3.1. Множества и операции над ними. Булевы функции, КНФ, ДНФ. Базисы, теорема Поста.

Множества — это объекты, которые рассматриваются в контексте двуместного отношения принадлежности. Запись «$a \in A$» является высказыванием (истинным или ложным) и означает «a принадлежит A». Свойства отношения $\in$ устанавливаются аксиоматикой теории множеств. На основе отношения $\in$ можно строить другие конструкции.
Пример 1. «$\forall x$: $x \in A \Rightarrow x \in B$» = «$A \subseteq B$» — «$A$ содержится в B».
При рассмотрении операций над множествами часто предполагают, что фиксирован некий универсум U, содержащий любое из множеств, с которыми имеют дело.
Функция f:$\{0;1\}^n \rightarrow \{0;1\}$ называется n-местной булевой. Класс всех таких функций обозначим через **B**. Элементы множества $\{0;1\}$ называют *пропозициональными переменными*.
Пусть $x_1, \ldots, x_n$ — пропозициональные переменные. Сопоставим каждой переменной x_i высказывание «$x \in X_i$». Тогда про каждую булеву функцию f над переменными $x_1, \ldots, x_n$ можно сказать, что она задаёт операцию над множествами $X_1, \ldots, X_n$. Результатом этой операции считается такое множество Y, что $x \in Y \leftrightarrow f(x \in X_1, \ldots, x \in X_n)$.
Пример 2. Конъюнкция $y = x_1 \wedge x_2$ задаёт операцию пересечения множеств $\cap$ высказыванием вида $x \in Y \leftrightarrow x \in X_1 \wedge x \in X_2$.
Пример 3. Функция вида $f(x_1, x_2) = x_1 \wedge \neg x_2$ задаёт операцию вычитания множеств \.
Тавтология соответствует универсуму U, а противоречие — пустому множеству.

Def 1. Литерал — это формула вида x или вида $\neg x$, где x — пропозициональная переменная.
Def 2. *Конъюнктивная нормальная форма* функции — это формула, задающая эту функцию в виде конъюнкции нескольких дизъюнкций литералов, причём операнды в дизъюнкциях и конъюнкции не повторяются. *Дизъюнктивная нормальная форма* функции — это формула, задающая эту функцию в виде дизъюнкции нескольких конъюнкций литералов, причём операнды в конъюнкциях и дизъюнкции не повторяются.
Def 3. Стандартная КНФ n-местной функции — это такая её КНФ, в которой каждая дизъюнкция содержит n литералов. Стандартная ДНФ n-местной функции — это такая её ДНФ, в которой каждая конъюнкция содержит n литералов.

Каждая булева функция единственным образом (с точностью до порядка операндов) представляется в виде СКНФ и в виде СДНФ. Построение выполняется по таблице истинности. Для СДНФ конъюнкции соответствуют выполняющим наборам, и в каждой конъюнкции отрицания стоят у тех переменных, которые являются ложными в наборе, которому эта конъюнкция сопоставлена. Для СКНФ наоборот: дизъюнкции соответствуют невыполняющим наборам, и в каждой из них отрицания стоят у тех переменных, которые являются истинными в наборе. ДНФ и КНФ являются двойственными друг другу относительно операции отрицания.

Def 4. Пусть $P \subseteq \mathbf{B}$ — некоторый класс булевых функций. Класс Q, состоящий из всех суперпозиций функций класса P, называют *замыканием* P и обозначают так: $Q = [P]$. При этом говорят, что P *порождает* Q. Класс называется (функционально) замкнутым или *классом Поста*, если он совпадает со своим замыканием. Класс P называют полным в Q, если любую функцию из Q можно выразить через суперпозиции функций из P.
Пример 4. $[\vee, \wedge, \neg] = \mathbf{B}$.
Def 5. Класс булевых функций P называется *независимым*, если ни одна функция f из класса P не содержится в $[P \setminus \{f\}]$, т. е. не выражается через суперпозиции всех остальных. Полный независимый класс называется *базисом*.
Пример 5. Все эти классы: $\{\vee, \neg\}$, $\{\wedge, \neg\}$, $\{\rightarrow, \neg\}$, $\{\rightarrow, 0\}$, $\{\,|\,\}$, $\{\uparrow\}$, $\{\vee, +, 1\}$, $\{\wedge, +, 1\}$ — являются базисами для класса **B**.
Комментарий. «$|$» — штрих Шеффера ($a \mid b = \neg(a \wedge b)$), «$\uparrow$» — стрелка Пирса ($a \uparrow b = \neg(a \vee b)$).
«+» — это xor, «→» — импликация. Малая теорема Поста рассмотрит пять важнейших замкнутых классов. В ней высказывание «класс полон» будет подразумевать, что он полон в **B**.

