Министерство образования и науки
Российской Федерации
Государственная классическая академия им. Маймонида

В.В.Вьюгин

Дискретная математика

Часть 1

Элементы теории множеств.
Комбинаторика.
Функции алгебры логики.

Москва - 2009

Вьюгин В.В . «Дискретная математика. Часть 1. (Элементы теории множеств.. Комбинаторика. Функции алгебры логики.) М.: 2009 – 65с.
Пособие составлено на основе первой части годового курса «Дискретная» математика», который входит в обязательную программу факультета математики и и информатики Государственной классической академии им. им. Маймонида.. Другие части курса: - «Дискретная математика. Часть 2 (Элементы теории графов), «Дискретная математика. Часть 3 (Основы теории вычислений). В конце каждого раздела приведены образцы задач для практических занятий по курсу.
Графические материалы пособия подготовлены студентом ГКА им. Маймонида А.Феденко. .
Для студентов первых курсов прикладных математических специальностей.
Библ. 4 .

Оглавление

1. Элементы теории множеств.

1.1. Множества. Операции над множествами. Основные тождества.

Понятие множества является исходным в современной математике и не имеет точного определения. Мы даем лишь неформальное пояснение этого понятия.

Множество – это собрание элементов, обладающих некоторым общим признаком - пишем

A={x: E(x)}, где E – некоторое свойство элементов *x*. Обозначим $x \in A$, если x является элементом множества A, обозначим также $x \notin A$, если *x* не является элементом *A*.

Например, можно рассматривать множество всех точек на плоскости, множество всех прямых, множество студентов группы и т.д. Более точный смысл имеют числовые множества:

N={n: n – натуральное число}={ 1, 2, 3, 4, ... }, Z={n: n – целое число={ ..., -1, 0, 1, 2, ... }, Q={r: r – рациональное число}, R={r: r – вещественное число}, [0,1]={r: 0≤ r≤ 1} – множество всех вещественных чисел, лежащих в единичном замкнутом интервале.

Конечное множество можно задать просто перечислением всех его элементов. Например, $A=\{7,1,12,4,8\}$, $B=\{a_1,a_2,\dots a_n\}$.

Множество *A* является подмножеством множества *B*, обозначается это как $A \subseteq B$, если всякий элемент *A* является элементом *B*, т.е. из следует $x \in B$ для всех *x*.

Операции над множествами:

Объединение $A \cup B = \{x : x \in A\_или\_x \in B\}$ - состоит из всех элементов множеств A и B, собранных вместе.

Пересечение $A \cap B = \{x : x \in A\_и\_x \in B\}$ - состоит из элементов, принадлежащих A и B одновременно.

В некоторых случаях пересечение двух множеств может не содержать ни одного элемента. Для обозначения пустого множества, т.е. множества, не содержащего ни одного элемента, используется символ $\emptyset$.

Разность двух множеств $A \div B = \{x : x \in A\_и\_x \notin B\}$ состоит из всех элементов множества А, которые не являются элементами множества B. Симметрическая разность двух множеств определяется как $A \Delta B = (A \div B) \cup (B \div A)$.

Часто все рассматриваемые множества являются подмножествами одного так называемого универсального множества E. В этом случае, вводится понятие дополнения множества $A \subseteq E$, а именно, это множество $\overline{A} = E \div A$. Из определения $A \cap \overline{A} = \emptyset$ и $A \cup \overline{A} = E$.

Свойства операций над множествами.

$A \cup A = A$ и $A \cap A = A$ - рефлексивность

$A \cup B = B \cup A$ - коммутативность

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ - дистрибутивность пересечения относительно объединения

$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$ - дистрибутивность объединения относительно пересечения

$\overline{A \cup B} = \overline{A} \cap \overline{B}$ - законы де Моргана

$\overline{A \cap B} = \overline{A} \cup \overline{B}$

Задачи. Доказать тождества. $A \div (B \cup C) = (A \div B) \cap (A \div C)$,

$A \div (B \cap C) = (A \div B) \cup (A \div C)$, $A \div B = A \div (A \cap B)$,

$(A \div B) \div C = (A \div C) \div (B \div C)$.

1.2. Конечные множества. Формула включений и исключений.

Множество А называется **конечным**, если оно содержит конечное число элементов. В этом случае, все его элементы можно занумеровать с помощью чисел начального отрезка натурального ряда *1,2,… n*. Число *n* называется числом элементов этого множества. Обозначаем число элементов множества $n=|A|$.

Для конечных множеств имеет место **формула включений и исключений**. Предварительно рассмотрим случай двух множеств A и B. Тогда $|A \cup B| = |A| + |B| - |A \cap B|$.

Действительно, пересчитаем сначала все элементы множества A, а затем все элементы множества B - получим величину $|A| + |B|$. При этом все элементы, принадлежащие их пересечению $A \cap B$, будут пересчитаны дважды. Поэтому вычтем это число из общей суммы и получим число $|A \cup B|$. Теперь все элементы множества $A \cup B$ пересчитаны по одному разу. Таким образом, $|A \cup B| = |A| + |B| - |A \cap B|$.

Аналогичным образом получим формулу включений и исключений для трех множеств

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B\} - |A \cap C| - |B \cap C| + |A \cap B \cap C|$.

Для доказательства вновь пересчитаем сначала все элементы множества A, получим число $|A|$, затем все элементы множества B, получим число $|B|$, а затем все элементы множества C, получим число $|C|$. Всего, таким образом, насчитаем $|A|+|B|+|C|$ элементов. При этом, элементы, принадлежащие взаимным по парным пересечениям $A \cap B$, $A \cap C$ и $B \cap C$ этих множеств будут пересчитаны дважды, а элементы, принадлежащие пересечению

$A \cap B \cap C$, всех этих множеств, были посчитаны по три раза каждый. Вычтем число попарно общих элементов из общего числа $|A|+|B|+|C|$ пересчитанных элементов. Заметим, что при этом элементы, принадлежащие пересечению трех множеств $A \cap B \cap C$, вычитались по три раза, поэтому восстановим их число - прибавим это число к сумме. В результате получим формулу

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B\} - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

.

В общем случае имеет место формула

Теорема 1.1.

$$|\bigcup_{i=1}^{n} A_i| =$$

$$\sum_{i=1}^{n} |A_i| - \sum_{i \neq j} |A_i \cap A_j| + \sum_{i \neq j \neq k} |A_i \cap A_j \cap A_k| - \ldots (-1)^n |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Данная формула полезна при подсчете количества элементов объединения пересекающихся множеств.

Рассмотрим следующие задачи:

1) Найти число всех натуральных чисел, не превосходящих 1000, которые делятся на 4 или на 5 или на 6.

2) Найти число всех натуральных чисел, не превосходящих 1000, которые не делятся ни на 4, ни на 5, ни на 6.

Для решения первой задачи введем множества:

A={n : n делится на 4}

B={n : n делится на 5}

C={n : n делится на 6}

Тогда $|A|=333$ (целая часть от деления числа 1000 на 3), $|B|=200$, $|C|=166$, $|A \cap B| = 50$, $|A \cap C| = 83$ (целая часть от деления числа 1000 на 12 – наибольший общий делитель чисел 4 и 6), $|B \cap C| = 33$, $|A \cap B \cap C| = 16$. По формуле включений и исключений получаем

$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B\} - |A \cap C| - |B \cap C| + |A \cap B \cap C|$ =333+200+166-50-83-33+.16=549. Ответ второй задачи равен 1000-549=451.

Задача. Найти число всех натуральных чисел, не превосходящих 1000, которые

1) делятся на 4, но не делятся на 6.
2) не делятся ни на 4, ни на 6.
3) Делятся на 4 или на 5, но не делятся на 7

1.3. Отношения. Функция.

Заданы множества $A_1, A_2, \ldots A_n$. **Кортежем**, составленным из элементов этих множеств, называется любая последовательность $<x_1, x_2, \ldots x_n>$, где $x_1 \in A_1$, $x_2 \in A_2, \ldots x_n \in A_n$.

Декартовым произведением множеств $A_1, A_2, \ldots A_n$ называется множество кортежей, составленных из элементов этих множеств $A_1 \times A_2 \times \ldots A_n = \{<x_1, x_2, \ldots x_n> : x_1 \in A_1, x_2 \in A_2, \ldots x_n \in A_n\}$.

Отношением между элементами множеств $A_1, A_2, \ldots A_n$ называется любое подмножество R их декартового произведения $R \subseteq A_1 \times A_2 \times \ldots A_n$. Если $<x_1, x_2, \ldots x_n> \in R$, то также пишем $R(x_1, x_2, \ldots x_n)$.

В современных реляционных базах данных отношениям соответствуют **файлы**, в которых кортежи $<x_1, x_2, \ldots x_n> \in R$, это **записи файла**, их элементы $x_1, x_2, \ldots x_n$ соответствуют **полям этих записей**.

Операции над отношениями. Отношения можно умножать и переставлять их элементы. Пусть R_1 – отношение между элементами множества $A \times A_1 \times A_2 \times \ldots A_n$, а R_2 – отношение между элементами множества $B_1 \times B_2 \times \ldots B_m \times A$. Тогда можно

рассмотреть **произведение (или композицию)** $R = R_2 \circ R_1$ этих отношений по ключу $x \in A$. По определению – это отношение

$R = \{< y_1, y_2 ... y_m, x_1, x_2, ... x_n >:$
$\exists x \in A (< y_1, y_2 ... y_m, x > \in R_2 \_ u \_ < x, x_1, x_2 ... x_n > \in R_1)\}$.

На языке файлов композиция означает, что создается новый файл, в котором любые две записи файлов $< y_1, y_2 ... y_m, x > \in R_2$ и $< x, x_1, x_2 ... x_n > \in R_1$, соответствующих отношениям R_1 и R_2, имеющие общий ключ $x \in A$, объединяются в новую запись $< y_1, y_2 ... y_m, x_1, x_2, ... x_n > \in R$.

