2-я лекция курса "Теория дискретных функций"

(1-й курс; лектор - проф. А.С.Подколзин)

Формулы алгебры логики определялись таким образом, что символ функции всегда располагался в начале формулы. Такая запись называется префиксной. Однако, на практике символ операции часто встречается между операндами, а не перед ними. Это называется инфиксной записью. В особенности она удобна, если операция ассоциативная и соединяет более двух операндов. Мы будем разрешать использование инфиксной записи, рассматривая ее как условное обозначение для "настоящей формулы", где запись префиксная. В частности, запись $a_1\varphi a_2 \dots \varphi a_n$ где операция φ ассоциативна и коммутативна, будет пониматься как условное обозначение для формулы $\varphi(a_1, \varphi(a_2, \dots, \varphi(a_{n-1}, a_n)))$.

Как и обычно, будем пользоваться некоторыми правилами опускания скобок. Например, в алгебре запись $ab + c$ понималась как $(ab) + c$ - умножение "притягивает" операнды сильнее, чем сложение. В алгебре логики вводится следующее упорядочение по убыванию такой силы: $\&, \vee, \to, +, \leftrightarrow$. Если отрицание записывается как $\neg a$, то оно считается сильнее всех прочих операций. Например, в записи $\neg a \& b \vee c \to d$ скобки восстанавливаются так: $(((\neg a)\&b) \vee c) \to d$.

Формулы Φ_1 и Φ_2 в сигнатуре Σ назовем эквивалентными, если они определяют равные функции относительно объединения своих переменных. Слово $\Phi_1 = \Phi_2$, где Φ_1, Φ_2 - эквивалентные формулы, будем называть тождеством. Используя тождества, можно выполнять эквивалентные преобразования формул алгебры логики, например, для их упрощения. Обоснованием такой возможности служит уже упоминавшаяся лемма о замене из математической логики. В данном курсе мы принимаем это без доказательства.

Приведем список основных тождеств для элементарных функций алгебры логики.

1. Ассоциативность и коммутативность для операций $\vee$, $\&$, $+$, $\leftrightarrow$.

2. Дистрибутивности:

   $(a \vee b)\&c = a\&c \vee b\&c$

   $(a\&b) \vee c = (a \vee c)\&(b \vee c)$

   $(a + b) \cdot c = a \cdot c + b \cdot c$

   В последнем тождестве вместо символа $\&$ использован символ $\cdot$, обозначающий ту же самую функцию.

3. Тождества для отрицания:

   $\bar{\bar{a}} = a$

   $\overline{a \vee b} = \bar{a}\&\bar{b}$

   $\overline{a\&b} = \bar{a} \vee \bar{b}$

   (эти два тождества называются законами Моргана)

   $a \cdot \bar{a} = 0$

   $a \vee \bar{a} = 1$

   $\overline{a \to b} = a\&\bar{b}$

4. Тождества для идентичных операндов:

   $a\&a = a$

   $a \vee a = a$

   $a \to a = 1$

   $a \leftrightarrow a = 1$

   $a + a = 0$

5. Тождества с константным операндом:

   $a \vee 0 = a$

   $a\&0 = 0$

   $a \to 0 = \bar{a}$

   $a + 1 = \bar{a}$

   $0 \to a = 1$

   и т.д. - список таких тождеств легко продолжить самостоятельно.

Как и в алгебре, вводятся "конечные операции":

$$a_1\& \ldots \&a_n = \bigwedge_{i=1}^{n} a_i$$

$$a_1 \vee \ldots \vee a_n = \bigvee_{i=1}^{n} a_i$$

Заметим, что в первой из формул обычно используется не знак $\bigwedge$ (появившийся здесь лишь из-за трудностей набора в LaTex), а большой знак конъюнкции &.