3.1

<u>Большая теорема Поста.</u> Каждый замкнутый класс имеет конечный базис.
Доказательство теоремы состоит в том, чтобы перечислить *все* существующие замкнутые классы (их около 50, включая несколько бесконечных регулярных семейств), предъявить конечный базис для каждого из них и доказать, что никаких других замкнутых классов не существует.

<u>Def 6.</u> Замкнутый класс P называется *предполным* (*максимальным*), если $P \neq \mathbf{B}$ и P не содержится ни в каком другом замкнутом классе, отличном от **B**.
$\mathbf{B_0}$ — класс функций, удовлетворяющих условию $f(0, 0, \ldots, 0) = 0$ (*сохраняющих нуль*).
$\mathbf{B_1}$ — класс функций, удовлетворяющих условию $f(1, 1, \ldots, 1) = 1$ (*сохраняющих единицу*).
L — класс всех *линейных* функций, т. е. функций вида $a_1 x_1 + \ldots + a_n x_n + a_0$, где $a_k \in \{0;1\}$ $(0 \le k \le n)$.
S — класс всех *самодвойственных* функций, т. е. таких, что $f(\neg x_1, \ldots, \neg x_n) = \neg f(x_1, \ldots, x_n)$.
M — класс всех *монотонных* функций: $x_1 \le y_1, \ldots, x_n \le y_n \Rightarrow f(x_1, \ldots, x_n) \le f(y_1, \ldots, y_n)$.
Классы $\mathbf{B_0}$, $\mathbf{B_1}$, **L**, **S**, **M** являются замкнутыми. Это проверяется непосредственно из определений.

