***1. Логические связки. Понятие. Пример.***

**Логическая связка**— это символические конструкции логических языков, используемые для образования сложных высказываний из элементарных высказываний.

**Логические связки**:

Конъюнкция: A ∧ B

Дизъюнкция: A ∨ B

Импликация: A → B

Эквивалентность: A ↔ B

**Пример:** Пусть P означает «идёт дождь», а Q – «на улице холодно». Тогда P ∧ Q означает: «идёт дождь и на улице холодно».

***2. Тавтология. Пример. Док-во разбором случаев.***

**Тавтология** - составное высказывание, которое истинно при любых значениях входящих в них элементарных высказываний.

**Пример:** P ∨ ¬P

**Док-во разбором случаев:**

Рассмотрим два случая для высказывания P ∨ ¬P:

*Случай 1:* Пусть P истинно. Тогда ¬P ложно, и P ∨ ¬P = истина ∨ ложь = истина

*Случай 2:* Пусть P ложно. Тогда ¬P истинно, и P ∨ ¬P = ложь ∨ истина = истина

Во всех случаях формула истинна, то есть она является тавтологией.

***3. Транзитивность. Пример. Док-во от противного.***

Отношение R называется **транзитивным**, если для любых элементов a, b и c верно:

Если aRb и bRc, то aRc (тавтология).

**Пример:** Отношение «строго больше» на множестве вещественных чисел.

Если a > b и b > c, то a > c.

**Док-во от противного:** Пусть у нас есть два истинных утверждения: A→B и B→C.

Мы хотим доказать, что A→C истинно.

Предположим, от противного, что A→C ложно. Тогда должно быть истинно A и ложно C. Но из истинности A и истинности A→B следует, что B истинно. Далее, имея B истинным и B→C истинным, получаем, что C истинно, что противоречит предположению. Следовательно, наше предположение неверно, и A→C транзитивно.

***4. Закон контрапозиции. Док-во. Пример.***

**Закон контрапозиции:** Импликация A→B эквивалентна ¬B → ¬A (тавтология).

**Док-во:** Левая часть ложна тогда и только тогда, когда A = И, B = Л.

Правая часть ложна тогда и только тогда, когда ¬В = И, ¬A = Л. Но это равносильно первым двум условиям. Поэтому значения левой и правой части всегда одинаковы.

**Пример:** Если «Если идёт дождь, то улицы мокрые» (P → Q), то контрапозиционное утверждение: «Если улицы не мокрые, то дождя нет» (¬Q → ¬P) тоже истинно.

***5. Законы де Моргана. Док-во.***

Формулировка **законов де Моргана**:

¬(A ∧ B) ≡ ¬A ∨ ¬B;

¬(A ∨ B) ≡ ¬A ∧ ¬B.

**Док-во с использованием таблицы истинности** (пример для первой формулы):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 3A | B | A∧B | ¬(A∧B) | ¬A | ¬B | ¬A∨¬B |
| 0 | 0 | 0 | 1 | 1 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 | 1 |
| 1 | 0 | 0 | 1 | 0 | 1 | 1 |
| 1 | 1 | 1 | 0 | 0 | 0 | 0 |

Так как для каждой комбинации переменных значения ¬(A ∧ B) и ¬A ∨ ¬B совпадают, формула доказана. Аналогичный метод применим для второй формулы.

***6. Булевы функции. Понятие. Существенные и несущественные переменные.***

**Булева ф-ция** - это ф-ция вида f :{0, 1}N т.е. ф-ция, принимающая на вход N булевых значений и выдающая 0 или 1.

Переменная xi является **существенной**, если выполняется

f(a1, … , ai-1, 0, ai+1, … , aN) ≠ f(a1, … , ai-1, 1, ai+1, … , aN) для любых a1, … , ai-1, ai+1, … , aN ∈ {0, 1}.

Переменная xi является **несущественной**, если выполняется

f(a1, … , ai-1, 0, ai+1, … , aN) = f(a1, … , ai-1, 1, ai+1, … , aN) для любых a1, … , ai-1, ai+1, … , aN ∈ {0, 1}.

**Пример:** Для функции f(x, y) = x переменная x существенная, так как её изменение влияет на f. Переменная y несущественная, так как f не зависит от y.

