Теорема: Существует $2^{2^n}-1$ различных СДНФ от *n* переменных.

Доказательство: Поскольку каждая переменная входит в элементарную конъюнкцию в одном из двух состояний, то всего элементарных конъюнкций 2^n. СДНФ однозначно определяется подмножеством входящих в нее конъюнкций. Общее количество непустых подмножеств равно $2^{2^n}-1$.

Теорема: Существует $2^{2^n}-1$ различных СКНФ от *n* переменных.

Полином Жегалкина.

Логический полином по модулю 2, не содержащий одинаковых слагаемых, называется полиномом Жегалкина.

Алгоритм построения полинома Жегалкина.

Шаг 1. Построить ДНФ.

Шаг 2. С помощью формулы де Моргана $X \vee Y = \overline{(\overline{X} \wedge \overline{Y})}$ избавиться от дизъюнкций.

Шаг 3. Пользуясь формулой $\overline{X} = X \oplus 1$ избавиться от отрицаний.

Шаг 4. Пользуясь дистрибутивностью раскрыть скобки.

Шаг 5. Пользуясь формулой $X \oplus X = 0$ убрать повторяющиеся слагаемые.

Пример. $x \vee yz = \overline{(\overline{x} \wedge \overline{yz})} = (x \oplus 1)(yz \oplus 1) \oplus 1 = xyz \oplus yz \oplus x \oplus 1$.

Теорема: Существует 2^{2^n} различных полиномов Жегалкина от *n* переменных.

Доказательство. Каждое слагаемое полинома Жегалкина однозначно определяется входящими в него переменными, поэтому количество различных слагаемых равно количеству подмножеств *n*-элементного множества, т.е. 2^n. Так как каждое слагаемое входит в полином ровно один раз, то полином однозначно определяется набором слагаемых. Количество различных наборов равно 2^{2^n}.

Следствие. Логические высказывания эквивалентны тогда и только тогда когда совпадают их полиномы Жегалкина.

Доказательство. Каждой СДНФ ставится в соответствие некоторый полином Жегалкина, при этом различным СДНФ соответствуют различные полиномы. Но количество ненулевых полиномов равно количеству СДНФ. Поэтому соответствие взаимно-однозначное.

Булевы функции.

Булевой функцией называется функция $f:\{0,1\}^n \to \{0,1\}$.

Обозначения.

$\mathcal{P}_2$ — множество всех булевых функций;

$\mathcal{P}_2^n$ — множество всех булевых функций от n переменных;

$E^n=\{0,1\}^n$ — булев куб.

Любую булеву функцию можно задать таблицей $2^n \times (n+1)$, называемой *таблицей истинности.*

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	0
1	1	0	1
1	1	1	0

Теорема: Существует в точности 2^{2^n} различных булевых функций от *n* переменных.

Доказательство. Булева функция однозначно определяется значением последнего столбца таблицы истинности. Существует ровно 2^{2^n} различных значений булевого вектора длины 2^n.

Каждое высказывание от *n* переменных реализует булеву функцию. По определению эквивалентным высказываниям соответствуют одинаковые функции.

Справедливо обратное утверждение.

Любую булеву функцию не равную тождественно 0 можно реализовать высказыванием в виде СДНФ.

Доказательство. Достаточно каждому единичному значению функции сопоставить элементарную конъюнкцию, принимающую значение истина на соответствующем наборе значений переменных.

Пример. Функция, приведённая в таблице, реализуется высказыванием $\bar{x}yz \vee x y \bar{z}$.

Утверждение. Любую булеву функцию не равную тождественно 1 можно реализовать СКНФ.

Пример. Функция, приведённая в таблице, реализуется высказыванием $(\bar{x} \vee \bar{y} \vee \bar{z})(\bar{x} \vee \bar{y} \vee z)(\bar{x} \vee y \vee \bar{z})(x \vee \bar{y} \vee \bar{z})(x \vee \bar{y} \vee z)(x \vee y \vee z)$.

Булеву функцию можно задавать только 2^n-мерным вектором значений. При этом считается, что аргументы упорядочены в лексикографическом порядке.

