7-я лекция курса "Теория дискретных функций"

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

1 Вопросы по предыдущей лекции

На почту $tdf2020@yandex.ru$ вопросов не поступило.

2 Лекция 7

На предыдущей лекции были доказаны следующие теоремы:

Теорема (Слупецкий) Пусть система F функций k-значной логики, где $k \geq 3$, содержит все функции одной переменной. Тогда для полноты F необходимо и достаточно, чтобы она содержала существенную функцию, принимающую все k значений.

Теорема(С.В.Яблонский) Пусть система F функций k-значной логики, где $k \geq 3$, содержит все функции одной переменной, принимающие не более $k-1$ значения. Тогда для полноты F необходимо и достаточно, чтобы она содержала существенную функцию, принимающую все k значений.

Докажем следующее следствие теоремы Яблонского:

Теорема(Мартин) Функция $f(x_1, \ldots, x_n)$ из P_k, где $k \geq 3$, образует полную систему (является шефферовой) тогда и только тогда, когда она порождает все функции одной переменной, принимающие не более чем $k-1$ значение.

Необходимость очевидна. Докажем достаточность. Пусть f порождает все функции одной переменной, принимающие не более $k-1$ значения. В частности, она порождает все константы. Поэтому f должна принимать все k значений. Предположим, что она не является существенной. Тогда она должна иметь ровно одну существенную переменную (отсутствие существенных переменных делало бы функцию константной, и она не могла бы принимать k значений). Обозначим через $M(k)$ класс всех функций в P_k, принимающих k значений и имеющих одну существенную переменную. Фактически, это перестановки с добавлением несущественных переменных. Очевидно, что ничего кроме таких же перестановок суперпозициями из f получить нельзя. Однако, для доказательства данного факта придется все же воспользоваться определением операций суперпозиции:

1. Операция подстановки переменных.

   Пусть функция $g(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$ получена из функции f класса $M(k)$. Если f имела существенную переменную x_j, то g будет иметь единственную существенную переменную x_{i_j}. Варьируя значение этой переменной в правой части равенства, будем получать все k значений функции f, но тогда и g принимает все k значений. Следовательно, g принадлежит $M(k)$.

2. Операция подстановки одной функции в другую.

   Пусть функция $h(x_1, \dots, x_{n+m-1}) = f(x_1, \dots, x_{n-1}, g(x_n, \dots, x_{n+m-1}))$ получена из функций f, g класса $M(k)$.

   Если f имеет существенную переменную x_i, где $i < n$, то и h будет иметь единственную существенную переменную x_i. Варьируя значение этой переменной, будем получать в правой части равенства все k значений. Следовательно, g принадлежит $M(k)$.

   Если f имеет существенную переменную x_n, то рассматриваем единственную существенную переменную функции g. Тогда задание ее значения однозначно определяет значение $g(x_n, \dots, x_{n+m-1})$, а вслед за этим и значение $f(x_1, \dots, x_{n-1}, g(x_n, \dots, x_{n+m-1}))$. Таким образом, она является единственной существенной переменной функции h. Варьируя значение данной переменной, можно получить любые k значений функции g, а значит - любые k значений правой части равенства, т.е. все k значений функции h. Следовательно, h принадлежит $M(k)$.

3. Операция добавления либо удаления несущественной переменной. Этот случай очевиден.

Таким образом, из функции f можно получить суперпозициями только функции с единственной существенной переменной, принимающие все k значений. Но тогда нельзя получить ни одной константы. Полученное противоречие означает, что функция f должна быть существенной. И тогда, согласно теореме С.В.Яблонского, она образует полную систему. Теорема доказана.

2.1 Особенности k - значных логик

Для k-значных логик, как и для алгебры логики, имеется критерий полноты в терминах предполных классов. Их лишь конечное число, хотя и быстро растущее с ростом k. Как уже говорилось, Пост получил описание всех замкнутых классов алгебры логики. Их оказалось счетное число. Каждый из них имеет конечный базис. Однако, уже начиная с $k = 3$, множество всех замкнутых классов резко увеличивается. Их мощность становится континуальной, и аналога результатов Поста здесь не известно. Ситуация становится качественно более сложной.

В этом разделе мы рассмотрим несколько теорем, характеризующих отличие случая k-значных логик при $k \geq 3$ от алгебры логики.

Теорема(Янов) Для любого $k \geq 3$ в P_k существует замкнутый класс, не имеющий базиса.

Напомним, что базисом в замкнутом классе Q называется такая систем функций, замыкание которой равно Q, а замыкание любой ее собственной подсистемы не равно Q. Иными словами, базис - такая полная в Q система, что любая ее функция не выражается суперпозициями через остальные ее функции.