***7. Способы задания Булевых ф-ций. Система булевых ф-ций. Понятие.***

**Способы задания булевых ф-ций:**

**Таблица истинности:** Перечисляются все 2n комбинаций значений для n переменных и соответствующие значения функции.

**Формулой:** f(x1, x2, x3) = (x1 ∧ x2) ∨ (x1 ∧ x3) ∨ (x2 ∧ x3)

**Система булевых ф-ций** - это набор булевых ф-ций.

***8. Теорема о полноте системы {∧, ∨, ¬}. Док-во.***

Ф-цию ƒ будем называть **выразимой** в системе В, если существует формула в системе В, которая задаёт ф-цию f.

Система называется **полной**, если любая булева ф-ция выразима в этой системе.

**Теорема:** Система логических операций {∧, ∨, ¬} является функционально полной.

**Док-во.** Сначала научимся выражать через конъюнкции и отрицания особые функции, которые равны 1 для одного набора аргументов (а1, a2, ..., an), а на остальных равны 0. Примером такой функции является конъюнкция переменных: x1 ∧ … ∧ xn. Она равна 1 только лишь на наборе (1, 1, … , 1).

Чтобы получить ф-цию ea, которая равна 1 лишь на наборе аргументов а = (a1, a2, ... , an), нужно в конъюнкции заменить часть переменных на отрицания. А именно, если аi = 1, то включаем в конъюнкцию переменную хі; если аi = 0, то включаем в конъюнкцию ¬хі. Это гарантирует, что на наборе (а1, a2, ... , аn) такая формула принимает значение 1. Для любого другого набора (b1, b2, ... , bn) при некотором і выполняется неравенство bi ≠ аi. Но тогда соответствующий член конъюнкции обращается в 0 и вся конъюнкция также равна 0.

Теперь выразим произвольную булеву ф-цию. Для этого возьмём дизъюнкцию формул для ф-ций ea по всем а, для которых f(a) = 1. Такая формула даёт значение 1 только если один из членов дизъюнкции равен 1. Но каждый член дизъюнкции ea равен 1 ровно на одном наборе а. Поэтому построенная формула выражает f.

***9. Теорема о полноте систем {∨, ¬}, {∧, ¬}, {1, ⊕, ∧}. Док-во.***

**Док-во.** Полнота первых двух систем следует из тождеств:

x ∧ y = ¬(¬x ∨ ¬y), x ∨ y = ¬(¬x ∧ ¬y) то есть законов де Моргана.

Для полноты третьей системы (базис Жегалкина) нужно тождество, выражающее ¬ через 1, ⊕:

¬x = 1 ⊕ x, это тождество очевидно из определения ⊕. Получаем представления обеих ф-ций из полной системы {∨, ¬} в базисе Жегалкина.

***10. Многочлен Жегалкина. Существование и единственность.***

**Многочленом Жегалкина** называются сумма по модулю 2 конъюнкций переменных.

**Теорема:** Каждая булева ф-ция однозначно представляется в виде многочлена Жегалкина.

**Док-во.** *Существование.* Индукция по числу переменных n. База индукции n = 0, то есть константы. По нашим соглашениям они выражаются в виде многочлена Жегалкина.

Шаг индукции. По функции f(x1, ... , xn+1 ) от n+1 переменной определим две функции от n переменных: f0(x1, ... ,xn) = f(x1, … , xn, 0) и f1(x1, … , xn) = f(x1, ... , xn, 1).

Тогда f=((1 ⊕ xn+1 )f0) ⊕ (xn+1 f1) = f0 ⊕ xn+1 (f0 ⊕ f1).

Действительно, при xn+1 = 0 получаем f = f0, а при xn+1 = 1 – f = f1.

По предположению индукции и f0, и f1 выражаются как многочлены Жегалкина. Тогда и fo ⊕ f1 выражается как многочлен Жегалкина (возьмём симметрическую разность множеств одночленов для f0 и для f1).

Раскрывая скобки во втором слагаемом, получим многочлен Жегалкина для f.