Определение. Переменная x_i является *фиктивной* для функции $f(x_1, x_2, \ldots, x_n)$ если для любого набора значений переменных $(\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n)$ выполняется соотношение

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

Определение. Булевы функции называются равными, если они отличаются только своими фиктивными переменными.

Пример. Для функции $f(x, y, z) = xyz \vee x y \bar{z}$ переменная *z* — фиктивная, а переменные *x* и *y* — существенные.

Пример. Функции $f(x, y, z) = xyz \vee x y \bar{z}$ и $f(x, y) = xy$ равны.

Замкнутые классы булевых функций.

Определение. Пусть $\mathcal{F}$ класс функций из $\mathcal{P}_2$. Множество $[\mathcal{F}]$ всех функций, полученных суперпозициями функций из $\mathcal{F}$, называется *замыканием* класса $\mathcal{F}$.

Определение. Класс $\mathcal{F}$ называется замкнутым, если $\mathcal{F} = [\mathcal{F}]$.

Определение. Система функций $\{f_1, f_2, \ldots, f_n\}$ называется базисом класса $\mathcal{F}$, если любая функция из $\mathcal{F}$ может быть получена с помощью суперпозиции функций из базиса. Говорят, что система $\{f_1, f_2, \ldots, f_n\}$ полна в $\mathcal{F}$.

Теорема: Система функций $\{\bar{}, \wedge, \vee\}$ является базисом $\mathcal{P}_2$.

Доказательство. Любая ненулевая булева функция записывается в виде СДНФ и, следовательно, является суперпозицией отрицаний, конъюнкций и дизъюнкций. Осталось заметить, что $0 = x \wedge \bar{x}$, т.е. тоже является суперпозицией отрицания и конъюнкции.

Следствие 1. Системы функций $\{\bar{\ }, \wedge\}$ и $\{\bar{\ }, \vee\}$ являются базисами $\mathcal{P}_2$.

Для доказательства первого утверждения достаточно выразить все дизъюнкции через конъюнкции и отрицания с помощью формулы де Моргана $x \vee y = \overline{\bar{x} \wedge \bar{y}}$.

Следствие 2. Штрих Шеффера является базисом.

Доказательство. Достаточно выразить через штрих Шеффера функции известного базиса: $\bar{x} = x \mid x, \; x \wedge y = \overline{x \mid y}$.

Следствие 2. Стрелка Пирса является базисом.

Классы Поста.

Определение. Максимальный по включению замкнутый класс функций отличный от $\mathcal{P}_2$ называется *предполным*.

Определение. Булева функция f называется функцией, сохраняющей 0, если $f(0,0,\ldots,0)=0$. Обозначим класс функций, сохраняющих 0, —$\mathcal{F}_0$.

Утверждение. Класс функций, сохраняющих 0, замкнут.

Доказательство. Пусть функции $g(x_1,x_2,\ldots,x_n)$, $f_1,\ldots,f_n$ принадлежат $\mathcal{F}_0$. Тогда $g(f_1(0,\ldots,0),\ldots,f_n(0,\ldots,0))=g(0,\ldots,0)=0$. Т.е. суперпозиция тоже принадлежит $\mathcal{F}_0$.

Определение. Булева функция f называется функцией, сохраняющей 1, если $f(1,1,\ldots,1)=1$. Обозначим класс функций, сохраняющих 1, —$\mathcal{F}_1$.

Утверждение. Класс функций, сохраняющих 1, замкнут.

Определение. Булева функция f^* называется функцией, *двойственной* к функции f, если $f^*(x_1,\ldots,x_n)=\bar{f}(\bar{x}_1,\ldots,\bar{x}_n)$.

Пример. $(x\vee y)^*=\overline{(\bar{x}\vee\bar{y})}=xy$.

Теорема: Функция двойственная к суперпозиции функций равна суперпозиции двойственных функций. (Принцип двойственности)

Доказательство. Пусть функция Φ является суперпозицией функций $f_1,\ldots,f_m$ и функции g. Поскольку можно добавлять фиктивные переменные будем считать, что все функции f_i зависят от *n* переменных.