Пусть теперь $\sigma = < i_1, i_2, ... i_n >$ - некоторая перестановка натуральных чисел $< 1,2....n >$, $R \subseteq A_1 \times A_2 \times ... A_n$ - некоторое отношение. Тогда можно определить отношение
$R^\sigma \subseteq A_{i_1} \times A_{i_2} \times ... A_{i_n} = \{< x_{i_1}, x_{i_2}, ... x_{i_n} >: < x_1, x_2, ... x_n > \in R\}$.

На языке файлов **перестановка отношения** означает, что создается новый файл, в котором поля всех записей переставлены в соответствии с перестановкой σ их номеров.

Если отношение $R \subseteq A_1 \times A_2$ - бинарное, то перестановка $\sigma = \{2,1\}$ определяет **обратное отношение**
$R^{-1} \subseteq A_2 \times A_1 = \{< x_2, x_1 >: < x_1, x_2 > \in R\}$.

Пусть заданы произвольные множества $A_1, A_2, ... A_n, Y$. Произвольное отношение F между элементами множеств $A_1, A_2, ... A_n$, Y называется **функцией** из множества $X = A_1 \times A_2 \times ... A_n$ в множество Y, обозначается $f : X \to Y$, если

1) $F \subseteq A_1 \times A_2 \times ... A_n \times Y$

2) из $\langle x_1, ... x_n, y \rangle \in F$ и $\langle x_1, ... x_n, y' \rangle \in F$ следует, что $y' = y$.

В этом случае также обозначают $y = F(x_1, ... x_n)$.

Множество всех кортежей $\langle x_1, ... x_n \rangle \in A_1 \times A_2 \times ... A_n$ таких, что $\langle x_1, ... x_n, y \rangle \in F$ хотя бы для одного у, называется **областью определения функции** F, множество всех таких у, что $\langle x_1, ... x_n, y \rangle \in F$ хотя бы для одного набора $\langle x_1, ... x_n \rangle$, называется **множеством значений функции** F.

Отметим, что множество определения функции F не обязательно совпадает с множеством всех кортежей $A_1 \times A_2 \times ... A_n$ (в этом случае функция называется частично определенной, или просто частичной), а множество всех значений не обязательно совпадает с множеством Y.

Функция $f : X \to Y$ называется **инъектив.ной**, если $f(x) \neq f(x')$ при $x \neq x'$. Функция f называется **сюръективной**, если область значений функции f совпадает со всем множеством Y. Функция f называется **биективной**, если она является инъективной и сюръективной (т.е. ее область значений совпадает со всем множеством Y), а ее область определения совпадает со всем множеством X. Про биективную функцию $f : X \to Y$ говорят, что она осуществляет **взаимнооднозначное** соответствие между элементами множеств X и Y.

1.4. Некоторые специальные бинарные отношения

1.4.1. Отношения эквивалентности.

Бинарное отношение между элементами множества A и B - это любое подмножество декартового произведения $R \subseteq A \times B$. В случае бинарного отношения R часто вместо $R(a,b)$ пишут aRb. Если $A=B$, то отношение $R \subseteq A \times A$ называется отношением на

множестве A. Бинарное отношение $a \sim b$, заданное на множестве A, называется **отношением эквивалентности**, если оно удовлетворяет следующим трем свойствам:
$a \sim a$ для всех a (рефлексивность)

Если $a \sim b$, то $b \sim a$ для всех a,b (симметричность)

Если $a \sim b$ и $b \sim c$, то $a \sim c$ для всех a, b, c (транзитивность)

Разбиением множества А – называется любое представление его в виде объединения непустых попарно непересекающихся подмножеств

$A = A_1 \cup A_2 \cup ... \cup A_n$, где $A_i \cap A_j = \emptyset$ при всех $i \neq j$.

Теорема 1.2. *Каждому отношению эквивалентности $a \sim b$ на множестве А соответствует разбиение этого множества, и обратно – каждому разбиению множества $A = A_1 \cup A_2 \cup ... \cup A_n$, где $A_i \cap A_j = \emptyset$ при всех $i \neq j$, соответствует некоторое отношение эквивалентности. Элементы такого разбиения называются классами эквивалентности.*

Доказательство. По произвольному отношению эквивалентности $a \sim b$ на множестве A построим разбиение $A = A_1 \cup A_2 \cup ... \cup A_n$ следующим образом. Выберем произвольный элемент a этого множества и отнесем все элементы, ему эквивалентные в первое подмножество разбиения – A_1. Если во множестве A остался хотя бы один элемент b, не попавший в это подмножество, создадим еще одно подмножество A_2, состоящее из всех элементов множества A, эквивалентных элементу b. Два подмножества A_1 и A_2 не пересекаются, так в противном случае существовал бы элемент c в этом пересечении, для которого было бы $c \sim a$ и $c \sim b$.

Отсюда по свойству транзитивности было бы $b \sim a$. А в этом случае элемент b должен принадлежать подмножеству A_1. Продолжая это рассуждение до тех пор, пока не исчерпаются все элементы множества A, получим представление множества A в виде объединения попарно непересекающихся подмножеств $A = A_1 \cup A_2 \cup ... \cup A_n$.

В обратную сторону, если нам задано представление множества A в виде объединения попарно непересекающихся подмножеств $A = A_1 \cup A_2 \cup ... \cup A_n$, то определим отношение эквивалентности: $a \sim b$ тогда и только тогда, когда a и b являются элементами одного и того же подмножества A_i из разбиения. Легко проверить, что такое отношение является рефлексивным, симметрическим и транзитивным.

Примеры отношений эквивалентности.

Рассмотрим отношение $n \sim m$ на множестве N всех натуральных чисел, где $n \sim m$ тогда и только тогда, когда число $n-m$ делится на число k. Здесь k – произвольное натуральное число. Доказать, что это отношение удовлетворяет трем свойствам отношения эквивалентности - рефлексивность, симметричность и транзитивность.

Задача. На какое число классов эквивалентности (в зависимости от k) разбивается множество всех натуральных чисел?

Другой пример отношения эквивалентности: пусть множество V состоит из всех направленных отрезков на плоскости (или в пространстве). Два отрезка $a, b \in V$ называются эквивалентным, если они параллельны, имеют одинаковую длину и одинаково направлены. Проверить, что это отношение удовлетворяет всем трем свойствам отношения эквивалентности. Класс таких эквивалентных отрезков называется **вектором**.

Определим отношение на множестве всех пар целых чисел $(p,q) \sim (s,r)$ тогда и только тогда $pr=qs$.

Задача. Доказать, что это отношение удовлетворяет трем свойствам отношения эквивалентности. Какая хорошо известная из школьной математики структура соответствует классам эквивалентности этого отношения?

1.4.2. Отношения частичного порядка, линейный порядок.

Бинарное отношение $a \leq b$, заданное на множестве A, называется **отношением частичного порядка**, если оно удовлетворяет следующим трем свойствам:

$a \leq a$ для всех a (рефлексивность)

Если $a \leq b$ и $b \leq a$, то $a=b$ для всех a,b (антисимметричность)

Если $a \leq b$ и $b \leq c$, то $a \leq c$ для всех a, b, c (транзитивность)

Множество, на котором задано отношение частичного порядка, называется **частично-упорядоченным.**

Примерами таких отношения являются отношения обычного неравенства $\leq$ на множествах всех натуральных, рациональных, действительных чисел.

Другой пример отношения частичного порядка – отношение быть подмножеством $A \subseteq B$ на множестве всех подмножеств $\{A : A \subseteq E\}$ произвольного множества E.

Задача. Проверить все эти три свойства для таких отношений.

Самое последнее из всех этих отношений $A \subseteq B$ отличается от первых трех тем, что не все подмножества множества E находятся в отношении $A \subseteq B$ или $B \subseteq A$, тогда как для любых двух чисел a и b выполнено $a \leq b$ или $b \leq a$. Таким образом, любые два числа сравнимы, тогда как для подмножеств это не верно.

Отношение частичного порядка на некотором множестве, для которого будет выполнено четвертое свойство: $a \leq b$ или $b \leq a$ для всех элементов a и b из этого множества, будет называться **линейным порядком**, а множество, на котором задан этот линейный порядок будет называться **линейно-упорядоченным**.

Задачи. Доказать тождества $(A \cap B) \times (C \cap D) = (A \times C) \cap (B \times D)$, $(A \cup B) \times C = (A \times C) \cup (B \times C)$, $(A \div B) \times C = (A \times C) \div (B \times C)$.

Пусть $A = \{< x_1, x_2, ...x_n > : x_i \in R\}$ - множество всех кортежей длины n, состоящих из вещественных чисел. Определим $< x_1, x_2, ...x_n > \prec\prec < x'_1, x'_2, ...x'_n >$ тогда и только тогда, когда $x_1 \leq x'_1, x_2 \leq x'_2, ...x_n \leq x'_n$. Доказать, что отношение $\prec$ является отношением частичного порядка, но оно не есть отношение линейного порядка. Привести подтверждающий пример.

Привести пример отношения на конечном множестве: 1) рефлексивного, симметричного, но не транзитивного; 2) рефлексивного, транзитивного , но не симметричного; 3) транзитивного и симметричного, но не рефлексивного.

Привести примеры функций , которые не являются инъективными, но являются сюрьективными, примеры сюрьективных, но не биективных функций и т.д.

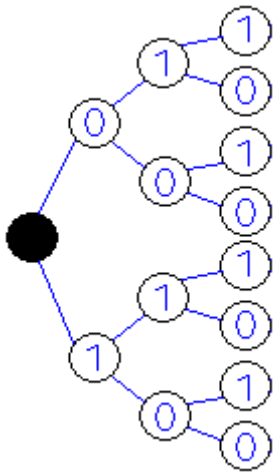
2. Комбинаторика.

2.1. Дерево двоичных последовательностей.

Последовательность, составленная из *0* и *1*, называется **двоичной** или **бинарной**. Числа *0* и *1* называются **битами**. Примеры таких последовательностей: *0000010110101110 10, 000000000000*, *1111111111*. Длиной последовательности называется общее число битов в ней.