*Единственность.* Двоичных слов длины 2^n ровно 2^(2^n), поэтому и булевых ф-ций столько же. А сколько многочленов Жегалкина? В каждом одночлене все переменные разные (это не ограничивает общности, так как x ∧ x ≡ 2). Поэтому различных одночленов столько же, сколько подмножеств множества n переменных, то есть 2^n. Каждому многочлену однозначно сопоставляется множество одночленов, суммой которых он является (так как x ⊕ x ≡ 0, это не ограничивает общности). Поэтому всего многочленов Жегалкина столько же, сколько подмножеств 2^n-элементного множества, то есть, тоже 2^(2^n)

Но мы уже знаем, что соответствие «многочлен f» → «ф-ция, задаваемая многочленом f» является сюръективной ф-цией (существование прообраза уже доказано). Осталось заметить, что сюръекция между двумя конечными множествами одинакового размера является также и инъекцией (если два различных элемента из множества А имеют одинаковый образ в множестве В, то в образе f(А) меньше элементов, чем в А), а потому биекцией. Это и означает единственность.

***11. Замкнутость систем булевых ф-ций. Док-во. Примеры.***

Система ф-ций F называется **замкнутой**, если любая формула в этой системе выражает ф-цию из F.

Замкнутая система полна лишь в том случае, когда совпадает с множеством всех ф-ций.

Доказательства замкнутости системы основаны на следующей лемме.

**Лемма:** Пусть система F содержит функции-переменные и для любых f, g1, g2, ... , gn ∈ F выполняется f(g1(x(1)), g2(x(2)), ... , gn(x(n)) ∈ F, где х(і) какие-то множества переменных. Тогда F замкнутая.

**Док-во**. Докажем, что любая формула в системе F задаёт ф-цию из F.

*Индукция по разбору формулы*. Технически это Док-во по длине формулы. Базисом индукции будут формулы хі, они принадлежат F по условию.

Шаг индукции. Рассмотрим формулу вида Φ = f( g1(x(1)), g2(x(2)), ... , gn (x(n)) ), где ƒ ∈ F, а gі - какие-то формулы в системе F. Для формул gі выполняется индуктивное предположение, то есть gі Є F. Но тогда по условию Ф задаёт ф-цию из F.

**Примеры замкнутых систем булевых ф-ций (классов).**

Все они неполные, так как не содержат всех булевых ф-ций.

**Функции, сохраняющие 1, класс Т1.** Это функции, удовлетворяющие равенству

f(1, 1, ..., 1, 1) = 1.

**Функции, сохраняющие 0, класс Т0.** Это функции, удовлетворяющие равенству

f(0,0,..., 0, 0) = 0.

***12. Примеры замкнутых классов. Теорема Поста (без доказательства).***

**Примеры замкнутых классов булевых ф-ций:**

**Функции, сохраняющие 0, класс T0:** Функции, удовлетворяющие f(0, 0, ... , 0, 0) = 0.

**Функции, сохраняющие 1, класс T1:** Функции, удовлетворяющие f(1, 1, ... , 1, 1) = 1.

**Монотонные функции, класс M:** Функции, у которых увеличение значений переменных не уменьшает результат функции, т.е. xі ≤ yi для всех 1 ≤ i ≤ n: f(x1, ... , xn) ≤ f(y1 ,.... , yn).

**Линейные функции, класс L:** Функции, представимые линейными многочленами Жегалкин, т. е. xi1 ⊕ xi2 ⊕ … ⊕ xik ⊕ a, где xij – переменные, ∈ {0, 1}.

**Самодвойственные функции, класс S:** Функции, для которых верно f(¬x1, … , ¬xn) = ¬f(x1, … , xn), для всех наборов аргументов x1, … , xn.

**Теорема Поста:** Система В является полной тогда и только тогда, когда она не лежит целиком ни в одном из классов Т0, Т1, M, L, S.

***13. Формула включений и исключений. Замечания.***

Формула включений и исключений

N(a’1, a’2, ... , a’n) = N - N(a1 ) - ... - N(an) + N(a1, a2) + ... + N(an-1 , an) + ... + (-1)n N(a1, ... , an).

Без доказательства.

**Замечание.** Рассмотрим A = {a1, ... , an} и все m-размещения с повторениями из А, m < n. Таких размещений всего N = nm . Объектами, к которым мы будем применять формулу включений и исключений будут эти N размещений. Размещение обладает свойством ai, если элемент аi, не принадлежит ему. N(a’1, a’2, ... , a’n) - количество объектов не обладающих ни одним из n свойств. Очевидно,

N(a’1, a’2, ... , a’n) = 0; N(ai) = (n - 1)m; N(ai, aj) = (n - 2)m; … ; N(a1, ... , an) = (n - n)m = 0;

Тогда, 0 = N(a’1, a’2, ... , a’n) = Cn0(nm) - Cn1((n – 1)m) + Cn2((n - 2)m) - ... + (-1)n - 1 (n - (n - 1))m + (-1)n (n - n)m.