Рассмотрим двойственную функцию

$$\Phi^*(x_1,\ldots x_n)=\overline{\Phi}(\bar{x}_1,\ldots,\bar{x}_n)=\bar{g}(f_1(\bar{x}_1,\ldots,\bar{x}_n),\ldots,f_m(\bar{x}_1,\ldots,\bar{x}_n))=$$
$$\bar{g}(\bar{f}_1(\bar{x}_1,\ldots,\bar{x}_n),\ldots,\bar{f}_m(\bar{x}_1,\ldots,\bar{x}_n))=g^*(\bar{f}_1(\bar{x}_1,\ldots,\bar{x}_n),\ldots,\bar{f}_m(\bar{x}_1,\ldots,\bar{x}_n))=$$
$$g^*(f_1^*(x_1,\ldots x_n),\ldots,f_m{}^*(x_1,\ldots x_n)).$$

Утверждение. $f^{**}(x_1,\ldots,x_n)=\left(\bar{f}(\bar{x}_1,\ldots,\bar{x}_n)\right)^{*}=\bar{\bar{f}}(\bar{\bar{x}}_1,\ldots,\bar{\bar{x}}_n)=f(x_1,\ldots,x_n)$.

Пример. Найти функцию, двойственную к функции $f(x,y,z)=x\wedge(y\vee\bar{z})$.

Поскольку конъюнкция двойственна к дизъюнкции, а отрицание двойственно само к себе, то по принципу двойственности достаточно поменять конъюнкцию с дизъюнкцией. $f^{*}(x,y,z)=x\vee(y\wedge\bar{z})$.

Определение. Функция называется самодвойственной если $f^{*}=f$. Обозначим класс самодвойственных функций *S*.

Из принципа двойственности немедленно следует

Утверждение. Класс *S* замкнут.

Теорема: Классы $\mathcal{F}_0$ и $\mathcal{F}_1$ содержат ровно 2^{2^n-1} различных функций от *n* переменных.

Теорема: Класс S содержит ровно $2^{2^{n-1}}$ различных функций от *n* переменных.

Доказательство. Все булевы вектора размерности *n* можно разбить на пары противоположных векторов. Для определения самодвойственной функции достаточно определить значение только для одного представителя пары. Поэтому для определения самодвойственной функции нужно выбрать значение множества истинности только для половины булевых векторов. Т.е. мощность множества, на котором определяется функция, равна $2^n/2$. Количество его подмножеств равно $2^{2^{n-1}}$.

Определение. Пусть $a = (a_1,\ldots,a_n)$, $b = (b_1,\ldots,b_n) \in E^n$ — два двоичных вектора длины *n*. Будем говорить, что вектор *b* мажорирует вектор a и писать $a \prec b$, если для любого i $a_i \le b_i$.

Определение. Функция $f(x_1,\ldots,x_n)$ называется монотонной, если для любых векторов a и b из $a \prec b$ следует, что $f(a) \le f(b)$. Множество монотонных функций обозначим *M*.

Пример. $x \wedge y \in M$, $x \to y \notin M$.

Теорема: Класс *M* замкнут.

Доказательство. Пусть функция Φ является суперпозицией монотонных функций $f_1,\ldots,f_m$ и монотонной функции g. Поскольку добавление фиктивных переменных не влияет на монотонность, будем считать, что все функции f_i зависят от *n* переменных. Пусть $a=(a_1,\ldots,a_n),\ b=(b_1,\ldots,b_n)\in E^n$ — два двоичных вектора и $a\prec b$.

Тогда

$$(f_1(a_1,\ldots,a_n),\ldots,f_m(a_1,\ldots,a_n))\prec(f_1(b_1,\ldots,b_n),\ldots,f_m(b_1,\ldots,b_n)).$$

Отсюда

$$\Phi(a_1,\ldots,a_n)=g(f_1(a_1,\ldots,a_n),\ldots,f_m(a_1,\ldots,a_n))\le g(f_1(b_1,\ldots,b_n),\ldots,f_m(b_1,\ldots,b_n))=\Phi(b_1,\ldots,b_n)$$

Определение. Функция $f(x_1,\ldots,x_n)$ называется линейной, если ее многочлен Жегалкина линеен, т.е. не содержит конъюнкций. Множество линейных функций обозначим *L*.

