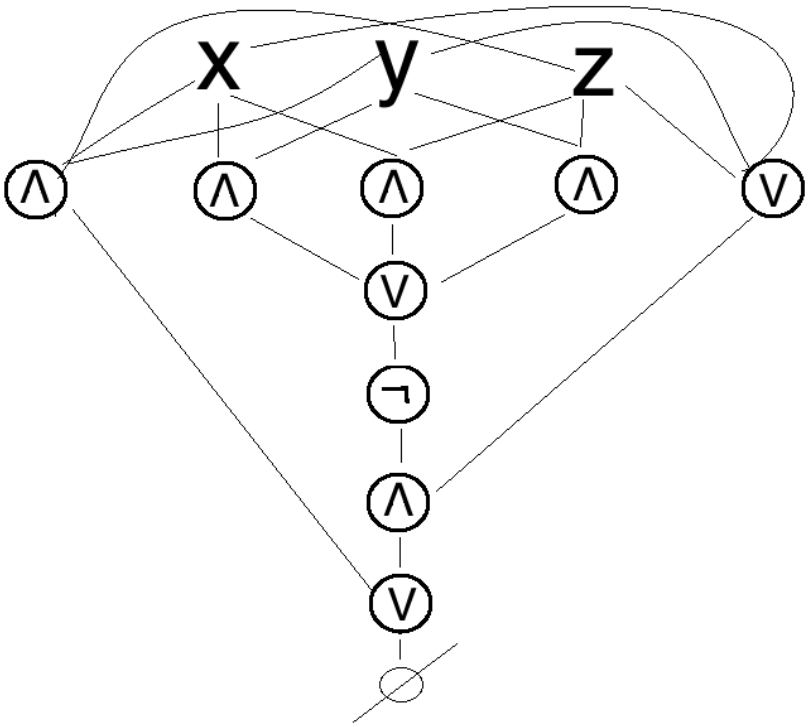
Егерев Артем
Домашнее задание №18

Задача 1

Докажите, что функцию $x \oplus y \oplus z$ можно вычислить схемой, используя лишь одно отрицание (и много конъюнкций и дизъюнкций).

Решение:

Рассмотрим все варианты, когда функция дает нам положительный результат $\rightarrow$ сумма равна 1 или 3 по модулю 2 $\Rightarrow$ 2 варианта: одна из переменных равна 1, остальные 0 или все равны 1.
Первое есть $(x \wedge y \wedge z)$
Второе есть $\neg((x \wedge y) \vee (x \wedge z) \vee (y \wedge z)) \wedge (x \vee y \vee z)$
В виде схемы это будет выглядеть следующим образом:



Задача 2

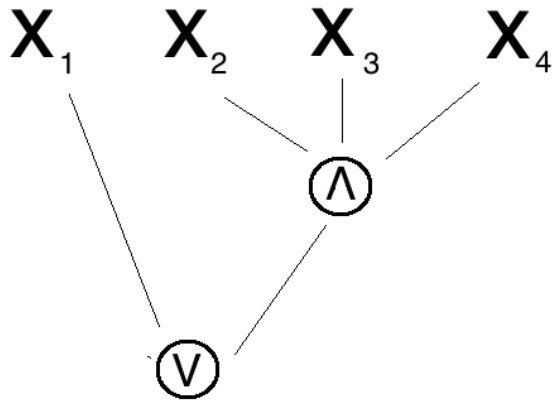
Функция $f(x_1, x_2, x_3, x_4)$ истинна на последних 9 наборах значений переменный (в стандатрном порядке) и только на них. Постройте схему, вычисляющая f, использующую только диъюнкцию и конъюнкцию длины не более чем 15.

Решение:

Выпишем в таблицу значения, на которых функция равна 1:

x_1	x_2	x_3	x_4
0	1	1	1
1	0	0	0
1	0	0	1
1	0	1	0
1	0	1	1
1	1	0	0
1	1	0	1
1	1	1	0
1	1	1	1

$\Rightarrow f(x) \Longleftrightarrow x_1 \vee (x_2 \wedge x_3 \wedge x_4)$:



Размер схемы - $11 < 15$.

Задача 3

Постройте схему полиномиального размера, проверяющую, что во входное слово входит подслово 101. Можно считать, что длина входного слова не меньше, чем 3

Решение:

Пусть n - размер входного слова. Тогда наша схема запишется в строку:

$$x_1, x_2 ... x_n;$$
$$\overline{x_2}, \overline{x_3} ... \overline{x_{n-1}} \ ;$$
$$(x_1 \wedge \overline{x_2} \wedge x_3), (x_2 \wedge \overline{x_3} \wedge x_4), ... (x_{n-2} \wedge \overline{x_{n-1}} \wedge x_n);$$
$$(x_1 \wedge \overline{x_2} \wedge x_3) \vee (x_2 \wedge \overline{x_3} \wedge x_4) ... (x_{n-2} \wedge \overline{x_{n-1}} \wedge x_n);$$

Оценим теперь рамер этой схемы. На каждом из 4 этапов мы вычисляем не более n элементов $\Rightarrow$ как следствие, суммарно нам потребуется $O(n)$ элементов.