Рассмотрим последовательность функций из P_k: $f_0 = 0$; $f_i(x_1, \dots, x_i) = (1 \text{ при } x_1 = \dots = x_i = 2, \text{ иначе } 0)$; $i = 1, 2, \dots$. Пусть M - замыкание множества $\{f_0, f_1, \dots\}$. Покажем, что оно состоит из функций, отличающихся от функций f_i лишь возможным добавлением несущественных переменных. Для этого рассмотрим операции суперпозиции, примененные к функциям такого вида:

1. Операция подстановки переменных.

   Пусть $g(x_1, \dots, x_n) = f(x_{i_1}, \dots, x_{i_n})$. Если f получалась из некоторой f_j добавлением несущественных переменных, то g, ввиду возможного отождествления переменных подстановкой $(i_1, \dots, i_n)$, будет получаться добавлением несущественных переменных из некоторой функции f_m, $m \leq i$.

2. Подстановка одной функции в другую.

   Пусть $h(x_1, \dots, x_{n+m-1}) = f(x_1, \dots, x_{n-1}, g(x_n, \dots, x_{n+m-1}))$, где f, g получаются из некоторых функций f_i добавлением несущественных переменных. Так как g не принимает значение 2, то h тождественно равна 0, т.е. получается добавлением несущественных переменных к f_0.

3. Добавление и удаление несущественных переменных. Этот случай очевиден.

Таким образом, класс M полностью описан. Предположим, что он имеет базис B (конечный либо бесконечный). Рассмотрим два случая:

1. В базисе B имеются хотя бы две различных функции. Пусть одна из них получена добавлением несущественных переменых к функции f_i, а другая - к f_j. Если $i = j$, то одна из них может быть получена из другой добавлением/удалением несущественных переменных. Если $i < j$, то первая получается из второй отождествлением части переменных, с последующим добавлением/удалением несущественных переменных. В обоих случаях одна из функций базиса получается из другой суперпозициями, что невозможно.

2. В базисе B имеется единственная функция. Пусть она получена добавлением несущественных переменных к функции f_i. Но тогда операциями суперпозиции (см. выше) можно получить только функции, получаемые добавлением несущественных переменных к функциям f_j, $j \leq i$. Функцию f_{i+1} получить нельзя, т.е. B - не базис в M.

Полученное противоречие и доказывает отсутствие базиса.

Теорема(Мучник) Для любого $k \geq 3$ в P_k существует замкнутый класс, имеющий счетный базис.

Рассмотрим последовательность функций $f_i(x_1, \dots, x_i)$; $i = 2, 3, \dots$. Функция $f_i(x_1, \dots, x_i)$ принимает значение 1 , если в наборе значений ее аргументов имеется ровно одна единица, а остальные значения равны 2. В прочих случаях она принимает значение 0. Обозначим через M замыкание множества $\{f_2, f_3, \dots,\}$. Покажем, что система $\{f_2, f_3, \dots,\}$ является базисом в M. Очевидно, она полна в M. Покажем, что никакая функция f_m, $m \geq 2$, не выражается суперпозициями через функции $f_2, \dots, f_{m-1}, f_{m+1}, \dots$.

Предположим противное. Рассмотрим какую-либо сигнатуру Σ для $\{f_2, \dots, f_{m-1}, f_{m+1}, \dots\}$. Должна существовать невырожденная формула Φ в данной сигнатуре, определяющая относительно переменных $x_1, \dots, x_m$ функцию $f_m(x_1, \dots, x_m)$. Будем считать, что Φ не имеет других (несущественных) переменных. Если таковые имелись, вместо них подставляем переменную x_1, что не изменит функции, реализуемой формулой. По определению формулы, Φ имеет вид $s(B_1, \ldots, B_r)$, где s - символ сигнатуры, обозначающий некоторую функцию f_r, $r \neq m$. Каждое B_i - либо переменная, либо невырожденная формула в Σ. Рассмотрим произвольный набор $(\alpha_1, \ldots, \alpha_m)$ значений переменных $x_1, \ldots, x_m$. Обозначим β_i значение формулы B_i на данном наборе; $i = 1, \ldots, r$. Тогда $f_m(\alpha_1, \ldots, \alpha_m) = f_r(\beta_1, \ldots, \beta_r)$. Рассмотрим три случая:

1. Среди формул B_i имеется не менее двух невырожденных. Тогда не менее двух значений β_i равны 0 либо 1. На таком наборе $(\beta_1, \ldots, \beta_r)$ функция f_r обращается в 0, т.е. f_m оказывается тождественно равной нулю, что неверно.

