Дискретная математика

1. Логические связки. Понятие. Пример.

**Логическая связка**— это функция, объединяющая односоставные (атомарные) высказывания в составное высказывание, при этом истинностное значение результата определяется значениями входящих высказываний.

**Логические связки**:

* Отрицание: ¬A
* 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. Доказательство разбором случаев.

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

**Пример:** P ∨ ¬P

**Доказательство 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. Доказательство 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.

**Доказательство 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. Доказательство. Пример.

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

**Доказательство:** 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. Доказательство.

Формулировка **законов де Моргана**:

* ¬(A ∧ B) ≡ ¬A ∨ ¬B;
* ¬(A ∨ B) ≡ ¬A ∧ ¬B.

**Доказательство с использованием таблицы истинности** (пример для первой формулы):

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| A | 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 | 0 | 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 функция** - это функция вида f :{0, 1}N т.е. функция, принимающая на вход N булевых значений и выдающая 0 или 1.

Переменная xi является **существенной**, если равенство f(a1, … , ai-1, 0, ai+1, … , aN) ≠ f(a1, … , ai-1, 1, ai+1, … , aN) выполняется для любых a1, … , ai-1, ai+1, … , aN ∈ {0, 1}.

Переменная xi является **несущественной**, если равенство f(a1, … , ai-1, 0, ai+1, … , aN) = f(a1, … , ai-1, 1, ai+1, … , aN) выполняется 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 функций. Система булевых функций. Понятие.

**Способы задания булевых функций:**

* 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 функций** - это набор булевых функций.

8. Теорема о полноте системы {∧, ∨, ¬}. Доказательство.

Функцию ƒ будем называть **выразимой** в системе В, если существует формула в системе В, которая задаёт функцию f.

Система называется **полной**, если любая булева функция выразима в этой системе.

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

**Доказательство.** 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 функцию 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 функцию. Для этого возьмём дизъюнкцию формул для функций 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, ⊕, ∧}. Доказательство.

**Доказательство.** 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 функций из полной системы {∨, ¬} в базисе Жегалкина.

10. Многочлен Жегалкина. Существование и единственность.

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

**Теорема:** Каждая булева функция однозначно представляется в виде многочлена Жегалкина.

**Доказательство.**

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

Шаг индукции. По функции f(x1, ... , xn+1 ) 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. Сколько всего есть булевых функций от переменных? Такая функция взаимно однозначно задаётся таблицей значений. Но таблицы значений находятся во взаимно однозначном соответствии с двоичными словами длины 2^n: запишем все 2^n различных наборов значений n булевых переменных в каком-то порядке, после этого таблица значений задаётся двоичным словом длины 2^n (на і-м месте стоит f( x^(i) ), где x^(i) – i набор значений переменных). В качестве иллюстрации запишем слово для конъюнкции x1∧ x2, предполагая, что наборы значений переменных упорядочены лексикографически:

00 01 10 11

0 0 0 1

Из этой таблицы видно, что конъюнкции соответствует слово 0001.

Двоичных слов длины 2^n ровно 2^(2^n), поэтому и булевых функций 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» → «функция, задаваемая многочленом f» является сюръективной функцией (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 функций. Доказательство. Примеры.

Система функций F называется **замкнутой**, если любая формула в этой системе выражает функцию из F.

Замкнутая система полна лишь в том случае, когда совпадает с множеством всех функций.

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.

**Доказательство**. Докажем, что любая формула в системе F задаёт функцию из F.

Индукция по разбору формулы. Технически это доказательство 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 функцию из Г.

**Примеры замкнутых систем булевых функций (классов).**

Все они неполные, так как не содержат всех булевых функций.

* **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 функций:**

* **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:** 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, a2, ... , an). Без доказательства.

**Замечание.** Рассмотрим A = {a1, ... , an} и все m-размещения с повторениями из А, m < n. Таких размещений всего N = n^m . 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, a2, ... , an) = (n - n)^m = 0,

Тогда, 0 = N(a’1, a’2, ... , a’n) = Cn^0(n^m) - Cn^1((n - 1)^m) + Cn^2((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 ).

Доказательство следует из формулы включений и исключений.

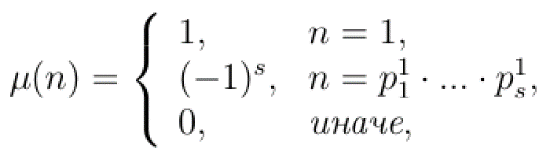
**Замечание.** Cn^0 - Cn^1 + ... + (-1)^n Cn^m = { 1, n = 0 \\ 0, n ≥ 1.

Доказательство. Применим бином Ньютона:

0 = (1 + (-1))^n = ∑k=0 по n ( Cn^k (-1)^k \* (1)^(n - k) ) = ∑k = 0 to n (- 1)^k \* Cn^k = Cn^0 - Cn^1 + Cn^2 + ... + (-1)^n Cn^m.

14. Функция Мёбиуса. Определение. Пример.