Иначе перепишем эту формулу в виде: 0 = ∑k = 0 по n ( (-1)^k \* Cn^k(n - k)^m ).

Док-во следует из формулы включений и исключений.

**Замечание.** Cn0 - Cn1 + ... + (-1)n Cnm = {1, n = 0 \\ 0, n ≥ 1.

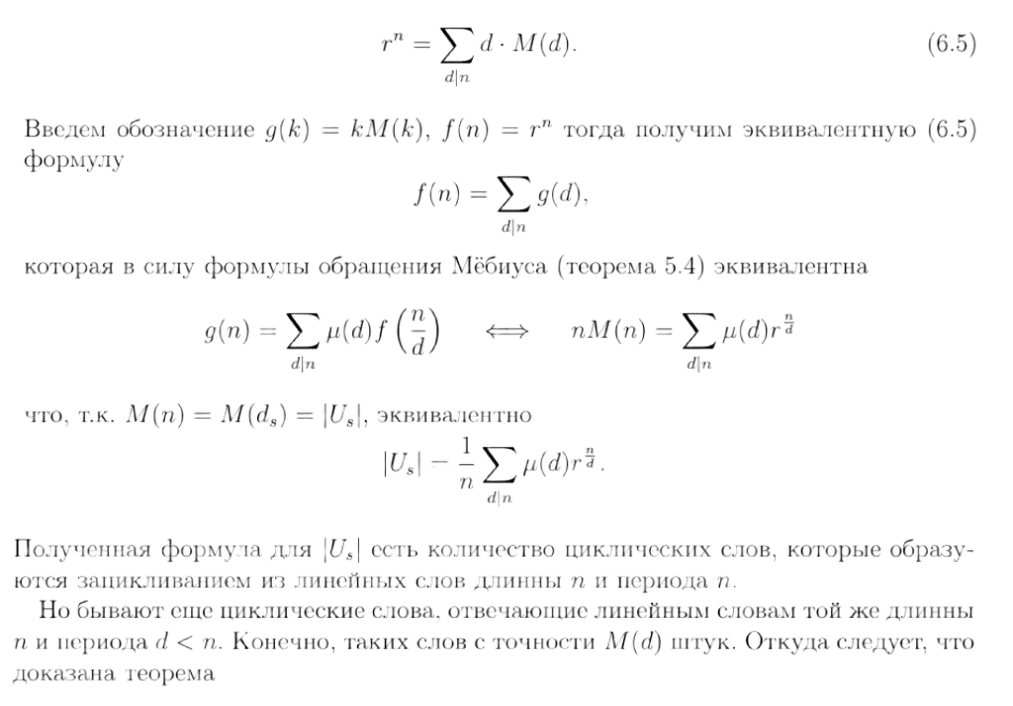
**Док-во**. Применим бином Ньютона:

0 = (1 + (-1))n = ∑k=0 по n (Cnk (-1)k (1)n - k) = ∑k = 0 по n (-1)k Cnk = Cn0 - Cn1 + Cn2 + ... + (-1)n Cnm.

***14. Ф-ция Мёбиуса. Определение. Пример.***

**Ф-цией Мёбиуса** называется ф-ция вида:

для числа n ∈ N.

**Пример:** ∑ d|12 f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12).

***15. Лемма о сумме ф-ций Мёбиуса по делителям числа. Док-во.***

**Лемма:**

**Док-во**. Для n = 1 лемма очевидна, докажем её для n ≥ 2. По основной теореме арифметики имеет место каноническое разложение: n = p1k1 \* p2k2 \* ... \* psks

Тогда d|n можно представить как d = p1l1 \* p2l2 \* ... \* psls , (5.3), где 0 ≤ l1 ≤ k1 , ... , 0 ≤ ls ≤ ks. Действительно, рассмотрим пример: d|12 (при каноническом разложении 12 = 22 \* 31 ) можно представить как d = 22 \* 31 = 12; d = 21 \* 31 = 6; d = 20 \* 31 = 3; d = 22 \* 30 = 4; d = 21 \* 30 = 2; d = 20 \* 30 = 1. Заметим, что u(d) = 0, если хотя бы одно li ≥ 2 в разложении (5.3) в силу определения функции Мёбиуса. Следовательно, такое d не дает вклад в сумму ∑d|n u(d). Теперь в разложении ∑d|n u(d) нас интересуют только слагаемые, в разложении (5.3) которых каждое li равно либо нулю либо единице. Таких слагаемых ровно 2s.

