_{f(\sigma_1, \ldots, \sigma_n)=1} (x_1 \oplus \bar{\sigma_1}) \ldots (x_n \oplus \bar{\sigma_n}) = \bigoplus_{k=0}^{n} \Big(\bigoplus_{i_1 < i_2 < \ldots < i_k} c_{i_1, \ldots, i_k} x_{i_1} \ldots x_{i_k} \Big), \text{ где } c_{i_1, \ldots, i_k} \in \{0, 1\}.$$

В этой сумме слагаемое с $k = 0$ соответствует произведению пустого множества переменных, то есть свободному члену. ■

Из определения следует, что если f — константа, то её полином Жегалкина имеет степень 0, то есть равен 1 или 0 (в зависимости от того, какой константой является f, разумеется).

Утверждение 2.9. *Для каждой булевой функции от n переменных существует единственный полином Жегалкина.*

□ Как было доказано выше, для каждой функции полином Жегалкина существует. Далее, очевидно, что разным функциям соответствуют разные полиномы Жегалкина. Покажем, что всевозможных полиномов степени не выше n от переменных $x_1, \ldots, x_n$ ровно столько же, сколько всевозможных булевых функций от этих переменных.
1) $|P_2(n)| = 2^{2^n}$.
2) Каждый коэффициент $c_{i_1, \ldots, i_k}$ соответствует подмножеству $\{x_{i_1}, \ldots, x_{i_k}\}$ (возможно пустому) из множества переменных $\{x_1, \ldots, x_n\}$. Таких подмножеств 2^n. Каждый коэффициент принимает значения 0 или 1, значит, всего полиномов 2^{2^n}. Отсюда всё очевидно. ■

3 Замкнутые классы булевых функций.

3.1 Функции, сохраняющие ноль и единицу.

Определение. f сохраняет 0, если $f(0, \ldots, 0) = 0$. T_0 — множество всех функций, сохраняющих ноль. Например, 0, x, $x\&y$, $x \vee y$, $x \oplus y$.

Определение. Селекторная функция — функция, тождественна равная переменной.

Лемма 3.1. T_0 — *замкнуто.*

□ Тождественная функция содержится в T_0. Значит, надо проверить, что если $f(x_1, \ldots, x_n), g_1, \ldots$ T_0, , то $f(g_1, \ldots, g_n) \in T_0$.
Можем полагать, что $g_1, \ldots, g_n$ зависят от одних и тех же переменных: $x_1, \ldots, x_n$ (иначе

можно добавить переменные в качестве фиктивных). Тогда:
$f(g_1(x_1,\dots,x_n),\dots,g_n(x_1,\dots,x_n)) = h(x_1,\dots,x_n)$
$h(0,\dots,0) = f(g_1(0,\dots,0),\dots,g_n(0,\dots,0)) = f(0,\dots,0) = 0. \Rightarrow h \in T_0$. ■

Определение. f сохраняет 1, если $f(1,\dots,1) = 1$. Обозначим за T_1 множество всех функций, сохраняющих единицу. Например, 1, x, $xy \to y$, $x \vee y$.

Лемма 3.2. T_1 — *замкнуто.*

□ Аналогично предыдущей лемме. ■

3.2 Монотонные функции.

Определим правило сравнения на наборах из нулей и единиц.
$\sigma' = \{\sigma'_1,\dots,\sigma'_n\}$, $\sigma'' = \{\sigma''_1,\dots,\sigma''_n\} \in \{0,1\}^n$.
Будем говорить, что $\sigma' \leqslant \sigma''$, если $\forall i \in \{1,\dots,n\}$ $\sigma'_i \leqslant \sigma''_i$.
Заметим, что существуют несравнимые наборы, например: (101) и (010).

Определение. f — монотонная, если для любых σ' и σ'' таких, что $\sigma' \leqslant \sigma''$ выполняется, что $f(\sigma') \leqslant f(\sigma'')$.

