ЛЕКЦИЯ 3

МНОГОЧЛЕН ЖЕГАЛКИНА. КЛАССЫ БУЛЕВЫХ ФУНКЦИЙ

1. Многочлен Жегалкина (продолжение)

Теорема 4 Любую булеву функцию можно представить в виде многочлена Жегалкина. *

Док-во: Известно, что всего булевых функций — 2^{2^n}. Общее количество одночленов — 2^n, так как одночлен — это произведение двух различных переменных, а значит, что любая переменная либо входит в него, либо не входит.

Общее количество многочленов — 2^{2^n}, так как многочлен — это сумма различных одночленов. Более того, один многочлен задает только одну функцию.

Значит, достаточно доказать одно из двух:

1. Что по каждой функции можно построить многочлен.
2. Что различные многочлены задают различные функции.

Для понимания того, почему доказательство любого из этих двух пунктов достаточно для доказательства теоремы, можно использовать рисунок 3.1. Говорится, что из каждой точки из правого множества идет ровно одна стрелка в левое.

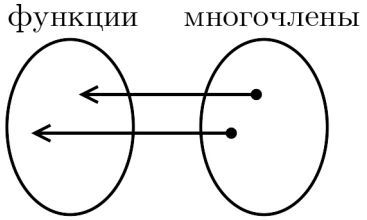

Рис. 3.1

Первый пункт утверждает, что в каждую точку из левого множества входит только

одна стрелка. Так как количество точек в левом и правом множествах — одинаковое, то это будет означать, что доказано и существование, и единственность.

Второй пункт говорит о том, что поскольку не может происходить «склейки» стрелок в одной точке, то на все функции хватит многочленов.

Для лучшего понимания темы докажем оба пункта.

1. Для доказательства первого пункта заметим, что на предыдущей лекции было показано, что:
$$\neg p = p + 1; \quad p \vee q = p + q + pq.$$

2. Пусть P и Q — разные многочлены, причем:
$$\forall x \ P(x) = Q(x).$$

   Рассмотрим их сумму S ($S = P + Q$). Получился ненулевой многочлен, однако он равен нулю в каждой точке:
$$\forall x \ S(x) = 0.$$

   Тогда в данном многочлене есть какие-то ненулевые слагаемые. Рассмотрим среди этих одночленов тот, который зависит от наименьшего числа переменных. Если таких одночленов несколько, то выберем любой из них.

   Без ограничения общности, будем рассматривать слагаемое $x_1 x_2 \dots x_k$. Тогда:
$$S\Big(\underbrace{1, 1, \dots, 1}_{k}, \underbrace{0, 0, \dots, 0}_{n-k}\Big).$$

   Это значение равняется единице, так как $x_1 x_2 \dots x_k = 1$, а остальные слагаемые равны нулю. Значит, получилось противоречие вышесказанному, и тогда этот пункт тоже можно считать разобранным.

Теорема 4 доказана. ■

2. Булевы функции (продолжение). Классы булевых функций

На основе предыдущей лекции можно сделать следующее наблюдение: не любую функцию можно выразить через конъюнкцию, дизъюнкцию и импликацию. Поясним это на примере единицы:
$$1 \wedge 1 = 1; \quad 1 \vee 1 = 1; \quad 1 \to 1 = 1.$$

Значит, если в формуле присутствуют только эти знаки (и в нее подставлены все единицы), то в итоге также будет единица.

Но не все функции имеют такой вид, например, если подставить единицу в отрицание, то получится ноль. Также если подставить единицу в XOR, то тоже будет ноль. Следовательно, таким образом можно выразить только те функции, которые сохраняют единицу.

Оказывается, что аналогичных «препятствий к полноте» не так много (помимо очевидных случаев с сохранением единицы и нуля). Значит, если такие «препятствия» отсутствуют, то можно выразить все формулы.

Определение 25: *Пусть $f_1, \dots, f_k$ — это булевы функции.* ***Композиция*** *булевых функций определяется следующим образом: нулевым порядком являются проекторы, то есть:*

$$\mathrm{pr}_i(a_1, \dots, a_m) = a_i.$$

Тогда $(s+1)$-й порядок — это все функции s-го порядка и все функции вида:

$$f_i\Big(g_1(p_1, \dots, p_m), \dots, g_m(p_1, \dots, p_m)\Big),$$

где $g_1, \dots, g_m$ — это композиции s-го порядка, а f_i — это функция от m переменных.♣

Возникает вопрос: для каких базовых систем через $f_1, \dots, f_k$ можно выразить все функции?