∑d|n u(d) = u(1) + s \* (-1) + Cs2 \* (-1)2 + Cs3 \* (-1)3 + ... + Css \* (-1)s (5.4), где второе слагаемое получается как произведение числа способов взять одну единицу и s - 1 нулей в представлении l1, ... , ls (т.е. s) на u(pi1) = -1 (где pi соответствует li равному 1). Третье слагаемое в формуле (5.4) получается как произведение числа способов взять две единицы и s - 2 нулей в представлении l1, ... , ls (т.е. Cs2) на u(pi1 \* pj1) = (-1)2. Аналогично рассуждая получаем последнее слагаемое. Выражение (5.4) представляет собой знакопеременную сумму равную нулю s ≥ 1.

***16. Формула обращения Мёбиуса. Док-во.***

**Теорема (Формула обращения Мёбиуса):** Пусть есть ф-ция g(n) натурального аргумента n и ф-ция f(n) = ∑d|n g(d). Тогда g(n) = Σd|n u(d) \* f(n/d).

Заметим, что для функции g(n) натурального аргумента и верно так же представление g(n) = ∑d|n u(n/d) \* f(n/d), т. к. n/d является делителем числа n если делителем является число d.

**Док-во:** f(n/d) = ∑d’|(n/d) g(d’) (d \* d’ = n)

g(n) = ∑d’|(n/d) g(d’) \* ∑d|n g(d) = ∑dd’|n u(d)\*g(d’) = ∑dd’|n u(d’)\*g(d) – коммутативно, (d \* d’ должно быть < n)

∑d|n g(d)\*( ∑d’|(n/d) u(d’) )

Пусть d = n: g(n) \* ∑d’|1 u(d’) + ∑d|n, d < n g(d) \* ∑d’|(n/d), d < n u(d’) = g(n)

Первое слагаемое равно 1, а второе 0. Противоречие.

***17. Циклические последовательности. Понятие. Пример.***

**Циклическая последовательность** – последовательность, элементы которого повторяются по кругу до заданного количества повторов.

**Пример:** 1,  2,  3,  1,  2,  3,  1,  2,  3,  … является циклической с периодом 3.

***18. Циклический сдвиг. Период. Лемма о периоде линейн слова. Док-во.***

**Циклическим сдвигом** линейного слова a1, a2, … , an будем называть операцию, переводящую это линейное слово в слово a2, … , an, a1.

**Период** dлинейного слова — это наименьшее количество циклических сдвигов, переводящих слово в само себя.

**Лемма о периоде линейного слова**: Период d любого линейного слова длинны n является делителем числа n.

**Док-во**. Предположим, что d не является делителем числа n. Тогда разделим n на d с остатком r:

N = d \* k + r, 1≤ r < d.

***19. Линейное слово. Циклическое слово. Лемма о длине линейного слова и его периоде. Док-во.***

**Линейное слово** – конечная последовательность символов из некоторого алфавита, у которого есть четкое начало и конец.

**Циклическое слово** – набор линейных слов, которые считаются одинаковыми, если одно можно получить из другого сдвигом символов по кругу.

*1-й блок 2-й блок -й блок*

**Лемма:** Любое линейное слово длинны n и периода d имеет вид

причем а1, a2, ... , ad - линейное слово у которого и длинна и период равны d.

**Док-во**. Рассмотрим d сдвигов линейного слова

где после d сдвигов должно образоваться исходное слово a1, a2, ... , аn, т.е. есть совпадение линейного слова а1, 2, ... , аd со словом аd+1, аd+2, ... , ad+d. Откуда и следует требуемое.

***20. Теорема о количестве всех циклических слов. Док-во.***

**Теорема:**