Лемма 3.3. *M является замкнутым классом.*

□ Тождественная функция содержится в M. Значит, осталось проверить, что если $f(x_1,\dots,x_n)$, $g_1,\dots,g_n \in M$, то $h = f(g_1,\dots,g_n) \in M$. Можно считать, что $g_1,\dots g_n$ — функции от одного и того же количества переменных, в противном случае недостающие переменные можно добавить в качестве несущественных. Выберем произвольные различные наборы $\sigma' = \{\sigma'_1,\dots,\sigma'_n\}$, $\sigma'' = \{\sigma''_1,\dots,\sigma''_n\}$, такие что $\sigma' \leqslant \sigma''$.
Рассмотрим $h(\sigma') = f(g_1(\sigma'), g_2(\sigma'),\dots,g_n\sigma'))$ и $h(\sigma'') = f(g_1(\sigma''),\dots,g_n(\sigma''))$.
$g_i(\sigma') < g_i(\sigma'')$, так как g_i — монотонная. $f(g_1(\sigma'), g_2(\sigma'),\dots,g_n(\sigma')) \leqslant f(g_1(\sigma''), g_2(\sigma''),\dots,g_n(\sigma''))$, так как f — монотонная, то h — тоже монотонная. ■

Лемма 3.4 (О немонотонных функциях). *$f(x_1,\dots,x_n) \notin M$. Тогда $\bar{x} \in [\{f;0;1\}]$.*

□ $f \notin M \Rightarrow \exists\, \sigma',\sigma'' : \sigma' \leqslant \sigma'',\ f(\sigma') = 1,\ f(\sigma'') = 0$. Без ограничения общности будем считать, что σ' и σ'' устроены следующим образом:
$\sigma' = (0,\dots,0,\dots,0,1,\dots,1)$
$\sigma'' = (\underbrace{1,\dots,1}_{k},\underbrace{0,\dots,0}_{s},\underbrace{1,\dots,1}_{n-k-s})$
$g(x) = f(\underbrace{x,\dots,x}_{k},\underbrace{0,\dots,0}_{s},\underbrace{1,\dots,1}_{n-k-s}) = \bar{x}$, так как $g(0) = 1$ и $g(1) = 0$. ■

3.3 Самодвойственные функции.

Определение. Двойственной функцией к $f(x_1,\dots,x_n)$ называется функция $f^*(x_1,\dots,x_n) = \overline{f(\bar{x}_1,\dots,\bar{x}_n)}$.

Пример 3.1. $(x\&y)^* = x \vee y$
Легко заметить, что $(f^*)^* = f$.

Определение. Самодвойственная функция — функция, двойственная самой себе; множество всех таких функций обозначается S.

Утверждение 3.5. *1)* $\bar{x}, x \oplus y \oplus z, m(x,y,z) \in S$*; 2)* $0, 1, x \oplus y, x \to y, x\&y, x \vee y \notin S$

□ В этом несложно убедиться явной проверкой. ■

Лемма 3.6. *S является замкнутым классом.*

□ Тождественная функция содержится в S. Значит, осталось проверить, что если $f(x_1,\dots,x_k), g_1,\dots,g_k \in S$, то $h = f(g_1(x_1,\dots,x_n),\dots,g_k(x_1,\dots,x_n)) \in S$.
$h^*(x_1,\dots,x_n) = \overline{f(g_1(\bar{x}_1,\dots,\bar{x}_n)),\dots,g_k(\bar{x}_1,\dots,\bar{x}_n)} = \overline{f(\overline{\overline{g_1(\bar{x}_1,\dots,\bar{x}_n)}},\dots,\overline{\overline{g_k(\bar{x}_1,\dots,\bar{x}_n)}}} =$

$\overline{f(\overline{g_1^*(x_1,\ldots,x_n)},\ldots,\overline{g_k^*(x_1,\ldots,x_n)}}$.
Так как $g_1 = g_1^*, \ldots, g_k = g_k^*$, то
$h = \overline{f(\overline{g_1(x_1,\ldots,x_n)},\ldots,\overline{g_k(x_1,\ldots,x_n)}} = f^*(g_1(x_1,\ldots,x_n),\ldots,g_k(x_1,\ldots,x_n))$.
$f^* = f$, значит $h^*(x_1,\ldots,x_n) = f^*(x_1,\ldots,x_n) = f(x_1,\ldots,x_n) =$
$= h(x_1,\ldots,x_n) \Rightarrow h \in S$. ■

Лемма 3.7 (О несамодвойственной функции). *Пусть* $f(x_1,\ldots,x_n) \notin S$, *тогда* $0, 1 \in [\{f,\bar{x}\}]$