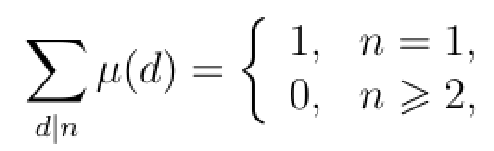
Функцией Мёбиуса называется функция вида:

 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 функций Мёбиуса по делителям числа. Доказательство.

Формулировка леммы: Для ∑ d|12 f(d) = f(1) + f(2) + f(3) + f(4) + f(6) + f(12).



**Доказательство**. Для n = 1 лемма очевидна, докажем её для n ≥ 2. По основной теореме арифметики имеет место каноническое разложение: n= p\_{1} ^ k\_{1} \* p\_{2} ^ k\_{2} \* ... \* p \_{s} ^ k\_{s}

Тогда d|n можно представить как d = p\_{1} ^ l\_{1} \* p\_{2} ^ l\_{2} \* ... \* p\_{s} ^ l\_{s} (5.3), где 0 ≤ l\_{1} ≤ k\_{1} , ... , 0 ≤ l\_{s} ≤ k\_{s}. Действительно, рассмотрим пример: d|12 (при каноническом разложении 12 = 2 ^ 2 \* 3 ^ 1 ) можно представить как d = 2 ^ 2 \* 3 ^ 1 = 12; d = 2 ^ 1 \* 3 ^ 1 = 6; d = 2 ^ 0 \* 3 ^ 1 = 3; d = 2 ^ 2 \* 3 ^ 0 = 4; d = 2 ^ 1 \* 3 ^ 0 = 2; d = 2 ^ 0 \* 3 ^ 0 = 1. Заметим, что u(d) = 0, если хотя бы одно l\_{i} ≥ 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 l\_{i} равно либо нулю либо единице. Таких слагаемых ровно 2^s.

∑d|n u(d)= u(1) + s \* (-1) + C\_{s} ^ 2 \* (- 1) ^ 2 + C\_{s} ^ 3 \* (-1) ^ 3 + ... + Cs ^ s \* (-1)^ s (5.4), где второе слагаемое получается как произведение числа способов взять одну единицу и s - 1 нулей в представлении l\_{1}, ... , l\_{s} (т.е. s) на u(p\_{i} ^ 1) = -1 (где p\_{i} соответствует l\_{i} равному 1). Третье слагаемое в формуле (5.4) получается как произведение числа способов взять две единицы и s - 2 нулей в представлении l\_{1}, ... , l\_{s} (т.е. C\_{s} ^ 2) на u(p\_{i} ^ 1 \* p\_{j} ^ 1) = (-1) ^ 2. Аналогично рассуждая получаем последнее слагаемое. Выражение (5.4) представляет собой знакопеременную сумму равную нулю s ≥ 1.

16. Формула обращения Мёбиуса. Доказательство.

**Теорема (Формула обращения Мёбиуса):** Пусть есть функция g(n) натурального аргумента n и функция 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.

ДОБАВИТЬ ДОКАЗАТЕЛЬСТВО

17. Циклические последовательности. Понятие. Пример.

НЕТ ОПРЕДЕЛЕНИЯ

1,  2,  3,  1,  2,  3,  1,  2,  3,  … является циклической с периодом 3.

18. Циклический сдвиг. Период. Лемма о периоде линейного слова. Доказательство.

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

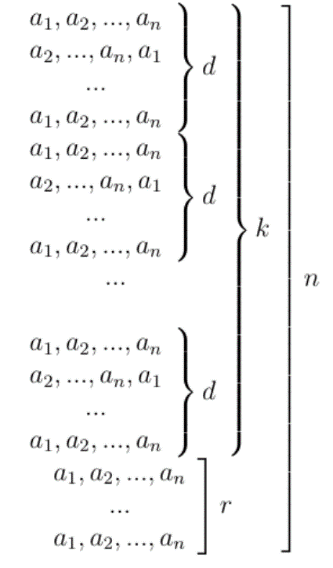
**Период** линейного слова — это наименьшее количество циклических сдвигов, переводящих слово в само себя.

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

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

N = d \* k + r, 1≤ r < d.

Произведем d \* k циклических сдвигов линейного слова а1, а2, ... , аn. С другой стороны, применим n циклических сдвигов линейного слова a1, a2, ... , аn. Получим тоже слово. Учитывая остаток от деления r мы должны получить:

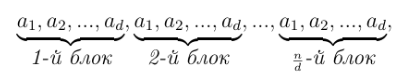


Получается, что за r < d сдвигов слово перешло в себя, но d - по определению наименьшее число сдвигов, после которых слово переходит в себя. Мы получили противоречие, и, следовательно, наше предположение не верно. Таким образом d делит n, что и требовалось доказать.

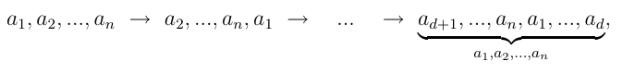
19. Линейное слово. Циклическое слово. Лемма о длине линейного слова и его периоде. Доказательство.

Определения:

НЕТ ОПРЕДЕЛЕНИЙ

**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.

**Доказательство**. 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.