<u>Малая теорема Поста.</u> Классы $\mathbf{B_0}$, $\mathbf{B_1}$, **L**, **S**, **M** являются предполными, и никаких других предполных классов не существует. Набор булевых функций является полным тогда и только тогда, когда он не содержится целиком ни в одном из этих пяти предполных классов.
<u>Доказательство.</u> Пусть $f(x_1, \ldots, x_n) \notin \mathbf{B_1}$. Тогда $f(1, \ldots, 1) = 0$ и $\to \in \mathbf{B_1}$, а $[0, \to] = \mathbf{B}$ (см. пример 5), т. е. $\mathbf{B_1}$ — предполный класс. Далее, пусть $f(x_1, \ldots, x_n) \notin \mathbf{B_0}$. Тогда $f(0, \ldots, 0) = 1$ и $+, \vee \in \mathbf{B_0}$, а $[1, +, \vee] = \mathbf{B}$ (см. там же), т. е. $\mathbf{B_0}$ — предполный. Предполнота классов **L**, **S**, **M** будет показана ниже.
Рассмотрим вторую часть теоремы. Если набор содержится в одном из этих пяти классов, то он не является полным, т. к. все они отличаются от **B**. Докажем обратное утверждение. Пусть наш набор для каждого класса содержит функцию, в нём не лежащую. Убедимся, что с помощью комбинаций выбранных функций можно получить все булевы функции.
У нас есть функция, не сохраняющая нуль. Подставим вместо всех аргументов одну и ту же переменную. Получится функция одного аргумента, отображающая нуль в единицу, то есть либо константа 1, либо отрицание. Сделав то же самое с функцией, не сохраняющей единицу, получим либо константу нуль, либо отрицание. Таким образом, у нас либо есть отрицание, либо обе константы 0 и 1.
Если есть обе константы, то всё равно можно получить отрицание. Возьмём немонотонную функцию. Легко понять, что она должна менять значение с единицы на нуль при изменении какого-то одного аргумента с нуля на единицу (в самом деле, будем увеличивать аргументы по одному, в какой-то момент значение функции уменьшится). Зафиксировав значения остальных аргументов (ведь мы считаем, что константы есть), получаем отрицание. Попутно заметим: мы смогли получить отрицание из произвольной немонотонной функции и констант $0, 1 \in \mathbf{M}$. Заметим также, что $\vee, \wedge \in \mathbf{M}$. Это означает (см. пример 4), что **M** — предполный класс.
Имея отрицание и несамодвойственную функцию, легко получить константы (если их не было). В самом деле, несамодвойственность означает, что $f(\neg x_1, \ldots, \neg x_n) = f(x_1, \ldots, x_n)$ для каких-то значений $x_1, \ldots, x_n \in \{0;1\}$. Вместо нулевых значений переменных $x_1, \ldots, x_n$ подставим p, вместо единиц подставим $\neg p$, легко видеть, что получается одна из констант. Вторая получается отрицанием. Т. е. константы можно получить из произвольной несамодвойственной функции и функции $\neg \in \mathbf{S}$. Попутно заметим: функция $h(x, y, z) = xy + xz + yz$ также принадлежит **S**. Тогда $h(x, y, 1) = x \vee y$. Ввиду того, что $[\neg, \vee] = \mathbf{B}$ (пример 5), класс **S** является предполным.
Теперь у нас есть константы, отрицание и нелинейная функция $f(x_1, \ldots, x_n)$. Нелинейность означает, что в её представлении в виде многочлена (полинома Жегалкина, см. пример 5 в конце) есть моном, состоящий более чем из одной переменной. Пусть, например, этот моном содержит переменные x_1 и x_2. Сгруппируем члены по четырём группам и получим выражение: $x_1 x_2 A(x_3, \ldots, x_n) + x_1 B(x_3, \ldots, x_n) + x_2 C(x_3, \ldots, x_n) + D(x_3, \ldots, x_n)$. Здесь $A(x_3, \ldots, x_n)$ не является константой 0. Фиксируем $x_3, \ldots, x_n$ так, чтобы $A(x_3, \ldots, x_n) = 1$. Тогда $g(x_1, x_2) = f(x_1, x_2, x_3, \ldots, x_n) = x_1 x_2 + a x_1 + b x_2 + c$ для некоторых a, b, c. Тогда $g(x_1 + b, x_2 + a) + ab + c = x_1 \wedge x_2$. Итак, $[\neg, \wedge] = \mathbf{B}$, и вторая часть теоремы доказана. Попутно заметим: мы получили $\wedge$ по $\neg \in \mathbf{L}$ и произвольной нелинейной функции, т. е. класс **L** предполон.
Если некоторый класс, отличный от $\mathbf{B_0}$, $\mathbf{B_1}$, **L**, **S**, **M**, содержится в одном из этих классов, то он не предполон (по определению), а если не содержится ни в одном из них, то он полон (по только что доказанному), следовательно, опять же, не предполон. Значит, других предполных классов (кроме $\mathbf{B_0}$, $\mathbf{B_1}$, **L**, **S**, **M**) нет, ч.т.д.

<u>Следствие.</u> Всякий базис для **B** содержит не более четырёх функций.
<u>Доказательство.</u> Из любого полного набора для **B** можно оставить не более пяти функций: $f_1 \notin \mathbf{B_0}$, $f_2 \notin \mathbf{B_1}$, $f_3 \notin \mathbf{L}$, $f_4 \notin \mathbf{S}$, $f_5 \notin \mathbf{M}$. Если $f_1(x, \ldots, x) = 1$, то $f_1 \notin \mathbf{S}$, и можно выбросить f_1 или f_4. Если $f_2(x, \ldots, x) = 0$, то $f_2 \notin \mathbf{S}$, и можно выбросить f_2 или f_4. Если $f_1(x, \ldots, x) = f_2(x, \ldots, x) = \neg x$, то можно выбросить f_1 или f_2.