□ Пусть $f(x_1,\ldots,x_n) \notin S$, тогда $f^*(x_1,\ldots,x_n) = \overline{f(\bar{x}_1,\ldots,\bar{x}_n)} \neq f(x_1,\ldots,x_n) \Rightarrow \exists\sigma = (\sigma_1,\ldots,\sigma_n)$, т.ч. $\overline{f(\bar{\sigma}_1,\ldots,\bar{\sigma}_n)} \neq f(\sigma_1,\ldots,\sigma_n) \Rightarrow f(\bar{\sigma}_1,\ldots,\bar{\sigma}_n) = f(\sigma_1,\ldots,\sigma_n) = C$.
Будем считать, что $(\sigma_1,\ldots,\sigma_n) = (\underbrace{0,\ldots,0}_{k},\underbrace{1,\ldots,1}_{n-k})$.
Пусть $g(x) = f(\underbrace{x,\ldots,x}_{k},\underbrace{\bar{x},\ldots,\bar{x}}_{n-k})$.
$g(0) = f(\underbrace{0,\ldots,0}_{k},\underbrace{1,\ldots,1}_{n-k}) = f(\sigma_1,\ldots,\sigma_n)$,
$g(1) = f(\underbrace{1,\ldots,1}_{k},\underbrace{0,\ldots,0}_{n-k}) = f(\bar{\sigma}_1,\ldots,\bar{\sigma}_n)$,
значит, $g(0) = g(1) = C$, причём g задаётся формулой над $\{f,\,\bar{x}\} \Rightarrow g \in S$.
Получаем $C \in [\{f,\bar{x}\}] \Rightarrow \bar{C} \in [\{f,\bar{x}\}] \Rightarrow 0,\,1 \in [\{f,\bar{x}\}]$. ■

3.4 Линейные функции.

Определение. Булева функция называется линейной, если степень её полинома Жегалкина не превосходит 1.

Здесь под степенью полинома Жегалкина понимается максимальная длина слагаемого в нём или, говоря алгебраическим языком, его степень как многочлена над $\mathbb{Z}_2$. Например, степень полинома $xyz \oplus x \oplus 1$ равна 3.

Определение. L — класс всех линейных булевых функций.

Предложение 3.8. *1)* $0,\,1,\,x,\,\bar{x},\,x\oplus y,\,x\sim y \in L$, *2)* $x \to y,\,x\vee y,\,x\&y \notin L$.

□ Первая часть утверждения очевидна, кроме утверждения про функцию $x \sim y$. Чтобы доказать оставшееся, представим следующие функции в виде полиномов:
$x \sim y = x \oplus y \oplus 1$ $(\deg = 1)$,
$x \to y = \bar{x} \vee xy = xy \oplus x \oplus 1$ $(\deg = 2)$,
$x \vee y = xy \oplus x \oplus y$ $(\deg = 2)$. ■

Лемма 3.9. *L является замкнутым классом.*

□ $x \in L$. Достаточно доказать, что $f(x_1,\ldots,x_k)$, $g_1(x_1,\ldots,x_n)$, $\ldots$,
$g_k(x_1,\ldots,x_n) \in L \Rightarrow h(x_1,\ldots,x_n) = f(g_1(x_1,\ldots,x_n),\ldots,g_k(x_1,\ldots,x_n)) \in L$.
Проверим это напрямую:
$f \in L \Rightarrow f(x_1,\ldots,x_k) = c_1x_1 \oplus \ldots \oplus c_kx_k \oplus c;\ c_i, c \in \{0,1\}$.
$g_1,\ldots,g_k \in L \Rightarrow g_i(x_1,\ldots,x_n) = d_{i1}x_1 \oplus \ldots \oplus d_{in}x_n \oplus d_i;\ d_{ij}, d_i \in \{0,1\}$.
$h(x_1,\ldots,x_n) = c_1\big(d_{11}x_1 \oplus \ldots \oplus d_{1n}x_n \oplus d_1\big) \oplus \ldots \oplus c_k\big(d_{k1}x_1 \oplus \ldots \oplus d_{kn}x_n \oplus d_k\big) \oplus c =$
$= (c_1d_{11} \oplus c_kd_{k1})x_1 \oplus \ldots \oplus (c_1d_{1n} \oplus \ldots \oplus c_kd_{kn})x_n \oplus (c_1d_1 \oplus \ldots c_kd_k \oplus c)$. Видно, что это линейная функция. ■

Лемма 3.10 (О нелинейной функции). *Пусть* $f(x_1,\ldots,x_n) \notin L$. *Тогда* $x\&y \in [\{f,\bar{x},0,1\}]$.