Задача 4

Посройте схему полиномиального размера, умнощающее двоичное число на 3.

Решение:

Для удобства определим сразу функции, которыми мы будем пользоваться в дальнейшем :

$$XOR(x, y) \Leftrightarrow x \oplus y :$$
$$x, y; \quad \overline{x}, \overline{y}; \quad (\overline{x} \wedge y), (x \wedge \overline{y}); \quad (\overline{x} \wedge y) \vee (x \wedge \overline{y})$$

$$MAJ(x, y, z) :$$
$$x, y, z; \quad \overline{x}, \overline{y}, \overline{z}; \quad (x \wedge y), (x \wedge z), (y \wedge z); \quad (x \wedge y) \vee (x \wedge z) \vee (y \wedge z)$$

Умножение на 3 есть сумма 3 чисел, равных данному, поэтому для определения схемы нам достаточно определить сложение двух двоичных чисел: пусть n - длина большего числа, тогда первое число в сумме представимо в виде : $\overline{a_n a_{n-1} ... a_1 a_0}$, второе: $\overline{b_n b_{n-1} ... b_1 b_0}$. Будем записывать в c_i дополнительную единицу, которая получается при сложение (по аналогии с обычным сложением). Обозначим результат сложения за: $\overline{d_{n+1} d_n ... d_1 d_0}$. $c_0 = 0$ соответственно. Тогда, для каждого i от 0 до $n+1$: $d_i = a_i \oplus b_i \oplus c_i$; $c_{i+1} = MAJ(a_i, b_i, c_i)$ (исходя из правил сложения). Таким образом, мы можем однозначно определить нашу схему.

Оценим теперь размер этой схемы. Нам нужно посчитать сумму 2 раза. Для каждого разряда нам нужно не более 2-х раз применить подсхему для вычисления $\oplus$ и не более 1-ого раза подсхему для вычисления MAJ_3. Все схемы имеют постоянный размер, отсюда нам нужно всего $O(n)$ элементов.

Задача 5

Постойте схему полиномиального размера, проверяющую, будет ли n - битное двоичное число делиться на 3.

Решение:

Двоичное число представимо в виде: $a = \overline{a_n a_{n-1} ... a_1 a_0} = a_n 2^n + a_{n-1} 2^{n-1} ... + a_1 2^1 + a_0$.
Посмотрим какой остаток дает нам каждое слагаемое при деление на 3:

$$\begin{cases} a_k 2^{2i} \equiv a_k 4^i \equiv a_k \text{ по модулю 3} & // \text{при четном } k \\ a_k 2^{2i+1} \equiv a_k 4^i \cdot 2 \equiv -a_k \text{ по модулю 3} & // \text{при нечетном } k \end{cases}$$

$\Rightarrow a \equiv a_0 - a_1 + a_2 ...$ по модулю 3.
Найдем остаток a при деление на 3. Для этого мы введем 2 бита u_1 и u_2, которые будут равны $\overline{u_1 u_2} = 00, 01, 10$ и будут символизировать остатки 0, 1, 2 соответственно.

Изначально $\overline{u_1 u_2} = 00$. Далее мы будем идти по каждой цифре и в зависимости от индекса k и значения a_k менять значения u_1, u_2 на:

$$\begin{cases} k - \text{четное} \begin{cases} a_k = 0 \quad (0,1,2) \to (0,1,2) \\ a_k = 1 \quad (0,1,2) \to (1,2,0) \end{cases} \\ k - \text{нечетное} \begin{cases} a_k = 0 \quad (0,1,2) \to (0,1,2) \\ a_k = 1 \quad (0,1,2) \to (2,0,1) \end{cases} \end{cases}$$

Таким образом, если в конце мы получаем $\overline{u_1 u_2} = 00 \Rightarrow a \vdots 3$
Теперь по-подробнее как мы производим следующие преобразования (новые u_1, u_2

относительно старых u'_1, u'_2):

$$
\begin{gathered}
(0,1,2) \to (0,1,2): \\
u_2 = u'_2 \\
u_1 = u'_1 \\
(0,1,2) \to (1,2,0): \\
u_2 = \overline{u'_1} \wedge \overline{u'_2} \\
u_1 = u'_2 \\
(0,1,2) \to (2,0,1): \\
u_2 = u'_1 \wedge \overline{u'_2} \\
u_1 = \overline{u'_1} \wedge \overline{u'_2}
\end{gathered}
$$

Запихнув в один блок обработку 2-х последовательных цифр числа (тем самым сразу обработав одно четное и одно нечетное k) мы получаем в этом блоке константное количество действий. Оценим теперь размер этой схемы. Нам нужно зайти в блок не более, чем $\lceil \frac{1}{2}n \rceil$ раз. Каждый блок это константа. Отсюда нам нужно всего $O(n)$ элементов.