Теорема 2.1. *Общее число всех двоичных последовательностей длины n равно* 2^n.

Доказательство основано на анализе представления множества всех таких последовательностей в виде дерева глубины *n*.



Все возможные последовательности (кортежи) длины *n*, состоящие из *0* и *1*, удобно наглядно представлять в виде так называемого **дерева**. Вершина дерева соответствует пустой последовательности (удобно рассматривать последовательность, не содержащую ни одно элемента), на следующем уровне находятся две вершины, соответствующие *0* и *1*, от каждой из них отходит по две вершины, также отмеченные *0* и *1*. Таким образом, получаем 4 вершины, соответствующие четырем последовательностям длины два: *00, 01, 10, 11*. Далее, от каждой из этих вершин откладываем еще по две вершины, каждая из которых помечена *0* и *1*. Получим 8 терминальных вершин, соответствующих восьми последовательностям: *000, 001, 010, 011, 100*, *101, 110, 111*. Продолжаем этот процесс расширения дерева *n* раз. На каждой стадии расширения число терминальных вершин увеличивается в два раза. На *n*-ой стадии получим 2^n терминальных вершин дерева, которые взаимно - однозначно соответствуют 2^n последовательностям длины *n*.

Побочным следствием этой теоремы является следующая теорема.

Теорема 2.2: *Число всех подмножеств множества, состоящего из n элементов равно* 2^n.

Для доказательства закодируем все подмножества множества *A* двоичными последовательностями длины *n*. Предварительно перенумеруем все элементы множества *A* в каком либо порядке и представим их в виде последовательности длины n без повторений, например, $A = \{a_1, a_2, ...a_n\}$. Пусть задано произвольное подмножество множества *A*. Мы сопоставим ему двоичную последовательность следующим образом: пройдем по всем элементам $\{a_1, a_2, ...a_n\}$ упорядоченного множества *A*, при этом пишем 1, если этот элемент находится в нашем подмножестве и 0, если не находится. Получим некоторую двоичную последовательность длины *n*, в которой число единиц равно числу элементов подмножества. Ясно, что по любой двоичной последовательности можно однозначно восстановить соответствующее ей подмножество. Например, последовательности из одних нулей соответствует пустое подмножество, последовательности, состоящих из одних единиц, соответствует все множество *A*. Как было доказано раньше, общее число таких последовательностей равно 2^n.

2.2. Кортежи.

Пусть E - конечное множество. **Кортеж** - это произвольная последовательность элементов из E (не обязательно всех). Если элементы множества E, перечисленные в кортеже, не повторяются, то кортеж называется **кортежем без повторений**. В противном случае, это **кортеж с повторениями**.

Пусть $E=\{1,2,3,4\}$. Пример кортежей без повторений - $<4,2>$, $<1>$, $<4,2,3,1>$. Пример кортежа с повторениями $<1,3,2,4,1>$. Ясно, что длина кортежа без повторений не может превышать число элементов множества E. Возможная длина кортежа с повторениями может быть произвольной. Отличие от множеств: из элементов одного множества можно составить несколько кортежей без повторений и бесконечное множество различных кортежей с повторениями. Например, из элементов множества $\{1,2,3\}$ можно составить 3 кортежа без повторений длины 1 это- $<1>$, $<2>$, $<3>$, 6 кортежей без повторений длины 2- это $<1,2>$, $<2,1>$, $<1,3>$, $<3,1>$, $<2,3>$, $<3,2>$ и 6 кортежей без повторений длины 3 – это $<1,2,3>$, $<1,3,2>$, $<2,1,3>$, $<2,3,1>$, $<3,1,2>$, $<3,2,1>$. Кортежей с повторениями - бесконечно много, например, $<1,1,1,...1>$, ….$<1,2,1,2,...1,2>$ и т.д.

Число всех кортежей с повторениями

Число всех кортежей с повторениями дается в следующей теореме.

Теорема 2.3 *Число всех кортежей с повторениями длины k, состоящих из элементов множества A равно* n^k *, где n – число элементов множества A.*

Доказательство основано на анализе дерева всех кортежей с повторениями глубины k.

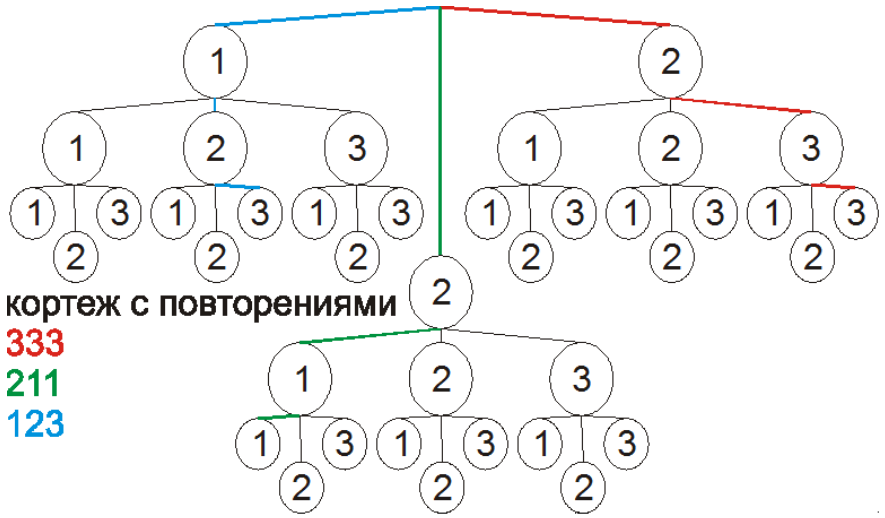


Рис.2.2. *Дерево кортежей с повторениями глубины 3.*

Во многих случаях приходится рассматривать кортежи $<x_1,x_2...x_k>$, элементы которых принадлежат различным множествам $E_1,E_2,...E_k$. В этом случае получаем обобщение предыдущей теоремы.

Теорема 2.4 *Число всех кортежей* $<x_1,x_2...x_k> \in E_1 \times E_2 \times ...E_k$ *длины k, состоящих из элементов* $x_1 \in E_1, x_2 \in E_2 ... x_k \in E_k$ *, равно произведению* $|E_1|\cdot|E_2|\cdot...|E_k|$ *, где* $|E_i|$ *– число элементов множества* E_i *,* $i = 1,2,...k$ *. Теорема верна также в случае, когда каждое множество* E_i *зависит от элементов* $x_1,x_2...x_{i-1}$ *кортежа.*

Доказательство также основано на подсчете числа терминальных вершин в дереве всех таких кортежей.

Число всех кортежей без повторений

Число всех кортежей без повторений дается в следующей теореме.

Теорема 2.5. *Число всех кортежей без повторений длины k, состоящих из элементов n-элементного множества A, равно* $A_n^k = n(n-1)....(n-k+1)$, где $k \le n$.

Доказательство основано на анализе дерева всех кортежей без повторений глубины k.

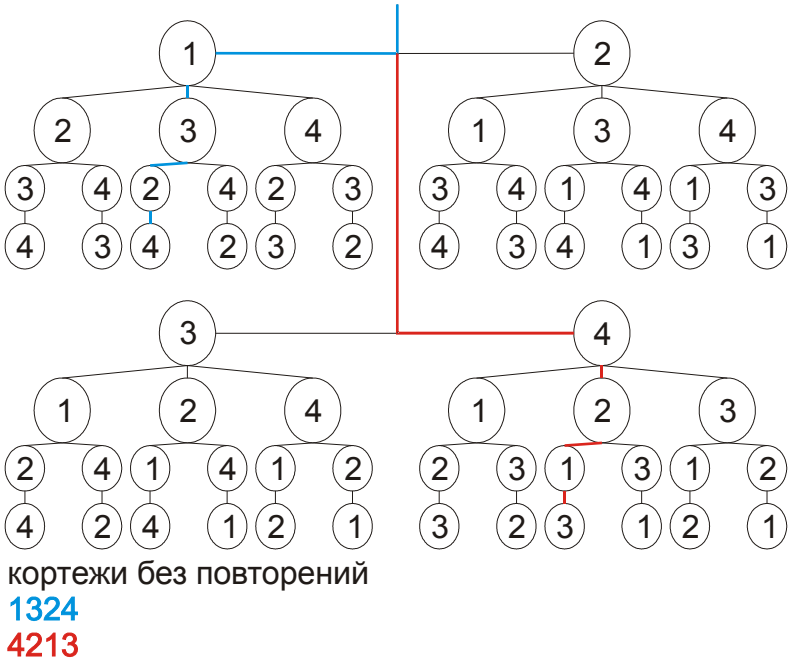


Рис.2.3. *Дерево кортежей без повторений глубины 4.*

Перестановкой элементов конечного множества называется кортеж без повторений, составленный из всех элементов этого множества.

Следствие. *Число всех перестановок n- элементного множества равно* $n! = 1 \cdot 2 \cdot ...n$.

Действительно, при $k=n$ получаем $A_n^k = n(n-1)....(n-n+1) = n!$.

Задача. Найти число всех слов длины 5, которые можно составить из 33 различных букв, если

1) буквы в слове могут повторяться.
2) буквы не могут повторяться
3) соседние буквы разные

Задача. Найти число всех трехцветных флагов, которые можно составить из 7 цветов, если

1) все цвета на флаге – разные,
2) соседние цвета разные.

Задача. Сколькими способами можно раскрасить 7 цветами квадрат 4×4, если

1) все клетки должны быть раскрашены в разные цвета,
2) клетки, имеющие общую сторону, должны быть раскрашены в разные цвета.

Задача. Сколькими способами можно рассадить

1) 7 человек на скамейке.
2) 7 человек на скамейке так, чтобы два друга оказались сидящими рядом.
3) 7 человек на скамейке так, чтобы два врага не оказались сидящими рядом
4) 7 человек за круглым столом (важен только порядок сидящих).

Задача. Сколькими способами можно расставить на шахматной доске (8×8) одного ферзя, одного офицера и одну пешку (цвет полей не учитывать).