Функция $g(x_1 \ldots x_n) = \bar{f}(\bar{x_1} \ldots \bar{x_n})$ называется двойственной к функции $f(x_1, \ldots x_n)$. Используется обозначение $g = f^*$. Очевидно, что $(f^*)^* = f$. Таблица для функции g получается из таблицы функции f одновременной заменой всех нулей на единицы, а единиц на нули. Замена предпринимается как в левой части таблицы, где перечисляются наборы значений аргументов, так и в правой, где указываются значения функции. Примеры:

$(a\&b)^* = a \vee b$

$(a \vee b)^* = a\&b$

$(a + b)^* = a \leftrightarrow b$

Если $f = f^*$, то функция называется самодвойственной. Примеры:

$\bar{a}^* = \bar{a}$

$(a + b + c)^* = a + b + c$

Имеет место следующий принцип двойственности. Пусть $\Sigma : S \to F$ - сигнатура. Определим двойственную сигнатуру $\Sigma^* : S \to F^*$ равенством $\Sigma^*(s) = (\Sigma(s))^*$. Иными словами, в двойственной сигнатуре символ обозначает функцию, двойственную той, которую он обозначал в исходной сигнатуре. Принцип двойственности утверждает,

что если формула Φ определяет над Σ некоторую функцию g, то она же определяет над Σ^* двойственную функцию g^*. Списки переменных в обоих случаях совпадают.

Данный принцип можно доказать индукцией по определению формулы. С другой стороны, он и без этого очевиден. Действительно, таблицы "элементарных" функций, обозначенных символами из S, отличаются в двойственной сигнатуре от их таблиц в исходной сигнатуре лишь тем, что нули и единицы меняются местами. То, что раньше было нулем, теперь обозначается как единица, и наоборот. Однако, последовательность вычислений для построения таблицы функции g по исходным таблицам "элементарных" функций в обоих случаях одна и та же. Поэтому и результат вычислений для двойственной сигнатуры будет отличаться от результата для исходной сигнатуры лишь переобозначением нулей и единиц. Этот принцип мы далее почти не используем, и более подробного его доказательства не рассматриваем.

Введем обозначение x^σ, где $\sigma \in E_2$. Если $\sigma = 1$, то оно обозначает переменную x; если $\sigma = 0$ то - отрицание переменной $\bar{x}$. Очевидно, что $x^\sigma = 1$ тогда и только тогда, когда $x = \sigma$. Заметим, что x^σ - это не функция от переменных x, σ, а лишь способ задать, в зависимости от ситуации, переменную либо ее отрицание.

Теорема. Для любой функции алгебры логики $f(x_1, \ldots, x_n)$ при любом $m \in \{1, \ldots, n\}$ имеет место тождество:

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_m) \in B_m} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n).$$

Рассмотрим произвольный двоичный набор $(\alpha_1, \ldots, \alpha_n)$. Если $(\sigma_1, \ldots, \sigma_m) \neq (\alpha_1, \ldots, \alpha_m)$, то для некоторого $i \in \{1, \ldots, m\}$ имеем $\sigma_i \neq \alpha_i$. Тогда $\alpha_i^{\sigma_i} = 0$, и все произведение $\alpha_1^{\sigma_1} \cdot \ldots \cdot \alpha_m^{\sigma_m} f(\sigma_1, \ldots, \sigma_m, \alpha_{m+1}, \ldots, \alpha_n)$ обращается в 0. Единственным членом дизъюнкции, влияющим на ее значение, оказывается член для $(\sigma_1, \ldots, \sigma_m) = (\alpha_1, \ldots, \alpha_m)$. Он равен $\alpha_1^{\alpha_1} \cdot \ldots \cdot \alpha_m^{\alpha_m} f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n)$, т.е. равен левой части равенства. Теорема доказана.

Рассмотрим два важных частных случая доказанной теоремы. При $m = 1$, изменив нумерацию переменных, получим тождество:

$f(x_1, \ldots, x_n) = x_n \cdot f(x_1, \ldots, x_{n-1}, 1) \ \vee \ \bar{x_n} \cdot f(x_1, \ldots, x_{n-1}, 0)$

Это - так называемое разложение функции f по переменной x_n. Оно обычно используется при доказательствах по индукции, так как обеспечивает переход от функции n переменных к функциям $n - 1$ переменной.