□ Пусть $f \notin L$, тогда степень её полинома Жегалкина равна $k \geqslant 2$. Выберем нелинейное слагаемое наименьшей степени $l \geqslant 2$ в этом полиноме. Без ограничения общности можно считать, что это слагаемое $x_1 ... x_l$. Запишем f в виде $f(x_1,\ldots,x_n) = f_{\deg > l} \oplus x_1...x_l \oplus f_{\deg \leqslant 1}$, где $f_{\deg > l}$ — сумма всех слагаемых степени больше l, а $f_{\deg \leqslant 1}$ — сумма всех слагаемых степени не больше 1.

Рассмотрим функцию $g(x,y) = f(x, \overbrace{y,...,y}^{l-1}, 0,...,0)$. Ясно, что при подстановке аргументов $(x, y, ..., y, 0, ..., 0)$ в полином Жегалкина для f занулятся все слагаемые, входящие в $f_{\deg > l}$. Далее, $g(x,y) = x\underbrace{y...y}_{l-1} \oplus \ldots = xy \oplus c_1 x \oplus c_2 y \oplus c$.

Теперь рассмотрим функцию $g'(x,y) = g(x \oplus c_2, y \oplus c_1) = xy \oplus c_1c_2 \oplus c = xy \oplus d$. Значит, $xy = g'(x,y) \oplus d = g(x \oplus c_2, y \oplus c_1) \oplus d = f(x \oplus c_2, \underbrace{y \oplus c_1, \ldots, y \oplus c_1}_{l-1}, 0, \ldots, 0) \oplus d$.

Так как $x \oplus d = x$ при $d = 0$ и $x \oplus d = \bar{x}$ при $d = 1$, то $xy \in [\{f, \bar{x}, 0, 1\}]$. ■

3.5 Критерий Поста.

Теорема 3.11 (Критерий полноты). *Пусть $\mathcal{F} \subseteq P_2$, тогда*
$\mathcal{F}$ является полной в $P_2 \iff \mathcal{F}$ не содержится ни в одном из классов T_0, T_1, M, L, S.

□
1. $(\Rightarrow)$. Пусть X — один из классов T_0, T_1, M, L, S. Они замкнуты, то есть $[X] = X$. Предположим, $\mathcal{F} \subseteq X$, тогда $[\mathcal{F}] \subseteq [X] = X \neq P_2$. Противоречие. Значит, $\mathcal{F}$ не содержится ни в одном из классов T_0, T_1, M, L, S.
2. $(\Leftarrow)$. Пусть $\mathcal{F}$ не содержится ни в одном из классов T_0, T_1, M, L, S. Тогда существуют функции $f_X \in \mathcal{F} \setminus X$, где $X \in \{T_0, T_1, M, L, S\}$. Получим из этих функций константы, отрицание и дизъюнкцию.
$f_{T_0} \notin T_0 \Rightarrow f_{T_0}(0, \ldots, 0) = 1$, аналогично $f_{T_1} \notin T_1 \Rightarrow f_{T_1}(1, \ldots, 1) = 0$. Положим $\varphi(x) = f_{T_0}(x, \ldots, x)$. Ясно, что $\varphi(0) = 1$. Если $\varphi(1) = 1$, то это константа 1, а функция $\psi(x) = f_{T_1}(\varphi(x), \ldots, \varphi(x))$ — константа 0. Если же $\varphi(1) = 1$, то $\varphi(x) = \bar{x}$, и по лемме о несамодвойственной функции при помощи отрицания можно получить обе константы. По лемме о немонотонной функции, из f_M, имея константы, можно получить отрицание. По лемме о нелинейной функции при помощи констант и отрицания можно получить конъюнкцию. Таким образом, мы выделили в F полную подсистему, а значит, $[\mathcal{F}] = P_2$. ■

Следствие 3.1. *Из любого полного множества функций можно выделить полное подмножество из $\leqslant 5$ функций.*

□ Достаточно взять функции f_{T_0}, f_{T_1}, f_M, f_S, f_L, которые содержатся (по теореме 1) в этом полном множестве. ■

