Нешина Екатерина М1-14

Билет 2

Лемма о нелинейной функции

Обозначим за L класс линейных функций из P_2.

Определение 1

Функция из P_2 называется линейной, если её полином Жегалкина степени не выше один.

Замкнутость класса L

Класс линейных функций замкнут.

Доказательство

Пусть есть линейная функция $f(x_1, ..., x_n)$. Для того, чтобы проверить, является ли класс L замкнутым, достаточно проверить, не выводят ли операции суперпозиций над функциями за пределы класса. Так как функция линейная, то она представима в виде полинома Жегалкина степени не выше один:
$f(x_1, ..., x_n) = a_0 + a_1 \cdot x_1 + ... + a_n \cdot x_n$.
Разбираем случаи:
1. Добавление фиктивной переменной.
Пусть x_{n+1} новая фиктивная переменная, тогда коэффициент при этой переменной в полиноме Жегалкина будет равен нулю. Соответственно, при добавлении этой переменной функция останется линейной.
2. Удаление фиктивной переменной.
Пусть x_n фиктивная переменная, тогда коэффициент при этой переменной в полиноме Жегалкина будет равен нулю. Соответственно, при удалении этой переменной функция останется линейной.
3. Переименование переменных.
Пусть над переменными $x_1, ..., x_n$ совершили перестановку. Обозначим переставленные переменные за $y_1, ..., y_n$. Получим новую функцию:
$F(y_1, ..., y_n) = a_0 + a_1 \cdot y_1 + ... + a_n \cdot y_n$, которая также является линейной.
4. Отождествление переменных.
Пусть отождествлены (без ограничения общности) первые m переменных, тогда

$f(x_1, ..., x_m) = a_0 + a_1 \cdot x_1 + ... + a_n \cdot x_m$.
5. Операция подстановки.
Пусть есть две линейные функции
$f(x_1, ..., x_n) = a_0 + a_1 \cdot x_1 + ... + a_n \cdot x_n$ и $g(x_1, ..., x_m) = a_0 + a_1 \cdot x_1 + ... + a_n \cdot x_m$.
Без ограничения общности, подставим функцию $g(x_1, ..., x_m)$ в функцию $f(x_1, ..., x_n)$ вместо переменной x_1. Получим
$f(x_1, ..., x_n) = a_0 + a_1 \cdot g(x_1, ..., x_m) + ... + a_n \cdot x_n = a_0 + a_1 \cdot (a_0 + a_1 \cdot x_1 + ... + a_n \cdot x_m) + ... + a_n$. Получили линейную функцию.

Теорема доказана.

Лемма о нелинейной функции

Если функция $f(x_1, ..., x_n) \notin L$, то из неё путём подстановки констант 0 и 1, и функций вида x и $\overline{x}$ в переменные и может быть навешивания отрицания над самой функцией, можно получить функцию $x_1 \& x_2$.

Доказательство:

Представим нелинейную функцию $f(x_1, ..., x_n)$ в виде полинома Жегалкина. Так как функция нелинейная, то существует слагаемое в полиноме, содержащее не менее двух множителей. Без ограничения общности, пусть это будет конъюнкция $x_1 \& x_2$, то есть:

$f(x_1, ..., x_n) = x_1 \& x_2 \& f_1(x_3, ..., x_n) + x_1 \& f_2(x_3, ..., x_n) + x_2 \& f_3(x_3, ..., x_n) + f_4(x_3, ..., x_n)$.

Пусть $f_1(x_3, ..., x_n) = 0$, значит слагаемое $x_1 \& x_2$ зануляется. Если дальше будут проводится аналогичные рассуждения, то в итоге конъюнкцию вывести не получится. Значит $f_1(x_3, ..., x_n) = 1$.

Найдутся такие константы, что $a = f_2(x_3, ..., x_n), b = f_3(x_3, ..., x_n), c = f_4(x_3, ..., x_n)$.

Получаем: $f(x_1, ..., x_n) = x_1 \& x_2 + x_1 \& a + x_2 \& b + c$.

Если $a = b = c = 0$, то получится сразу конъюнкция.

Рассмотрим случай, когда a, b, c не равняются нулю.

Навесим отрицание на x_1, тогда получим:
$f(x_1, ..., x_n) = \overline{x_1} \& x_2 + \overline{x_1} \& a + x_2 \& b + c = (x_1 + 1) \& x_2 + (x_1 + 1) \& a + x_2 \& b + c = x_1 \& x_2 + x_2 + x_1 \& a + a + x_2 \& b + c = x_1 \& x_2 + x_2 \& (b + 1) + x_1 \& a + a + c = x_1 \& x_2 + x_1 \& a + a + c =$ /навесим отрицание над x_2/ $= x_1 \& \overline{x_2} + x_1 \& a + a + c = x_1 \& x_2 + x_1 \& (a + 1) + a + c = x_1 \& x_2 + a + c = x_1 \& x_2$.

Теорема доказана.