Задача. Сколькими способами можно расставить на шахматной доске (8×8) одного ферзя и одну пешку, если их разрешается ставить на поля

1) одного цвета
2) разных цветов (неважно каких).

Задача. Сколькими способами можно расставить на шахматной доске (8×8) двух слонов так, чтобы они не били друг друга. Тот же вопрос для трех слонов. Цвет полей не учитывать.

2.3. Число всех *k*-элементных подмножеств *n*-элементного множества

Число всех подмножеств заданного размера дается в следующей теореме.

Теорема 2.6. *Число всех k-элементных подмножеств n-элементного множества равно*

$C_n^k = \frac{A_n^k}{k!} = \frac{n(n-1)(n-2)...(n-k+1)}{k!}$, где $k \le n$.

Доказательство. Предварительно перечислим все кортежи длины *k*, составленные из элементов *n*-элементного множества. Как было доказано ранее в теореме 2.5, всего имеется $A_n^k = n(n-1)....(n-k+1)$ таких кортежей. Сгруппируем все эти кортежи так, чтобы в одну группу входили бы все кортежи длины *k*, составленные из элементов одного и того же *k*-элементного подмножества. По следствию из теоремы 2.5, в каждой группе имеется *k!* кортежей – это все перестановки элементов группы.

Итак, множество всех кортежей разбивается на группы по *k!* элементов. Каждая такая группа кортежей соответствует одному и тому же подмножеству. Ясно, что число таких групп может быть получено путем деления общего числа всех кортежей на размер группы. Таким образом, мы доказали, что число всех *k*-элементных подмножеств *n*- элементного множества равно

$$\frac{A_n^k}{k!} = \frac{n(n-1)(n-2)...(n-k+1)}{k!}.$$

Другое представление этой формулы $C_n^k = \frac{n!}{(n-k)!k!}$ получается путем умножения обоих частей выражения $\frac{n(n-1)(n-2)...(n-k+1)}{k!}$ на *(n-k)!*.

Используя предыдущую теорему, легко подсчитать число всех двоичных последовательностей, имеющих заданное число единиц и нулей.

Теорема 2.7. *Число всех двоичных последовательностей длины n, содержащих k единиц и n-k нулей равно*

$$C_n^k = \frac{n(n-1)(n-2)...(n-k+1)}{k!}$$

Для доказательства заметим, что общее число всех двоичных последовательностей длины *n*, содержащих ровно *k* единиц, равно числу всех подмножеств, состоящих из *k* элементов *n* элементного множества. Эти подмножества составляются из номеров тех позиций в двоичной последовательности, на которых стоят единицы. Как мы выяснили ранее, это число равно C_n^k. Теорема доказана.

Свойства биномиальных коэффициентов. Приведем некоторые свойства чисел C_n^k, которые называются **биномиальными коэффициентами**. Прежде всего заметим, что по определению $C_n^0 = 1$ и $C_n^n = 1$.

Теорема 2.8. $C_n^k = C_n^{n-k}$ *при* $k \le n$.

Эта формула получается с помощью простой перестановки сомножителей $C_n^k = \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!k!} = C_n^{n-k}$.

Теорема 2.9. $C_n^k = C_{n-1}^k + C_{n-1}^{k-1}$ *при* $k \le n$.

Доказательство основано на приведении к общему знаменателю суммы

$$C_{n-1}^k + C_{n-1}^{k-1} = \frac{(n-1)!}{k!(n-1-k)!} + \frac{(n-1)!}{(k-1)!(n-k)!} =$$

$$\frac{(n-1)!(n-k)+(n-1)!k}{k!(n-k)!} = \frac{n!}{k!(n-k)!} = C_n^k$$

Теорема 2.10. $C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^k + \ldots C_n^n = 2^n$**.**

Доказательство. Каждый из биномиальных коэффициентов C_n^k равен числу всех *k*-элементных подмножеств n элементного множества. Как было доказано ранее, общее число всех подмножеств *n* элементного множества равно 2^n. Поэтому и сумма всех биномиальных коэффициентов также равна 2^n.

Треугольник Паскаля. Предыдущая теорема 2.9 дает идею простого алгоритма для вычисления биномиальных коэффициентов – **треугольник Паскаля**.

$$C_0^0$$

$$C_1^0 \quad C_1^1$$

$$C_2^0 \quad C_2^1 \quad C_2^2$$

$$C_3^0 \quad C_3^1 \quad C_3^2 \quad C_3^3$$

....

В треугольнике Паскаля каждое число, расположенное внутри треугольника, равно сумме двух вышестоящих над ним чисел. Все числа по краям треугольника равны 1. Треугольник Паскаля также можно переписать в виде

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

.... …

Таким образом, удобно вычислять все биномиальные коэффициенты сразу. Вычисление всех биномиальных коэффициентов одновременно занимает примерно столько же времени, как и вычисление только одного биномиального коэффициента независимо от других. Такая идея вычисления положена в основу так называемого **метода динамического программирования**, который широко применяется на практике.

Бином Ньютона Числа C_n^k служат коэффициентами при степенях переменных *a* и *b* при представлении степени $(a+b)^n$ в виде многочлена от *a* и *b*.

Теорема 2.11. $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ *для всех n, a и b* .

Докажем это тождество с помощью **математической индукции по** *n*. При *n=1* тождество очевидно. Допустим, что оно верно при *n-1*, т.е. имеет место

$(a+b)^{n-1} = \sum_{k=0}^{n-1} C_{n-1}^{k} a^{n-k-1} b^{k}$. Умножим обе части этого тождества на *(a+b)*. Получим

$$(a+b)^{n} = \sum_{k=0}^{n-1} C_{n-1}^{k} a^{n-k-1} b^{k} (a+b) =$$

$$\sum_{k=0}^{n-1} C_{n-1}^{k} a^{n-k} b^{k} + \sum_{k=0}^{n-1} C_{n-1}^{k} a^{n-(k+1)} b^{k+1} =$$

$$\sum_{k=0}^{n-1} C_{n-1}^{k} a^{n-k} b^{k} + \sum_{k'=1}^{n} C_{n-1}^{k'-1} a^{n-k'} b^{k'} =$$

$$\sum_{k=1}^{n-1} (C_{n-1}^{k} + C_{n-1}^{k-1}) a^{n-k} b^{k} + C_{n-1}^{n-1} b^{n} + C_{n-1}^{0} a^{n} =$$

$$\sum_{k=1}^{n-1} C_{n}^{k} a^{n-k} b^{k} + C_{n}^{n} b^{n} + C_{n}^{0} a^{n} = \sum_{k=0}^{n} C_{n}^{k} a^{n-k} b^{k}.$$

Здесь во второй сумме второй строки мы делали замену *k'=k+1*, а впервой сумме третьей строки воспользовались теоремой 2.9. Мы сделали шаг индукции – перешли от тождества для *n-1* к тождеству для *n.* Следовательно, утверждение теоремы выполнено.

Следствие. *Имеют место следующие соотношения* $2^{n} = \sum_{k=0}^{n} C_{n}^{k}$ и

$\sum_{k=0}^{n} (-1)^{k} C_{n}^{k} = 0.$

Первое тождество получается из бинома Ньютона при *a=b=1*, второе тождество получается из бинома Ньютона при *a=1, b=-1.*

Ранее мы доказали первое тождество исходя из комбинаторных соображений.

Задача. Найти коэффициент при x^{10} в разложении выражения $(1+x)^{10}$ по степеням *x*.

Выписать в виде многочлена $(a+b)^{10}$.

2.4. Число всех разбиений конечного множества на фиксированное число подмножеств заданного размера.

Задача о числе всех *k*-элементных подмножеств множеств, состоящего из *n* элементов, может рассматриваться как задача о числе всех представлений *n* элементного множества *A* в виде объединения двух непересекающихся подмножеств $A = B \cup C$, где $|B|=k$, $|C|=n-k$. Ранее было показано, что число таких представлений равно C_{n}^{k}. Рассмотрим обобщение этой задачи – задачу нахождения числа всех представлений *n* элементного множества *A* в виде объединения r попарно непересекающихся подмножеств заданных размеров $A = A_1 \cup A_2 \cup \ldots A_r$, где $|A_1|=k_1$, $|A_2|=k_2, \ldots |A_r|=k_r$,.

Теорема 2.12. *Число всех представлений n элементного множества A в виде объединения r попарно непересекающихся подмножеств* $A = A_1 \cup A_2 \cup \ldots A_r$ *заданных размеров* $k_1, k_2, \ldots k_r$, *где* $k_1 + k_2 + \ldots k_r = n$, $|A_1|=k_1$, $|A_2|=k_2, \ldots, |A_r|=k_r$, *равно*

$$C_{n}^{k_1, k, \ldots k_r} = \frac{n!}{k_1! k_2! \ldots k_r!}.$$

Числа всех таких представлений можно подсчитать следующим образом. Сначала подсчитаем число способов выбора первого подмножества, состоящего из k_1 элементов. Как ранее было показано, это число равно $C_n^{k_1} = \frac{n!}{(n-k_1)!k_1!}$. Для каждого варианта выбора такого подмножества из оставшихся $n-k_1$ элементов можно выбрать второе подмножество, состоящее из k_2 элементов. Это можно сделать $C_{n-k_1}^{k_2} = = \frac{(n-k_1)!}{(n-k_1-k_2)!k_2!}$ способами. Продолжая выбор таким способом r раз, получим формулу для общего числа таких разбиений в виде произведения

$$C_n^{k_1,k,\ldots k_r} = \frac{n!}{(n-k_1)!k_1!}\frac{(n-k_1)!}{(n-k_1-k_2)!k_2!}\cdots\frac{(n-k_1-\ldots k_{r-1})!}{(n-k_1-\ldots k_r)!k_r!} =$$

$$= \frac{n!}{k_1!k_2!\ldots k_r!}.$$

Теорема доказана.