Следствие 3.2. *Из любого полного множества функций $\mathcal{F}$ можно выделить полное подмножество из $\leqslant 4$ функций.*

□ 1) Пусть $f_{T_0}(1, \ldots, 1) = 0$, тогда $f_{T_0} \notin M$ и $\{f_{T_0}, f_{T_1}, f_S, f_L\}$ — полное подмножество в $\mathcal{F}$.
2) Пусть $f_{T_0}(1, \ldots, 1) = 1$, тогда $f_{T_0} \notin S$ и $\{f_{T_0}, f_{T_1}, f_M, f_L\}$ — полное подмножество в $\mathcal{F}$. ■

Замечание. Для 3 функций утверждение уже будет неверным. В качестве полной системы из 4 функций можно рассмотреть $\{xy, x \oplus y \oplus z, 0, 1\}$. Наглядно изобразить принадлежность этих функций разным замкнутым классам можно следующей таблицей:

	T_0	T_1	M	S	L
xy	$\in$	$\in$	$\in$	$\notin$	$\notin$
$x \oplus y \oplus z$	$\in$	$\in$	$\notin$	$\in$	$\in$
0	$\in$	$\notin$	$\in$	$\notin$	$\in$
1	$\notin$	$\in$	$\in$	$\notin$	$\in$

При этом, если удалить любую из этих четырёх функций, то получившаяся система уже будет неполной ввиду принадлежности одному из классов T_0, T_1, M, L, S.

3.6 Предполные классы

Определение. Пусть $F \subseteq P_2$. Тогда F – предполный, если:

1. $F \neq P_2$
2. $[F] = F$
3. $\forall f \notin F : [F \cup f] = P_2$

В клетке таблице снизу стоит функция $\in$ строке и $\notin$ столбцу $\Rightarrow$ ни один из классов не содержится в другом.

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

Теорема 3.12. T_0, T_1, S, M, L *– множество всех предполных классов.*

$\square$ Пусть есть $A = [A]$ – предполный. Возьмем класс M.
Пусть $A \subset M \Rightarrow \exists f \in M \setminus A : [A \cup f] \subseteq [M] = M$.
Аналогичные рассуждения можно провести и для остальных классов. $\blacksquare$

3.7 Принцип двойственности

Формулировка.
Пусть формула Φ над F задает функцию f. Формула Φ', получающаяся из Φ путем замены $f_i \to f_i^*$ будет реализовывать f^*.
$\Big($Напомним, что функция $f^*(x_1, \ldots, x_n) = \overline{f(\overline{x_1}, \ldots, \overline{x_n})}\Big)$
Идея:
$\overline{f_0(\overline{\overline{\overline{f_{i_1}(\ldots)}}}, \ldots, \overline{\overline{\overline{f_{i_k}(\ldots)}}})}$ – возникаю двойные отрицания, которые изчезают, кроме *верхних* и *нижних*, что как раз дает функцию f^*.

4 Сложность.

5 Лекция 7 (продолжение оценки функции Шеннона).

5.1 В предыдущих сериях

Мы уже имеем для функции Шеннона следующую оценку скорости роста:

$$n \leqslant L(n) \leqslant 6 \cdot \frac{2^n}{n}$$

Попробуем теперь ее улучшить.
Напомним, что:

Определение. Приведенная схема — схема, в которой все элементы выполняют разные функции, то есть не существует таких двух одинаковых элементов, на входы которых подаются одни и те же переменные или результаты вычисления других функций.

Все булевы функции в этой лекции будем считать от переменных $x_1, \ldots, x_n$. Также все выкладки проводятся в выбранном «стандартном» базисе $\{\&, \vee, \neg\}$, если не указано обратное.

5.2 Определения.

Определение. $N_{=(n,l)}$ — число приведенных схем сложности l со входами $x_1, \ldots, x_n$.

Определение. $N_{\leqslant(n,l)}$ — число приведенных схем сложности не выше l со входами $x_1, \ldots, x_n$.

5.3 Основная оценка.