Определение 26: *C — это* ***замкнутый класс*** *булевых функций, если C содержит все проекторы, а композиция не выводит за пределы данного класса.* ♣

Определение 27: ***Решеткой Поста*** *называется полная классификация замкнутых классов.* ♣

Пример 9 Простые примеры замкнутых классов:

1. Класс P_1, сохраняющий единицу, то есть:

$$f(1, 1, \dots, 1) = 1.$$

2. Класс P_0, сохраняющий ноль, то есть:

$$f(0, 0, \dots, 0) = 0.$$

В обоих примерах замкнутость очевидна. *

Определение 28: *Класс D — это класс* ***самодвойственных функций****, то есть:*

$$f(\neg p_1, \dots, \neg p_n) = \neg f(p_1, \dots, p_n) \quad \Longleftrightarrow \quad f = f^*,$$

где f^* — это двойственная функция:

$$f^*(p_1, \dots, p_n) = \neg f(\neg p_1, \dots, \neg p_n).$$

Заметим, что двойственная конъюнкция — это дизъюнкция:

$$\neg(\neg p \wedge \neg q) = p \vee q.$$

Это верно и наоборот. Также можно отметить, что функция, двойственная к двойственной, есть исходная функция.

Проекторы являются самодвойственными функциями, так как:

$$f_i\Big(g_1(\neg p_1,\dots,\neg p_n),\dots,g_m(\neg p_1,\dots,\neg p_n)\Big) = \\ = f_i\Big(\neg g_1(p_1,\dots,p_n),\dots,\neg g_m(p_1,\dots,p_n)\Big) = \\ = \neg f_i\Big(g_1(p_1,\dots,p_n),\dots,g_m(p_1,\dots,p_n)\Big).$$

Значит, вся композиция — самодвойственна. Очевидно также, что и функция отрицания является самодвойственной.

Рассмотрим *функцию большинства*:

$$\mathrm{maj}(p_1,\dots,p_{2m+1}),$$

означающую, что если в аргументах содержится большинство единиц, то она равна единице, а если большинство нулей — то нулю. Нетрудно видеть, что для любого нечетного числа данная функция — самодвойственна.

Определение 29: *Класс M — это класс* ***монотонных функций****. Функция f — монотонна, если из того, что:*

$$p_1 \leqslant q_1, \quad \dots, \quad p_n \leqslant q_n$$

следует, что:

$$f(p_1,\dots,p_n) \leqslant f(q_1,\dots,q_n).$$

Класс монотонных функций является замкнутым классом. Поясним это:

$$f\Big(g_1(p_1,\dots,p_m),\dots,g_m(p_1,\dots,p_m)\Big).$$

Здесь p не уменьшаются с возрастанием индекса. Тогда, поскольку все внутренние функции монотонны, то соответствующие значения $g_1,\dots,g_m$ — тоже либо не меняются, либо изменяются всегда на единицу. Тогда и итоговое значение либо не меняется, либо изменяется всегда на единицу.

В итоге получим, что значение всей функции либо не изменилось, либо увеличилось. Значит, класс M — действительно замкнутый.

Утверждение 1 Если f не монотонна, то сущестует i, а также существуют значения $a_1,\dots,a_{i-1},a_{i+1},\dots,a_n$ такие, что:

$$f(a_1,\dots,a_{i-1},0,a_{i+1},\dots,a_n) = 1; \quad f(a_1,\dots,a_{i-1},1,a_{i+1},\dots,a_n) = 0.$$

Док-во: Идея доказательства данного утверждения — использование *гибридного аргумента.* ■

Определение 30: *Класс L — это класс* ***линейных функций*** *(иначе — класс аффинных функций, обозначается A).*

Линейные функции — это функции, у которых линейный многочлен Жегалкина (то есть все слагаемые в этом многочлене —- первой степени и, может быть, еще единица). Иначе говоря — это сумма каких-то переменных и, может быть, единица.♣

Таким образом, существует пять классов функций — сохраняющие единицу, сохраняющие ноль, самодвойственные, монотонные и линейные. Если все рассматриваемые функции попали в один из этих классов, то о полноте системы не может быть и речи, так как все, что можно выразить, окажется внутри соответствующего класса.

3. Критерий Поста

Теорема 5 (Критерий Поста) $\{f_1, \dots, f_n\}$ является полной системой булевых функций тогда и только тогда, когда срели функций $f_1, \dots, f_n$ есть функции, не сохраняющие единицу, не сохраняющие ноль, не самодвойственные, не монотонные и не линейные (причем это может быть всего одна функция, обладающая всеми перечисленными свойствами). *

Док-во: Первая часть ($\Rightarrow$): доказательство теоремы в эту сторону будет следовать из замкнутости.