Частный случай этой задачи – задача о числе всех слов длины n с заданным составом букв. Надо найти число всех различных слов, каждое которых содержит k_1-раз первую букву, k_2 – раз вторую букву…, k_r-раз r-тую букву, где $k_1 + k_2 + \ldots + k_r = n$. Для подсчета всех таких слов, занумеруем позиции всех букв в слове натуральными числами *1,2,…n*. После этого, выберем подмножество из k_1 позиций, на которые мы поставим первую букву, подмножество из k_2 позиций, на которые мы поставим вторую букву, и т.д. подмножество из k_r позиций, на которые мы поставим r-тую букву. Таким образом, число всех таких слов равно числу всех подмножеств заданного размера, т.е. числу

$$C_n^{k_1,k,\ldots k_r} = \frac{n!}{k_1!k_2!\ldots k_r!}.$$

Задача. Сколькими способами можно расставить 2 ферзя, 4 пешки на шахматной доске размера 8×8?

Задача. Сколько различных слов можно составить из букв слова ***метаматематика, балабаново, перерва.***

Задача. Сколькими способами можно собрать ожерелье из 20 красных, 15 синих и 5 белых бусинок.

Задача. Сколькими способами можно расставить на шахматной доске (8×8) клеток 2-х слонов, 3-х ферзей и 4-х пешек. Тот же вопрос, но слоны и пешки ставятся только на верхней половине доски.

2.5. Разложение неразличимых предметов по ящикам

Рассмотрим задачу разложения неразличимых предметов по ячейкам. Эта задача эквивалентна нахождению общего числа неотрицательных целых решений уравнения

$$x_1 + x_2 + \ldots + x_k = n.$$

Теорема 2.13. *Общее число различных разложений n неразличимых элементов по k ящикам равно* $C_{n+k-1}^{k-1} = C_{n+k-1}^{n-1}$.

Для того, чтобы подсчитать число всех вариантов разложения n предметов по k ящикам закодируем все варианты разложения с помощью каких-либо объектов, общее число которых мы уже

научились подсчитывать ранее. Сопоставим каждому варианту разложения двоичную последовательность, состоящую из наборов единиц и их разделителей. В качестве разделителя будем использовать *0*. Число единиц в *k*-ом наборе будет равно числу предметов, попавших в ящик соответствующий этому набору. Разделители ставятся только между последовательностями единиц, представляющими содержимое одного ящика, поэтому их число равно *k-1*. Суммарное число единиц в нашем коде равно *n*. Таким образом, длина всего кода для любого разложения *n* предметов по *k* ящикам равно *n+k-1*.

0	**5**	**3**	**2**

Рис 2.3. *Пример варианта разложения 10 предметов по 4-м ящикам*.

Например, разложению, приведенному на рисунке, соответствует код 0111110111011. Первый нуль означает, что в самом левом ящике предметы отсутствуют. Легко видеть, что по коду можно однозначно восстановить разложение предметов по ящикам. Иными словами, существует взаимно - однозначное соответствие между всеми такими кодами, состоящими из *k-1* нулей и *n* единиц, и всеми разложениями n предметов по *k* ящикам. Число всех двоичных последовательностей, состоящих из *k-1* нулей и *n* единиц, равно .

Следствие. *Общее число неотрицательных целочисленных решений уравнения* $x_1 + x_2 + \ldots x_k = n$ *равно* .

Задача. Сколькими способами можно купить 10 пирожных 4-х сортов.

Задача.. Крупа продается в пакетах по 1 кг. Сколькими способами можно купить 30 кг.

1) гречки, риса, пшена, перловки.
2) гречки не менее 3кг., риса не менее 2кг., пшена, перловки - без ограничений.
3) гречки не менее 3кг., риса не более 2кг., пшена, перловки - без ограничений

Задача. Найти число всех решений уравнения $x_1 + x_2 + \ldots + x_r = n$, удовлетворяющих условиям $x_1 \geq k_1, \ldots x_r \geq k_r$.

2.6. Комбинаторная вероятность

Определим **комбинаторную вероятность** события как отношение числа комбинаций объектов, при которых реализуется это событие, к общему числу всех возможных комбинаций объектов.

Например, рассмотрим события, заключающиеся в том, что при 10 подбрасываниях симметричной монеты герб (обозначим его единицей, а решку - нулем) выпал

1) точно 3 раза
2) не более чем 3 раза
3) не менее чем в 3 раза
4) от 3 до 5 раз.

Задача состоит в том, чтобы найти вероятности этих событий.

Каждая серия бросаний симметричной монеты представляется в виде комбинации объектов - нулей и единиц (единица соответствует выпадению герба, ноль – выпадению решки). В первой задаче - это последовательность, содержащая 10 нулей или единиц. Как мы выяснили ранее, общее число всех таких

двоичных последовательностей равно $2^{10}=1024$. В первой задаче, событие состоит из всех последовательностей длины 10, содержащих ровно 3 единицы и 7 нулей. Общее число всех двоичных последовательностей, содержащих ровно 3 единицы (герба) равно числу всех подмножеств из трех элементов 10-ти элементного множества. Эти подмножества составляются из номеров тех бросаний, при которых выпала 1. Как мы выяснили ранее, это число равно $C_{10}^3 = \frac{10 \cdot 9 \cdot 8}{1 \cdot 2 \cdot 3} = 120$. Поэтому искомая вероятность равна $\frac{120}{1024} = \frac{15}{128}$. Аналогичным образом, вероятность второго события равна $\frac{C_{10}^0 + C_{10}^1 + C_{10}^2 + C_{10}^3}{2^{10}}$.

Задача. Вычислить вероятности остальных событий.

Задача. Вычислить вероятность того, что при 10 подбрасываниях симметричной монеты

1) гербов выпало больше чем решек.

2) число гербов равно числу решек.

Задача. Симметричный кубик, на гранях которого написаны цифры от 1 до 6, подбросили один раз. Какова вероятность того, что наверху выпало четное (нечетное) число. Какова вероятность того, что при одновременном подбрасывании двух таких кубиков наверху оказались числа, которые: 1) равны друг другу; 2) сумма которых равна 5 (1, 2, 3, 12).

Задача. Найти вероятность события, состоящего в том, что при случайной расстановке 2-х ферзей, 4-х пешек и 3-х офицеров на шахматной доске размера 8×8 все они оказались на верхней половине доски.

Задача. Найти вероятность события, состоящего в том, что при случайной расстановке 2-х ферзей, 3-х пешек на шахматной доске размера 8×8 клеток

1) все они оказались на одной горизонтальной полосе.

2) все эти фигуры не стоят на одной горизонтальной полосе

3) все фигуры стоят на крайних полосах доски.

4) ферзи и пешки оказались на разных половинах доски (ферзи на верхней, пешки на нижней).

5) ферзи и пешки оказались на разных половинах доски (не важно – на какой половине).

6) один ферзь и две пешки оказались на верхней половине, а остальные фигуры – оказались на нижней половине.

Задача. Из 15 человек случайным образом выбрали троих. Какова вероятность того, что

1) я не попал в их число

2) я попал в их число

3) я и мой друг попали в их число

4) или я или мой друг попали в их число

Задача. 7 человек случайным образом расселись на скамейке. Какова вероятность того, что

1) я оказался с краю,

2) я и мой друг – оба оказались по краям скамейки,

3) я оказался точно в середине,

4) я и мой друг оказались рядом,

5) я и мой друг сидим через одного человека

Задача.. Случайным образом выбрали r неотрицательных целых чисел, сумма которых равна n. Какова вероятность того, что

1) каждое число оказалось больше нуля.
2) все числа не меньше 1.
3) Сумма первых двух чисел равна числу $m<n$.

3. Функции алгебры логики.

3.1. Функции и и формулы

Рассмотрим функции, аргументы и значения которых принимают два значения *0* и *1*. Эти значения называются **битами**, а функции называются **функциями алгебры логики** или **булевыми функциями**. Обозначим P_2 - класс всех функций алгебры логики. Пусть $E=\{0,1\}$. Мы рассмотрим операции над элементами E, которые одновременно являются арифметическими операциями над битами, а также логическими операциями над истинностными значениями **0 – ложь(Л)**, **1 - истина(И)**.

Каждая функция алгебры логики может быть задана своей таблицей значений, которая в логической интерпретации, также называется **таблицей истинности**. Предварительно введем некоторые стандартные функции алгебры логики: отрицание, дизъюнкция, конъюнкция, импликация, эквивалентность, сложение по модулю 2, штрих Шеффера, стрелка Пирса.

Всего имеется 4 функции алгебры логики от одной переменной – это две функции тождественно равные 0 и 1, тождественная функция $f(x)=x$ и отрицание $f(x)=\bar{x}$. Отрицание соответствует частице **не** и ее пониманию в математической логике.

Все функции алгебры логики от одной переменной представлены в следующей таблице истинности

x	0	1	x	$\bar{x}$
0	0	1	0	1
1	0	1	1	0

Значения основных функций алгебры логики от двух переменных приведены в следующей таблице истинности.

x_1 x_2	$x_1 \vee x_2$	$x_1 \wedge x_2$	$x_1 \to x_2$	$x_1 \leftrightarrow x_2$	$x_1 + x_2$	$x \mid x_2$	$x_1 \downarrow x_2$
0 0	0	0	1	1	0	1	1
0 1	1	0	1	0	1	1	0
1 0	1	0	0	0	1	1	0
1 1	1	1	1	1	0	0	0

Функция $x_1 \vee x_2$ называется **дизъюнкцией**. В логической интерпретации эта функция соответствует союзу **или** и его традиционному пониманию в математической логике.

По определению $x_1 \vee x_2 = \max\{x_1, x_2\}$.

Функция $x_1 \wedge x_2$ называется **конъюнкцией**. В логической интерпретации эта функция соответствует союзу **и**, который соединяет два истинностных значения.

По определению $x_1 \wedge x_2 = \min\{x_1, x_2\}$. Мы будем также писать $x_1 \cdot x_2 = x_1 \wedge x_2$.

Функция $x_1 \to x_2$ называется **импликацией**. Эта функция соответствует логическому смыслу выражения «**если … то …**» как он обычно используется в математических рассуждениях.