Лемма 5.1. *При достаточно больших n при $l \geqslant n$ $\exists C > 0$ выполняется неравенство*

$$N_{\leqslant(n,l)} \leqslant (C \cdot l)^l$$

Пусть S — приведенная схема сложности l со входами $x_1, \ldots, x_n$. Пронумеруем элементы схемы и зафиксируем нумерацию Num. Пусть L_i — элемент схемы, имеющий в данной нумерации номер i. На множестве пар из схемы и нумерации на ней введем функцию $t(S, Num) = T$, где T — таблица вида:

f	E_1	E_2
$\&$	x_1	x_3
$\vee$	x_1	x_3
$\neg$	x_2	x_2
$\vee$	x_2	L_2
$\&$	L_6	L_4
$\vee$	L_1	L_3

Таблица состоит из l строк и трёх столбцов, в строчке с номером i в первом столбце стоит знак функции, которую реализует элемент L_i, а в двух других — элементы множества $\{L_1, \ldots, L_l, x_1, \ldots, x_n\}$, которые поступают на вход этой функции. Если функция в левом столбце — отрицание, в два правых столбца запишем один и тот же элемент из вышеуказанного множества, над которым производится отрицание. Например, на схеме, задаваемой таблицей выше, переменные x_1 и x_3 передаются на элемент «и» (первая строчка), результат передаётся вместе с отрицанием переменной x_2 на вход элемента «или» (шестая строчка) и т.д. Также обозначим за a номер строки с элементом, выход которого является выходом всей схемы (тут $a = 5$).
По такой таблице, построенной по схеме и нумерации, можно однозначно восстановить схему S.

Обозначим за N_l число таблиц, соответствующих всем парам (S, Num) заданной сложности l. Имеет место оценка

$$N_l \leqslant 3^l \cdot (l+n)^{2l} \cdot l \leqslant 3^l \cdot 2l^{2l} \cdot l = (3 \cdot 2^2)^l \cdot l^{2l} \cdot l = 12^l \cdot l^{2l} \cdot l \leqslant 13^l \cdot l^{2l}.$$

Первое неравенство очевидно. Второе неравенство следует из предположения $n \leqslant l$, при котором мы доказываем лемму. Последнее неравенство верно асимптотически и следует из неравенства $12^l \cdot l \leqslant 13^l$.

Утверждение 5.2. *Пусть схема S — приведенная, $Num_1 \neq Num_2$ — две ее нумерации, $t(S, Num_1) = T_1$; $t(S, Num_2) = T_2$, тогда $T_1 \neq T_2$*

□ Предположим, что $T_1 = T_2$.

Введем на S еще одну монотонную нумерацию Num_0 и зафиксируем ее. Дальше, перебирая по порядку нумерации Num_0 элементы схемы S найдем первый элемент L_i (по нумерации Num_0), такой, что он имеет в Num_1 и Num_2 номера k_1 и k_2, причем $k_1 \neq k_2$. Такой элемент существует, потому что $Num_1 \neq Num_2$. Рассмотрим строки k_1 и k_2 таблиц T_1 и T_2 соответственно.

В первой их клетке стоит один и тот же знак, так как функция, которую реализует элемент, не зависит от нумерации. Для двух других клеток есть две возможности: либо там стоит знак переменной, тогда они тоже одинаковы, либо элемент множества $\{L_1 \cdots L_l\}$, для каждой таблицы в своей нумерации.
Посмотрим, «выход» каких элементов может подаваться на «вход» элемента L_i (в нумерации Num_0). Так как Num_0 — монотонная, то это могут быть только элементы с меньшим номером в данной операции. Но для элементов с меньшим номером в Num_0 их номера в Num_1 и Num_2 совпадают.
Это значит, что строчки k_1 в T_1 и k_2 в T_2 одинаковые. Так как таблицы (по нашему предположению) одинаковые, то в таблице T_1 строчка с номером $k_2 \neq k_1$ совпадает со строчкой с тем же номером в T_2, которая, в свою очередь, совпадает со строчкой k_1 в T_1. Это значит, что в T_1 есть две одинаковые строчки. Другими словами, в схеме S есть два элемента, реализующие одинаковые функции. Это противоречит с приведенностью S.
Итак, $T_1 \neq T_2$ ■

Значит, число таблиц, соответствующей какой-либо схеме равно числу способов пронумеровать элементы этой схемы. Тогда, учитывая, что число способов пронумеровать l элементов — $l!$, и что $l! \geqslant (\frac{l}{3})^l$:

$$N_{=(n,l)} = \frac{N_l}{l!} \leqslant \frac{13^l \cdot l^{2l}}{l!} \leqslant 39^l \cdot l^l$$

Тогда:

$$N_{\leqslant(n,l)} \leqslant \sum_{i=0}^{l} N_{=(n,i)} \leqslant (l+1) \cdot 39^l \cdot l^l \leqslant (40l)^l$$

Данная оценка завершает доказательство леммы.