Утверждение. Класс *L* замкнут.

Утверждение. Класс *L* содержат ровно 2^{n+1} различных функций от *n* переменных.

Теорема Поста.

Теорема: Для того, чтобы система функций была полной необходимо и достаточно, чтобы она не содержалась ни в одном и классов $\mathcal{F}_0$, $\mathcal{F}_1$, *S*, *M* и *L*.

Доказательство. Поскольку все перечисленные классы замкнуты и отличны от $\mathcal{P}_2$, то необходимость условия очевидна.

Достаточность. Выделим подсистему функций $B = \{f_0, f_1, f_S, f_M, f_L\}$, каждая из которых не содержится в соответствующем классе.

Идея доказательства. С помощью функций из *B* выразить базис $\{\bar{}, \wedge\}$.

Схема доказательства.

Шаг 1. Построить $\bar{x}$ или обе константы с помощью функций f_0, f_1.

Шаг 2. С помощью констант и f_M построить $\bar{x}$.

Шаг 3. С помощью $\bar{x}$ и f_S построить обе константы.

Шаг 4. С помощью констант, $\bar{x}$ и f_L построить конъюнкцию.

1. Положим $g(x)=f_0(x,\ldots,x)$. Тогда $g(0)=1$.

   Если $g(1)=0$ то $g(x)=\bar{x}$, иначе $g(x)=1$.

   Аналогично с помощью f_1 строим отрицание или 0.

2. Поскольку f_M не монотонна, то существуют наборы $a=(a_1,\ldots,a_n)$, $b=(b_1,\ldots,b_n)\in E^n$ такие, что $a\prec b$, $f_M(a)=1$ и $f_M(b)=0$.

   Функцию $g(x)$ получаем из функции f_M подстановкой переменной x в тех позициях, где $a_i<b_i$ и соответствующей константы в остальных позициях. Тогда $g(0)=f_M(a)=1$ и $g(1)=f_M(b)=0$.

3. Поскольку f_S не самодвойственная функция, то существует вектор $a=(a_1,\ldots,a_n)$, для которого $f_S(a_1,\ldots,a_n)=f_S(\bar{a}_1,\ldots,\bar{a}_n)$. Функцию $g(x)$ получаем из функции f_S подстановкой переменной x в тех позициях, где $a_i=1$ и функции $\bar{x}$ в тех позициях где $a_i=0$. Тогда $g(1)=f_S(a_1,\ldots,a_n)$ и $g(0)=f_S(\bar{a}_1,\ldots,\bar{a}_n)$. Т.е. это константа.

4. По определению нелинейной функции полином Жегалкина для функции f_L имеет хотя бы одно нелинейное слагаемое. Не ограничивая общности можно считать, что минимальный по степени нелинейный член имеет вид $x_1 x_2 \ldots x_m$, где $m>1$. Подставим в f_L вместо x_1 переменную x, вместо переменных $x_2,\ldots,x_m$ переменную y, а вместо остальных переменных константу 0.

После удаления нулевых слагаемых и преобразования повторяющихся переменных функция примет следующий вид:

$$g(x,y)=f_L(x,y,\ldots,y,0,\ldots,0)=xy\oplus ax\oplus by\oplus c,$$

где $a,\ b,\ c$ — булевы константы.

Тогда

$$g(x\oplus b,y\oplus a)\oplus ab\oplus c=(x\oplus b)(y\oplus a)\oplus a(x\oplus b)\oplus b(y\oplus a)\oplus c\oplus ab\oplus c=$$
$$xy\oplus by\oplus ax\oplus ab\oplus ax\oplus ab\oplus by\oplus ab\oplus ab=xy.$$

Прибавление константы реализуется с помощью формул:

$$x\oplus 0=x;\ \ x\oplus 1=\bar{x}.$$