При $m = n$ получаем следующее тождество:

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n) : f(\sigma_1, \ldots, \sigma_n) = 1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$$

Выражение в правой части называется совершенной дизъюнктивной нормальной формой (сокращенно - совершенной д.н.ф.). Здесь сразу отброшены точки, в которых функция f обращается в 0. Заметим, что если функция тождественно нулевая, то запись в правой части равенства не имеет смысла, т.е. совершенная д.н.ф. существует только для функций, не являющихся тождественно нулевыми. Иногда по определению считают 0 тоже дизъюнктивной нормальной формой.

Рассматриваются также другие виды дизъюнктивных нормальных форм (д.н.ф.). Все они представляют собой дизъюнкции "одночленов" - произведений переменных

и их отрицаний. В каком-то смысле д.н.ф. - аналоги многочленов, у которых роль сложения играет дизъюнкция, а роль умножения - конъюнкция. Упрощение формул алгебры логики часто происходит путем преобразования их к виду д.н.ф. и последующего упрощения как дизъюнктивных нормальных форм. Для такого упрощения имеется достаточно развитый аппарат. После того, как д.н.ф. упрощена, предпринимается дальнейшее упрощение вне рамок д.н.ф. - путем группировок и вынесений за скобки. Данный процесс используется при проектировании чипов. Он реализован в виде программ для компьютера.

Теорема. Каждая функция алгебры логики может быть получена суперпозициями из отрицания, конъюнкции и дизюнкции.

Если функция не тождественно нулевая, то она реализуется совершенной дизъюнктивной нормальной формой. Такую д.н.ф. можно рассматривать как формулу алгебры логики, построенную при помощи отрицаний, конъюнкций и дизъюнкций. Если функция тождественно нулевая, то ее можно определить формулой $x_1 \cdot \bar{x_1}$, рассматриваемой относительно списка фиктивных переменных требуемой длины. Теорема доказана.

Для произвольной функции алгебры логики $f(x_1, \ldots, x_n)$ рассмотрим двойственную функцию $f^*(x_1, \ldots, x_n)$ и зададим ее посредством совершенной д.н.ф.:

$$f^*(x_1, \ldots, x_n) = \bigvee_{(\sigma_1,\ldots,\sigma_n):f^*(\sigma_1,\ldots,\sigma_n)=1} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$$

Здесь предполагается, что функция $f^*(x_1, \ldots, x_n)$ не тождественно нулевая, т.е. функция $f(x_1, \ldots, x_n)$ не тождественно единичная.

Согласно принципу двойственности, указанное равенство сохранится, если перейти к двойственной сигнатуре в правой его части и к двойственной функции в левой. В данном случае переход к двойственной сигнатуре означает, что конъюнкция и дизъюнкция "поменяются местами". Так как $(f^*)^* = f$, получим:

$$f(x_1, \ldots, x_n) = \bigwedge_{(\sigma_1,\ldots,\sigma_n):f^*(\sigma_1,\ldots,\sigma_n)=1} (x_1^{\sigma_1} \vee \ldots \vee x_n^{\sigma_n}).$$

Равенство $f^*(\sigma_1, \ldots, \sigma_n) = 1$ означает, что $\bar{f}(\bar{\sigma_1}, \ldots, \bar{\sigma_n}) = 1$, т.е. $f(\bar{\sigma_1}, \ldots, \bar{\sigma_n}) = 0$.

Сделаем замену переменных $\delta_i = \bar{\sigma_i}$; $i = 1, \ldots, n$. Тогда равенство для $f(x_1, \ldots, x_n)$ можно переписать в следующем виде:

$$f(x_1, \ldots, x_n) = \bigwedge_{(\delta_1,\ldots,\delta_n):f(\delta_1,\ldots,\delta_n)=0} (x_1^{\bar{\delta_1}} \vee \ldots \vee x_n^{\bar{\delta_n}}).$$

Выражение в правой части называется совершенной конъюнктивной нормальной формой для функции f. Это - еще один аналог многочленов в алгебре логики.

Назовем множество M функций алгебры логики полным, если любая функция алгебры логики может быть получена из него суперпозициями. Очевидно, что все множество P_2 полно. Кроме того, согласно доказанной выше теореме, полным является также множество $\{\bar{x}, x\&y, x \vee y\}$.