2. Среди формул B_i имеется ровно одна невырожденная формула; пусть это формула B_j. Так как $r \geq 2$, то существует j', отличное от j, такое, что $B_{j'}$ - переменная. Пусть это будет переменная x_q. Если положить $\alpha_q = 1; \alpha_1 = \ldots = \alpha_{q-1} = \alpha_{q+1} = \ldots = \alpha_m = 2$, то $f_m(\alpha_1, \ldots, \alpha_m) = 1$. Но $\beta_{j'} = 1$, $\beta_j \in \{0, 1\}$, так что $f_r(\beta_1, \ldots, \beta_r) = 0$ - противоречие.

3. Все формулы B_i суть переменные. Тогда $r > m$ (т.к. все переменные функции f_m существенные). Следовательно, существуют такие i, j; $i \neq j$, что B_i и B_j - одна и та же переменная. Пусть это будет переменная x_q. Снова берем $\alpha_q = 1; \alpha_1 = \ldots = \alpha_{q-1} = \alpha_{q+1} = \ldots = \alpha_m = 2$. Тогда $f_m(\alpha_1, \ldots, \alpha_m) = 1$. Но $\beta_i = \beta_j = 1$, и $f_r(\beta_1, \ldots, \beta_r) = 0$ - противоречие.

Во всех случаях получаем противоречие, и теорема доказана.

Из доказанной теоремы немедленно получаем следствие:

Теорема. Для любого $k \geq 3$ в P_k имеется континуум предполных классов.

Рассмотрим взаимно-однозначное отображение φ множества рациональных точек отрезка [0,1] на множество функций $f_2, f_2, \ldots$ из предыдущей теоремы. Для любого вещественного числа a из отрезка [0,1] рассмотрим множество Q_a всех рациональных чисел данного отрезка, меньших или равных числа a. Множества Q_a непусты и различны. Их континуум. Отображение φ переводит данные множества в различные множества F_a функций последовательности $f_2, f_3, \ldots$. Пусть M_a - замыкание множества F_a. Если $a < b$, то в F_b есть функция, не принадлежащая F_a. Согласно доказательству предыдущей теоремы, она не будет принадлежать и замыканию F_a, т.е. M_a. Таким образом, $M_a \neq M_b$, и все замкнутые классы M_a различны. Мощность их множества континуальна. Теорема доказана.

Интересно, что построено даже линейно упорядоченное по включению континуальное семейство замкнутых классов в P_k.

В заключение рассмотрим вопрос о представимости функций k-значной логики полиномами в кольце вычетов по модулю k. Напомним, что в двузначном случае любая функция была представима полиномом Жегалкина.

Теорема. Система полиномов по модулю k полна в P_k тогда и только тогда, когда k - простое число.

Рассмотрим произвольную функцию $f(x_1, \ldots, x_n)$ из P_k. Для нее имеет место следующее соотношение:

$$f(x_1, \ldots, x_n) = \sum_{(\sigma_1, \ldots, \sigma_m)} j_{\sigma_1}(x_1) \cdot \ldots \cdot j_{\sigma_n}(x_n) \cdot f(\sigma_1, \ldots, \sigma_n) (\mathrm{mod} k)$$

Это - аналог совершенной д.н.ф. из алгебры логики. Вместо максимума используется сумма по модулю k, а вместо минимума - умножение по модулю k.

Тождество $j_\sigma(x) = j_0(x - \sigma)$ позволяет выразить все функции j_σ через функцию j_0. Если функцию j_0 можно выразить полиномом по модулю k, то, подставляя это выражение в указанную выше формулу, раскрывая скобки и приводя подобные члены, получим представление полиномом произвольной функции f. Обратно, если j_0 не выразима полиномом, то не каждая функция из P_k выразима. Таким образом, все свелось к изучению того, при каких k функция j_0 представима в виде полинома. Рассмотрим два случая:

1. k - простое. Вспомним малую теорему Ферма, согласно которой $x^{k-1} \equiv 1 (\bmod\ k)$ при всех $x = 1, \ldots, k-1$. Из нее вытекает соотношение $j_0(x) = 1 - x^{k-1} (\bmod\ k)$, т.е. $j_0(x)$ представима полиномом по модулю k, и система полиномов в этом случае полна.

2. k - составное. Пусть $k = k_1 \cdot k_2$, где $k_1 \geq k_2 > 1$ - натуральные. Предположим, что $j_0(x) = b_0 + b_1 x + \ldots + b_s x^s (\bmod\ k)$. Подставляя $x = 0$, получаем $b_0 = 1$. Подставляя $x = k_1$, получаем:

   $0 = 1 + b_1 k_1 + \ldots + b_s k_1^s (\bmod\ k)$.

   Это означает, что для некоторого целого n выполнено:

   $1 + b_1 k_1 + \ldots + b_s k_1^s = kn$.

   После перегруппировки членов и замены k на $k_1 k_2$ имеем:

   $1 = k_1 k_2 n - b_1 k_1 - \ldots - b_s k_1^s$.

   Правая часть делится на k_1 а левая не делится - противоречие.

Теорема доказана.