Функция $x_1 + x_2$ называется сложением по модулю 2. Оно отличается от обычного сложения только тем, что *1+1=0*. Часто пишут $x \oplus y$, для того, чтобы отличить сложение битов от обычного сложения чисел.

Функция $x \mid x_2$ называется штрихом Шеффера. Функция $x \downarrow x_2$ называется стрелкой Пирса.

В таблице приведены не все функции от двух переменных, а только те, которые имеют ясный логический смысл. Общее число функций алгебры логики от двух переменных равно числу всех столбцов их значений, которые имеют высоту 4. Всего таких столбцов - 2^4=16.

Выражения, составленные из переменных, соединенных знаками элементарных логических функций, будут называться формулами. Приведем точное определение формулы в индуктивной форме (как это принято в математической логике и при определении языков программирования).

1. Выражения $\overline{x}$, $x_1 \vee x_2$, $x_1 \wedge x_2$, $x_1 \to x_2$, $x_1 \leftrightarrow x_2$, $x_1 \mid x_2$, $x_1 \downarrow x_2$ называются формулами;

2. Если F_1, F_1, F_2 - формулы, то выражения $\overline{F}$, $(F_1 \vee F_2)$, $(F_1 \wedge F_2)$, $(F_1 \to F_2)$, $(F_1 \to F_2)$, $(F_1 \leftrightarrow F_2)$, $(F_1 \mid F_2)$, $(F_1 \downarrow F_2)$ - также являются формулами.

Примеры формул - $\overline{(x_1 \vee x_2)}$, $\overline{(x_1 \vee (x_1 \wedge x_2))}$.

Мы будем использовать правила опускания скобок там, где это действие не нарушает смысла формулы.

Свойства сложения по модулю 2. Кодирование с секретным ,ключом.

Сложение по модулю 2 обладает свойством *x+x=0* для всех *x*. По другому, это свойство можно записать *(y+x)+x=y* для всех битов

x,y. На этом свойстве основана идея кодирования с секретным ключом.

Пусть задана достаточно длинная последовательность битов $\alpha_1\alpha_2...\alpha_n$ - секретный ключ. Этот ключ – секретный, его знают только отправитель сообщения и его получатель. Отправитель хочет передать исходное сообщение $x_1x_2...x_n$, состоящее из двоичных битов, по публичному каналу связи. Все сообщения, передаваемые по этому каналу, может читать «противник». Для того, чтобы противник не разгадал это сообщение его кодируют. Это можно сделать, переходя от сообщения $x_1x_2...x_n$ к сообщению $x_1+\alpha_1, x_2+\alpha_2...x_n+\alpha_n$. Получатель закодированного сообщения легко может декодировать его прибавляя секретный бит еще раз $(x_1+\alpha_1)+\alpha_1, (x_2+\alpha_2)+\alpha_2...(x_n+\alpha_n)+\alpha_n = x_1x_2...x_n$.

Для того, чтобы противник не разгадал секретную строку битов $\alpha_1\alpha_2...\alpha_n$, ее нужно выбрать максимально сложной – не содержащей закономерностей, например, получить в результате подбрасывания симметричной монеты. Можно также генерировать такую последовательность с помощью датчика псевдослучайных чисел. Правда алгоритм такого датчика надо держать в секрете от противника.

Прямой способ перебора всех последовательностей $\alpha_1\alpha_2...\alpha_n$ длины *n* противником вычислительно не эффективен, так как число таких последовательностей длины *n* равно 2^n. На этой идее основан способ **кодирования с секретным ключом**.

Число функций алгебры логики.

Каждая функция алгебры логики представляет собой конечный объект, так как однозначно задается таблицей своих значений. Эта таблица содержит 2^n строк и *n+1* столбцов.

Так как произвольная функция алгебры логики может содержать неограниченное число переменных, общее число всех функций алгебры логики бесконечно.

Число всех функций алгебры логики от *n* переменных дает следующая теорема.

Теорема 3.1. *Число всех функций алгебры логики от n переменных равно* $2^m = 2^{2^n}$, *где* $m=2^n$.

Мы узнаем число таких функций, если подсчитаем число всех таблиц их задающих. Так как первые *n* столбцов у всех таблиц одни и те же, эти таблицы различаются только в последнем столбце их значений, число всех функций от *n* переменных равно числу всех таких столбцов. Каждый такой столбец имеет высоту, равную числу всех всевозможных комбинаций значений *n* переменных. Число таких комбинаций равно $m=2^n$, а число всех столбцов длины *m* равно 2^m.

Например, число всех функций от 3-х переменных равно $2^8=256$. Число таких функций чрезвычайно быстро растет с ростом *n*. Благодаря этому, возрастает число возможных зависимостей, которые можно представить с помощью функций алгебры логики.

Тождества в алгебре логики.

Тождество – это равенство двух выражений (формул алгебры логики), верное при всех значениях входящих в них переменных. Тождества между функциями алгебры логики выражают законы

математической логики. Следующие ниже тождества необходимо поверить с помощью таблиц истинности.

$\overline{x_1 \vee x_2} = \overline{x_1} \wedge \overline{x_2}$ **- законы де Моргана**

$\overline{x_1 \wedge x_2} = \overline{x_1} \vee \overline{x_2}$

$x_1 \wedge (x_2 \vee x_3) = (x_1 \wedge x_2) \vee (x_1 \wedge x_3)$ **- дистрибутивность конъюнкции относительно дизъюнкции**

$x_1 \vee (x_2 \wedge x_3) = (x_1 \vee x_2) \wedge (x_1 \vee x_3)$ **- дистрибутивность дизъюнкции относительно конъюнкции**

Другие свойства

$x_1 \to x_2 = \overline{x_1} \vee x_2$

$x \vee x = x$, $x \wedge x = x$

$x \vee 1 = 1$, $x \wedge 1 = x$

$x \vee 0 = x$, $x \wedge 0 = 0$

$\overline{\overline{x}} = x$ **- закон двойного отрицания**

$x \vee \overline{x} = 1$ **- закон исключенного третьего**

$x \wedge \overline{x} = 0$ **- закон противоречия**

$x_1 + x_2 = \overline{x_1 \leftrightarrow x_2} = (\overline{x_1} \wedge x_2) \vee (x_1 \wedge \overline{x_2})$ …**- исключающее «или»**

$x_1 \leftrightarrow x_2 = x_1 \cdot x_2 \vee \overline{x_1} \cdot \overline{x_2}$

$x_1 \mid x_2 = \overline{x_1 \wedge x_2}$

$x_1 \downarrow x_2 = \overline{x_1 \vee x_2}$

$x_1 \cdot (x_2 + x_3) = x_1 \cdot x_2 + x_1 \cdot x_3$.

Приведенные примеры показывают, что две различные формулы могут задавать одну и ту же функцию алгебры логики. В частности, две формулы, задающие одну и ту же функцию, будут иметь одну и туже таблицу истинности. Напомним, что существует взаимнооднозначное соотношение между функциями алгебры логики и таблицами истинности.

Задача. Проверить все приведенные выше тождества с помощью таблиц истинности.

Используя тождество $x_1 \downarrow x_2 = \overline{x_1 \vee x_2}$, можно выразить (при $x = x_2 = x_1$) отрицание $\overline{x} = x \downarrow x$. Переходя к двойному отрицанию, получаем $x_1 \vee x_2 = \overline{x_1 \downarrow x_2} = (x_1 \downarrow x_2) \downarrow (x_1 \downarrow x_2)$. Таким образом, отрицание и дизъюнкция выражаются через одну функцию – стрелку Пирса.

Задача. Выразить конъюнкцию и импликацию через стрелку Пирса.

Задача. Выразить отрицание, конъюнкцию, дизъюнкцию и стрелку Пирса через штрих Шеффера $x_1 \mid x_2$.

3.2. Восстановление формулы по таблице истинности. СДНФ.

Покажем, как по таблице истинности создать формулу, построенную с помощью переменных, их отрицаний и

соединенных знаками конъюнкции и дизъюнкции, для которой эта таблица является таблицей истинности.

Приведем пример таблицы истинности некоторой функции.

X_1	X_2	X_3	$F(X_1, X_2, X_3)$
0	0	0	1
0	0	1	1
0	1	0	0
0	1	1	0
1	0	0	1
1	0	1	0
1	1	0	1
1	1	1	0

Напомним, что $x_1 \cdot x_2 = x_1 \wedge x_2$. Изучим свойства произведений переменных. Для каждой строки таблицы истинности существует только одно произведение переменных и их отрицаний, которое равно 1 на этой строке и равно 0 на любой другой строке. Это произведение называется **элементарной конъюнкцией** и строится следующим образом – если значение переменной в строке равно 1, то пишем в произведении эту переменную, если значение равно 0, то пишем ее отрицание. Перемножим все переменные или их отрицания – получим элементарную конъюнкцию.

Например, 1, 2, 5 и 7 строкам соответствуют элементарные конъюнкции (произведения):

$\overline{x_1} \cdot \overline{x_2} \cdot \overline{x_3}$ - значение равно 1 только на первой строке переменных 000

$\overline{x_1} \cdot \overline{x_2} \cdot x_3$ - значение равно 1 только на второй строке переменных 001

$x_1 \cdot \overline{x_2} \cdot \overline{x_3}$ - значение равно 1 только на пятой строке переменных 100

$x_1 \cdot x_2 \cdot \overline{x_3}$ - значение равно 1 только на седьмой строке переменных 110

Составим из этих элементарных конъюнкций дизъюнкцию.

Например, для приведенного примера получим дизъюнкцию

$\overline{x_1} \cdot \overline{x_2} \cdot \overline{x_3} \vee \overline{x_1} \cdot \overline{x_2} \cdot x_3 \vee x_1 \cdot \overline{x_2} \cdot \overline{x_3} \vee x_1 \cdot \overline{x_2} \cdot \overline{x_3}$

Такую дизъюнкцию назовем **СДНФ** (совершенная дизъюнктивная нормальная форма)..