Утверждение. Если множество M_1 полно, а каждая функция этого множества выражается суперпозициями через функции множества M_2, то множество M_2 тоже полно.

Утверждение очевидно: чтобы выразить суперпозициями какую-либо функцию через функции множества M_2, достаточно сначала выразить через функции этого множества все функции множества M_1, а затем использовать полноту M_1.

С помощью данного утверждения приведем еще ряд примеров полных систем.

1. Множество $\{\bar{x}, x\&y\}$ полно. Достаточно заметить, что оно сводится к множеству $\{\bar{x}, x\&y, x \vee y\}$ при помощи равенства $x \vee y = \overline{\bar{x}\&\bar{y}}$.
2. Множество $\{\bar{x}, x \vee y\}$ полно. Используем равенство $x\&y = \overline{\bar{x} \vee \bar{y}}$.
3. Множество $\{x|y\}$ полно. Напомним, что $x|y = \overline{x\&y}$. Поэтому $x|x = \bar{x}$, а $(x|y)|(x|y) = \overline{x|y} = x\&y$. Таким образом, получаем систему из пункта 1.
4. Множество $\{x \downarrow y\}$ полно. Аналогично предыдущему, так как $x \downarrow y = \overline{x \vee y}$.
5. Множество $\{0, 1, x \cdot y, x + y\}$ полно. Достаточно заметить, что $\bar{x} = x + 1$.

Последний пример рассмотрим подробнее. Полнота системы функций означает, что любую функцию алгебры логики можно выразить формулой, в которой будут встречаться только операции сложения и умножения по модулю 2, а также константы. В этой формуле можно раскрыть скобки и привести подобные члены (используя $a + a = 0$). В результате получится полином по модулю 2. Таким образом, имеем следующее утверждение:

Теорема (Жегалкин). Каждая функция алгебры логики представима полиномом по модулю 2.

Найдем число различных полиномов для переменных $x_1, \ldots, x_n$. Каждый такой полином имеет вид:

$$\sum_{\{i_1,\ldots,i_s\}\subseteq\{1,\ldots,n\}} a_{i_1\ldots i_s} x_{i_1} \cdot \ldots \cdot x_{i_s}.$$

Здесь берутся все подмножества множества $\{1, \ldots, n\}$, включая пустое, которому соответствует свободный член. Таким образом, количество членов в указанной сумме равно 2^n. Для каждого члена имеются две возможности выбора его коэффициента. Следовательно, общее число полиномов указанного вида равно 2^{2^n}. Так как оно равно числу функций алгебры логики от n переменных, то получаем, что каждая функция задается единственным полиномом - иначе для какой-то другой функции полинома не хватило бы.

В алгебре логики полиномы по модулю 2 обычно называются полиномами Жегалкина.

Замыканием множества M функций алгебры логики называется множество всех функций, которые можно получить суперпозициями над M. Оно обозначается $[M]$. В качестве простейшего примера заметим, что $[P_2] = P_2$. Несколько менее тривиальный пример - замыкание множества $\{1, x + y\}$. Очевидно, оно состоит из всех функций алгебры логики, задаваемых формулами вида $c_0 + c_1x_1 + \ldots + c_nx_n$. Такие функции называются линейными. Множество всех линейных функций алгебры логики обозначается L.

Число линейных функций, зависящих от n переменных, равно числу наборов коэффициентов, т.е. 2^{n+1}.

Приведем следующие очевидные свойства оператора замыкания:

1. $[M] \supseteq M$
2. $[[M]] = [M]$
3. Если $M_1 \subseteq M_2$, то $[M_1] \subseteq [M_2]$
4. $[M_1 \cup M_2] \supseteq [M_1] \cup [M_2]$

Класс M функций алгебры логики называется замкнутым, если $[M] = M$. В качестве простейшего примера замкнутого класса можно привести P_2. Класс $\{1, x + y\}$ незамкнут, а класс L - замкнут.

Свойство полноты множества M в терминах оператора замыкания можно сформулировать как $[M] = P_2$.