Вторая часть ($\Leftarrow$): пусть еслть пять функций, таких что f_0 не сохраняет ноль, f_1 не сохраняет единицу, g не является самодвойственной, h не является монотонной и k не является линейной, причем некоторые из этих функций могут совпадать.

Заметим, что штрих Шеффера (отрицание конъюнкции) обладает всеми пятью свойствами. Тогда:

$$p|q = \neg p; \quad (p|q)\big|(p|q) = p \wedge q.$$

Выразив отрицание и конъюнкцию, можно выразить дизъюнкцию. Далее через КНФ и ДНФ можно выразить любую формулу.

Теперь приведем общий метод. Сначала рассмотрим f_0. Утверждается, что:

$$f_0(0,0,\dots,0) = 1; \quad f_0(1,1,\dots,1) = \begin{bmatrix} 0, & \text{тогда } f_0(p,p,\dots,p) = \neg p, \\ 1, & \text{тогда } f_0(p,p,\dots,p) = 1. \end{bmatrix}$$

Таким образом, получено отрицание и константа 1. Теперь запишем то же самое для f_1:

$$f_1(1,1,\dots,1) = 0; \quad f_1(0,0,\dots,0) = \begin{bmatrix} 0, & \text{тогда } f_1(p,p,\dots,p) = 0, \\ 1, & \text{тогда } f_1(p,p,\dots,p) = \neg p. \end{bmatrix}$$

План таков: необходимо получить две константы и отрицание, затем, используя нелинейную функцию, получить все остальные формулы.

Кроме очевидного случая, когда уже получены отрицание и константа, есть два нетривиальных случая.

Первый случай: были получены ноль, единица и немонотонная функция h. Заметим, что для немонотонной функции верно следующее:

$$h(a_1, \dots, a_{i-1}, 0, a_{i+1}, \dots, a_n) = 1; \quad h(a_1, \dots, a_{i-1}, 1, a_{i+1}, \dots, a_n) = 0.$$

Тогда было получено отрицание:

$$\neg p = h(a_1, \dots, a_{i-1}, p, a_{i+1}, \dots, a_n),$$

где a_i — это константы.

Второй случай: были получены отрицание и несамодвойственная функция g. Раз функция — несамодвойственна, то значит, для каких-то значений условия двойственности самой себе не выполнены, то есть:

$$g(a_1, a_2, \dots, a_n) = g(\neg a_1, \neg a_2, \dots, \neg a_n).$$

Тогда можно рассмотреть следующую конструкцию:

$$g(p^{a_1}, p^{a_2}, \dots, p^{a_n}) = \text{const},$$

где имеется в виду, что:

$$p^1 = p, \quad p^0 = \neg p.$$

Заметим далее, что p^a и a^p — это одно и то же, но синтаксически верно писать именно p^a.

Остался последний шаг доказательства — как именно из нуля, единицы, отрицания и нелинейной функции получить все остальное.

Так как k — нелинейна, то у нее нелинейный многочлен Жегалкина. Значит, он содержитнелинейное слагаемое. Без ограничения общности, будем считать, что:

$$k(\overline{x}) = x_1 x_2 A(x_3, \dots, x_n) + x_1 B(x_3, \dots, x_n) + x_2 C(x_3, \dots, x_n) + D(x_3, \dots, x_n),$$

причем $A \neq 0$.

Далее используем лемму о многочлене Жегалкина — что если многочлен не равен нулю, то он не равен нулю на каком-то множестве. Значит, фиксацией $x_3, \dots, x_n$ можно получить:

$$x_1 x_2 + b x_1 + c x_2 + d.$$

Если $d = 1$, то возьмем отрицание. Получим тогда:

$$x_1 x_2 + b x_1 + c x_2.$$

Если $b = c = 0$, то получена конъюнкция. Из конъюнкции и отрицания уже можно выразить все функции.

Если $b = c = 1$, то получена дизъюнкция, что аналогично предыдущему случаю.

Если $b = 1$, а $c = 0$, то получено отрицание импликации:

$$x_1 \wedge \neg x_2 \;\Rightarrow\; x_1 \not\to x_2.$$

Тогда:

$$x_1 \not\to \neg x_2 \quad \Longleftrightarrow \quad x_1 \wedge x_2,$$

откуда снова можно получить все функции.

Таким образом, все случаи разобраны, и теорема 5 доказана. ■