Для любой строки таблицы, если значение функции на ней равно 1, то в СДНФ имеется соответствующая ей элементарная конъюнкция. Эта элементарная конъюнкция равна 1 и поэтому вся СДНФ принимает значение 1 на этой строке переменных. Если значение функции на строке равно 0, то в СДНФ нет соответствующей этой строке элементарной конъюнкции, а все элементарные конъюнкции СДНФ равны 0 на этой строке (так как ей не соответствуют), поэтому и вся СДНФ равно 0 на этой строке. Таким образом, значения СДНФ на всех строках переменных равны значениям функции, заданной с помощью таблицы.

В некоторых случаях полученную формулу можно упростить. Например, законом дистрибутивности конъюнкции относительно дизъюнкции

$$\overline{x_1}\cdot\overline{x_2}\cdot\overline{x_3}\vee\ \overline{x_1}\cdot\overline{x_2}\cdot x_3\vee\ x_1\cdot\overline{x_2}\cdot\overline{x_3}\vee\ x_1\cdot\overline{x_2}\cdot\overline{x_3}=\overline{x_1}\cdot\overline{x_2}(\overline{x_3}\vee\ x_3)\vee$$
$$x_1\cdot\overline{x_2}\cdot\overline{x_3}\vee\ x_1\cdot\overline{x_2}\cdot\overline{x_3}=\overline{x_1}\cdot\overline{x_2}\vee\ x_1\cdot\overline{x_2}\cdot\overline{x_3}\vee\ x_1\cdot\overline{x_2}\cdot\overline{x_3}\ .$$

3.3. Полные системы функций алгебры логики

Приведенный выше способ построения СДНФ по таблице показывает, что любую функцию алгебры логики (которую всегда можно задать с помощью таблицы) можно выразить через дизъюнкцию, конъюнкцию и отрицание, с помощью операции суперпозиции.

Система (множество) функций называется **полной**, если любую функцию алгебры логики можно выразить через функции этой системы с помощью операции суперпозиции.

Мы доказали, что система функций $\{\overline{x}, x_1\vee\ x_2, x_1\wedge\ x_2\}$ является полной.

Тождество $\overline{x_1\vee\ x_2}=\overline{x_1}\wedge\ \overline{x_2}$ показывает, что мы можем выразить дизъюнкцию через конъюнкцию и отрицание $x_1\vee\ x_2=\overline{\overline{x_1}\wedge\ \overline{x_2}}$, поэтому система функций $\{\overline{x}, x_1\wedge\ x_2\}$ также является полной.

Аналогичным образом, используя тождество $\overline{x_1\wedge\ x_2}=\overline{x_1}\vee\ \overline{x_2}$, мы можем выразить конъюнкцию через дизъюнкцию и отрицание $x_1\wedge\ x_2=\overline{\overline{x_1}\vee\ \overline{x_2}}$. Поэтому система функций $\{\overline{x}, x_1\vee\ x_2\}$ также является полной.

Следующая теорема дает простой способ определения полноты системы функций.

Теорема 3.2. *Система функций является полной тогда и только тогда, когда дизъюнкцию, конъюнкцию и отрицание можно выразить с помощью операции суперпозиции через функции этой системы.*

Действительно, если это возможно, то произвольную функцию алгебры логики можно сначала выразить через дизъюнкцию, конъюнкцию и отрицание, а потом эти функции выразить через функции нашей системы. В обратную сторону утверждение очевидно.

Иногда система функций порождает не все функции алгебры логики, а только некоторый их подкласс θ. В этом случае, говорят, что эта система образует **базис** этого класса.

Например, все функции, построенные из дизъюнкции и конъюнкции с помощью операции суперпозиции, обладают свойствами: они равны 1, если все их переменные положить равными 1, также, они равны 0, если все их переменные положить равными 0, Пример такой функции - $((x_1\wedge\ x_2)\vee\ ((x_3\wedge\ x_2)\vee\ (x_1\wedge\ x_4))\wedge\ x_5$.

Таким образом, никогда не получится отрицание, так как оно на 1 равно 0. Следовательно, система функций, порожденная с помощью базиса $\{\wedge,\vee\}$, не совпадает с классом P_2 всех функций алгебры логики.

Задачи. Доказать, что следующие системы функций являются полными.

$\{\bar{x}, x_1 \to x_2\}$, $\{x_1 \to x_2, 0\}$, $\{x_1 \mid x_2\}$, $\{x_1 \downarrow x_2\}$, $\{x_1 \cdot x_2, x_1 + x_2, 1\}$

Доказать, что следующие системы функций не являются полными
$\{x_1 \cdot x_2, x_1 + x_2, 0\}$, $\{x_1 \to x_2, x_1 \vee x_2, 1\}$, $\{x_1 \cdot x_2, x_1 \vee x_2, 1\}$

3.4. Многочлены Жегалкина

Докажем, что система функций $\{x_1 \cdot x_2, x_1 + x_2, 1\}$ является полной. Действительно, легко проверить по таблице, что $\bar{x} = x + 1$. Также имеем

$$x_1 \vee x_2 = \overline{\overline{x_1} \wedge \overline{x_2}} = (x_1 + 1) \cdot (x_2 + 1) + 1 = x_1 \cdot x_2 + x_1 + x_2 + 1 + 1 =$$
$$= x_1 \cdot x_2 + x_1 + x_2.$$

Отсюда следует полнота системы функций $\{x_1 \cdot x_2, x_1 + x_2, 1\}$. Таким образом, любую функцию алгебры логики можно выразить через умножение и сложение по модулю 2, используя также константу 1 и переменные Выражение, построенное из переменных с помощью операции умножения, сложения и свободного члена 1, называется многочленом Жегалкина. Таким образом, мы доказали первую часть теоремы.

Теорема 3.3. *Любая функция алгебры логики может быть записана в виде многочлена. Такое представление этой функции является единственным. Другими словами, два различных многочлена не могут принимать одинаковые значения при всех значениях переменных.*

Второе утверждение теоремы доказывается исходя из комбинаторных соображений. Во-первых, заметим, что мы ранее доказали, что число всех функций алгебры логики от *n* переменных равно 2^{2^n}. Найдем теперь число всех многочленов от *n* переменных. Каждый такой многочлен представляет собой сумму свободного члена, одночленов первой степени, одночленов второй степени и т.д.; последний одночлен имеет *n*-тую степень.

$$\alpha_0 + \alpha_1 x_1 + \alpha_2 x_2 + \ldots \alpha_n x_n + \alpha_{12} x_1 \cdot x_2 + \ldots \alpha_{n-1,n} x_{n-1} x_n + \ldots.$$
$$\alpha_{12\ldots n} x_1 \cdot x_2 \cdot \ldots x_n$$

Каждый из коэффициентов α с нижними индексами равен 0 или 1, в зависимости от того, присутствует ли соответствующий одночлен в данном многочлене или нет. Таким образом, число всех многочленов от *n* переменных равно числу всех наборов таких коэффициентов α. Каждый такой набор представляет собой последовательность, состоящую из 0 и 1. Остается вычислить число всех таких наборов. Для этого надо узнать длину такого набора. Он содержит один - $1 = C_n^0$, коэффициент, который определяет свободный член, $n = C_n^1$ коэффициентов, которые определяют *n* членов первого порядка, C_n^2 коэффициентов при попарных произведениях переменных, и т.д. Последний коэффициент определяет наличие одночлена – произведения всех переменных. Каждый из коэффициентов равен 1, если соответствующий ему одночлен присутствует в многочлене, он равен 0, если такого одночлена нет. Таким образом, произвольный многочлен однозначно характеризуется строкой из 0 и 1 длины $m = C_n^0 + C_n^1 + C_n^2 + \ldots + C_n^{n-1} + C_n^n = 2^n$. Общее число таких строк, а значит и многочленов от *n* переменных равно $2^m = 2^{2^n}$.

Так как число всех различных функций алгебры логики также равно числу $2^m = 2^{2^n}$, каждой функции может соответствовать только один многочлен. Если бы два различных многочлена определяли одну и ту же функцию алгебры логики, то

многочленов просто бы не хватило, для выражения всех функций алгебры логики.

Примеры представления функций алгебры логики через многочлен $x_1 \to x_2 = \overline{x_1} \vee x_2 = (x_1 + 1) \cdot x_2 + x_1 + 1 + x_2 = x_1 \cdot x_2 + x_1 + x_2 + 1$.

Задачи. Выразить через многочлены следующие функции

$x_1 \mid x_2$, $x_1 \downarrow x_2$, $x_1 \wedge (x_2 \vee x_3)$, $(x_1 \vee \overline{x_2}) \to x_3$, $x_1 \leftrightarrow x_2$

3.5. Каскадный сумматор

В современных вычислительных устройствах используется двоичное представление чисел и побитовые операции над ними. Мы построим логическую схему каскадного сумматора – устройства, с помощью которого производится сложение чисел в двоичной записи. Мы соберем это устройство из элементарных устройств, реализующих сумму двух битов по модулю 2. Будем рассматривать числа, составленные не более чем из N битов (обычно $N=32$ или $N=64$).

Рассмотрим два числа x и y в двоичной записи. Перенумеруем их биты в обратном порядке: $x = x_N x_{N-1} \ldots x_3 x_2 x_1$ и $y = y_N y_{N-1} \ldots y_3 y_2 y_1$.

Каскадный сумматор состоит из N соединенных между собой блоков. Каждый блок реализует сложение битов x_i и y_i очередного разряда и бита переноса u_i от предыдущего разряда (это тот бит, который мы сохраняем «в уме» при сложении столбиком). В i-ом блоке вычисляется сумма $z_i = x_i + y_i + u_i$, а также формирует бит переноса u_{i+1} для старшего разряда. На вход блока поступают три бита x_i, y_i, u_i, причем $u_1 = 0$. На выходе блока – два значения z_i, u_{i+1}. Если $u_{N+1} = 1$, то происходит переполнение сумматора. В этом случае результат сложения не определен. Если переполнения нет, то на выходе каскадного сумматора будет обычная арифметическая сумма $z = z_N z_{N-1} \ldots z_3 z_2 z_1$ чисел x и y в двоичной записи.