Утверждение 5.3.

$$L(n) \geqslant \frac{2^n}{n}$$

□ Положим $l_\varepsilon = (1-\varepsilon) \cdot \frac{2^n}{n}$, $0 < \varepsilon < 1$
При любом ε из заданного интервала верна оценка:

$$\log_2 \frac{N_{\leqslant(n,l_\varepsilon)}}{2^{2^n}} \leqslant l_\varepsilon \cdot \log_2 (C \cdot l_\varepsilon) - 2^n \leqslant (1-\varepsilon) \cdot \frac{2^n}{n} \cdot \log_2 2^n - 2^n = -\varepsilon \cdot \frac{2^n}{n}$$

При $n \to +\infty$ отношение $\dfrac{N_{\leqslant(n,l_\varepsilon)}}{2^{2^n}}$ стремится к нулю.

Это значит, что при достаточно больших n число функций, которые можно реализовать при помощи схем, сложности меньше $\frac{2^n}{n}$, много меньше числа всех функций от n переменных. А это значит, что существуют функции, сложность которых больше или равна $\frac{2^n}{n}$. А это и значит, что

$$L(n) \geqslant \frac{2^n}{n}$$

■

Теорема 5.4. *Пусть* $n \to +\infty$ *, тогда*

$$L(n) - \frac{2^n}{n} \geqslant \frac{2^n \log_2 n}{n^2}$$

□ Пусть $\varepsilon > 0$ — фиксировано. Положим $l_\varepsilon = \frac{2^n}{n} + (1-\varepsilon) \cdot \frac{2^n \log_2 n}{n^2}$.
Так как $\log_2 n \leqslant n$ при больших n, то $l_\varepsilon = \frac{2^n}{n} + (1-\varepsilon) \cdot \frac{2^n \log_2 n}{n^2} \leqslant 2 \cdot \frac{2^n}{n}$ и $C \cdot l_\varepsilon \leqslant 2C \cdot \frac{2^n}{n}$.

$$\log_2 \frac{N_{\leqslant(n,l_\varepsilon)}}{2^{2^n}} \leqslant \log_2 \frac{(Cl_\varepsilon)^{l_\varepsilon}}{2^{2^n}} = l_\varepsilon \log_2 Cl_\varepsilon - 2^n = (*).$$

Подставляем выражение для l_ε перед логарифмом в $(*)$, получаем:

$$(*) = \Big(\frac{2^n}{n} + (1-\varepsilon)\frac{2^n \log_2 n}{n^2}\Big) \cdot \log_2(Cl_\varepsilon) - 2^n \leqslant \Big(\frac{2^n}{n} + (1-\varepsilon)\frac{2^n \log_2 n}{n^2}\Big) \cdot \log_2(2C \cdot \frac{2^n}{n}) - 2^n =$$

$$= \Big(\frac{2^n}{n} + \frac{2^n \log_2 n}{n^2} - \varepsilon\frac{2^n \log_2 n}{n^2}\Big) \cdot (\log_2 2c + n - \log_2 n) - 2^n =$$

$$= 2^n - \frac{2^n \log_2 n}{n} + \frac{2^n \log_2 n}{n} - \varepsilon\frac{2^n \log_2 n}{n} - 2^n + \bar{o}\big(\frac{2^n \log_2 n}{n}\big) = -\varepsilon\frac{2^n \log_2 n}{n} + \bar{o}\big(\frac{2^n \log_2 n}{n}\big).$$

Получили оценку $\log_2 \frac{N_{\leqslant(n,l_\varepsilon)}}{2^{2^n}} \leqslant -\varepsilon\frac{2^n \log_2 n}{n} + \bar{o}\big(\frac{2^n \log_2 n}{n}\big)$; правая часть стремится к $-\infty$ при $n \to +\infty$, значит, $\frac{N_{\leqslant(n,l_\varepsilon)}}{2^{2^n}} \to 0$, значит, $L(n) \geqslant l_\varepsilon$.

Рассуждение верно для любого сколь угодно малого $\varepsilon > 0$. Переходя к пределу при $\varepsilon \to 0$, получаем утверждение теоремы. ■