Бит переноса u_{i+1} можно задать следующей таблицей значений

x_i	y_i	u_i	u_{i+1}
0	0	0	0
0	0	1	0
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	1
1	1	1	1

Строим СДНФ по этой таблице для функции, которая принимает значения u_{i+1} при заданных значениях x_i, y_i, u_i.

$$u_{i+1} = \overline{x_i} \cdot y_i \cdot u_i \vee x_i \cdot \overline{y_i} \cdot u_i \vee x_i \cdot y_i \cdot \overline{u_i} \vee x_i \cdot y_i \cdot u_i = x_i \cdot y_i + x_i \cdot u_i + y_i \cdot u_i$$

Задача. Провести необходимые преобразования формулы в многочлен.

Таким образом, блок с номером i получает на вход биты x_i, y_i, u_i и выдает в качестве выхода биты z_i, u_{i+1}, вычисленные по формулам

$$z_i = x_i + y_i + u_i,$$

$$u_{i+1} = x_i \cdot y_i + x_i \cdot u_i + y_i \cdot u_i$$

Этот блок можно реализовать в виде комбинации 4-х элементарных сумматоров и 3-х элементарных умножителей. Каждый такой сумматор вычисляет сумму $z = x + y$ по модулю 2. Каждый такой умножитель вычисляет произведение битов $z = x \cdot y$.

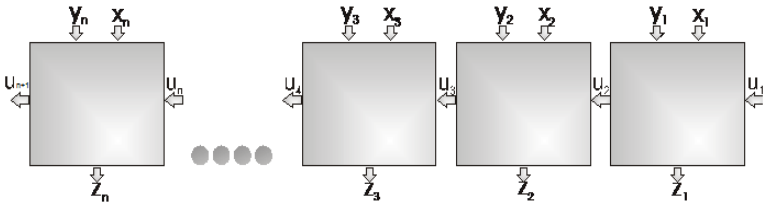


Рис. 3.1. *Блок - схема каскадного сумматора*

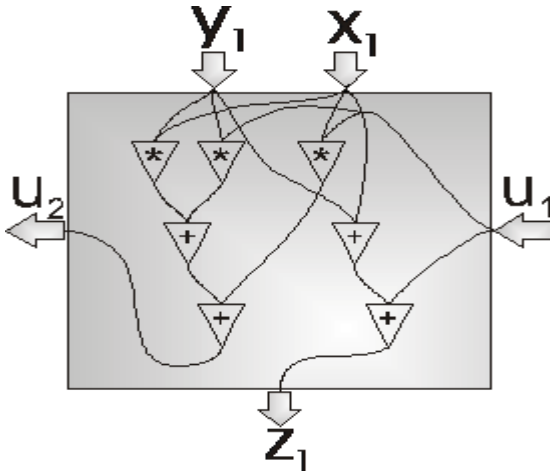


Рис. 3.2. Схема одного блока сумматора

Задача. Составить схему блока каскадного сумматора из элементов, вычисляющих функции $x_1 \vee x_2, x_1 \wedge x_2, \overline{x}$.

3.6. Замкнутые классы функций алгебры логики.

Напомним, что P_2 - класс всех функций алгебры логики. Рассмотрим более подробно **операцию суперпозиции** или просто **операцию подстановки** функций алгебры логики. Пусть имеются функции $f_1(x_1,...x_{k_1}) \in P_2, ...f_m(x_1,...x_{k_m}) \in P_2, F(y_1,...y_m) \in P_2$. Тогда можно рассмотреть новую функцию алгебры логики $G(x_1,...x_K) = F(f_1(x_1,...x_{k_1}),...f_m(x_1,...x_{k_m}))$, где множество ее переменных $x_1,...x_K$ получено путем объединения всех переменных всех функций $f_1,...f_m$. Будем говорить, что эта функция получена **операцией суперпозиции** из функций $f_1,...f_m, F$.

Мы будем рассматривать подклассы (подмножества) класса P_2 всех функций алгебры логики.. Пусть θ - некоторый подкласс

класса P_2 всех функций алгебры логики, т.е. $\theta \subseteq P_2$. Будем подставлять функции этого подкласса в другие функции этого подкласса. Подкласс, который получится в результате всех возможных таких подстановок, будет называться (функциональным) **замыканием** класса θ относительно операции суперпозиции и будет обозначаться $[\theta]$. Ясно, что $\theta \subseteq [\theta] \subseteq P_2$.

Из определения операции замыкания и полного класса функций алгебры логики следует, что система функций θ полна тогда и только тогда, когда $[\theta] = P_2$.

Класс (множество) функций алгебры логики θ называется **замкнутым** относительно операции суперпозиции, если он совпадает со своим замыканием - $[\theta] = \theta$. Более подробно, можно сказать, что класс функций алгебры логики θ называется замкнутым, если при подстановке любых функций из этого класса в любую другую функцию этого класса мы получаем функцию из того же класса. Формально, пусть θ - некоторый замкнутый класс функций алгебры логики и $f_1(x_1,...x_{k_1}) \in \theta, ...f_m(x_1,...x_{k_m}) \in \theta, F(y_1,...y_m) \in \theta$. Тогда $F(f_1(x_1,...x_{k_1}),...f_m(x_1,...x_{k_m})) \in \theta$.

Мы рассмотрим пять замкнутых классов функций алгебры логики.

1. **Класс T_0 всех функций алгебры логики, сохраняющих 0, т.е. таких, что $f(0,...0) = 0$.**

Легко проверить, что функции $x \wedge y$, $x \vee y$, $x + y$, 0 принадлежат этому классу, функции $\bar{x}$, $x \to y$, 1 не принадлежат ему.

Задача. Проверить, что класс T_0 является функционально замкнутым**.** Это значит, что при подстановке функций, сохраняющих 0, в функцию, сохраняющую 0, снова получается функция, сохраняющая 0.

Теорема 3.4. *Класс T_0 порождается операцией суперпозиции из двух функций x+y и $x \cdot y$.*

Доказательство. Любая функция из класса T_0 выражается в виде многочлена Жегалкина, в котором свободный член равен 0. Каждый такой многочлен выражается через функции *x+y и* $x \cdot y$.

2. **Класс T_1 всех функций алгебры логики, сохраняющих 1, т.е. таких, что $f(1,...1) = 1$.**

Легко проверить, что функции $x \wedge y$, $x \vee y$, $x \to y$, 1 принадлежат этому классу, функции $\bar{x}$, 0, $x + y$ не принадлежат ему.

Задача. Проверить, что класс T_1 является функционально замкнутым**.** Это значит, что при подстановке функций, сохраняющих 1, в функцию, сохраняющую 1, снова получается функция, сохраняющая 1.

Теорема 3.5. *Класс T_0 порождается операцией суперпозиции из двух функций x+y+1 и $x \vee y$.*

Доказать эту теорему в виде задачи.

3. **Класс *S* всех самодвойственных функций алгебры логики.**

Функция $f(x_1, x_2, ...x_n)$ называется **самодвойственной**, если $f(x_1, x_2, ...x_n) = \overline{f(\bar{x}_1, \bar{x}_2, ...\bar{x}_n)}$ для всех значений переменных. Для того, чтобы проверить является ли функция самодвойственной достаточно проанализировать таблицу ее значений. По

определению, значения функции в верхней половине таблицы должны быть отрицаниями симметрично расположенных значений нижней половины таблицы. Пример таблично заданной самодвойственной функции

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	1
1	1	0	0
1	1	1	1

Теорема 3.6. *Класс S является функционально замкнутым. Это значит, что при подстановке самодвойственных функций в самодвойственную функцию снова получается самодвойственная функция.*

Доказательство. Пусть заданы произвольные самодвойственные функции $f_1(x_1,...x_{k_1}) \in S,...f_m(x_1,...x_{k_m}) \in S, F(y_1,...y_m) \in S$. Это означает, что для всех этих функций выполнены равенства

$f_i(x_1, x_2,....x_{k_i}) = \overline{f_i(\bar{x}_1, \bar{x}_2,....\bar{x}_{k_i})}$, $i = 1,2,...m$, и

$F(x_1, x_2,....x_m) = \overline{F(\bar{x}_1, \bar{x}_2,....\bar{x}_m)}$ при всех значениях переменных.

Мы будем пользоваться эквивалентными тождествами $\overline{f_i(x_1, x_2,....x_{k_i})} = f_i(\bar{x}_1, \bar{x}_2,....\bar{x}_{k_i})$ и $\overline{F(x_1, x_2,....x_K)} = F(\bar{x}_1, \bar{x}_2,....\bar{x}_K)$, которые получены отрицанием обоих частей предыдущих тождеств.

Докажем, что результат подстановки $G(x_1,...x_K) = F(f_1(x_1,...x_{k_1}),...f_m(x_1,...x_{k_m}))$ также будет самодвойственной функцией. Действительно, из определения самодвойственной функции следует, что верны следующие тождества

$$\overline{G(\bar{x}_1, \bar{x}_2,....\bar{x}_K)} = \overline{F(f_1(\bar{x}_1,...\bar{x}_{k_1}),....f_1(\bar{x}_1,...\bar{x}_{k_m}))} =$$
$$= \overline{F(\overline{f_1(x_1, x_2....x_{k_1})},....\overline{f_m(x_1, x_2....x_{k_m})})} =$$
$$= F(f_1(x_1,...x_{k_1}),...f_m(x_1,...x_{k_m})) = G(x_1,...x_K).$$

Таким образом, результат подстановки – функция $G(x_1,...x_K)$, также является самодвойственной. Теорема доказана.

4 Класс *M* всех монотонных функций алгебры логики.

Рассмотрим отношение частичного порядка на всех кортежах, состоящих из 0 и 1 одинаковой длины: $(x_1, x_2,...x_n) \prec (y_1, y_2,...y_n)$ тогда и только тогда, когда $x_1 \le y_1, x_2 \le y_2,...x_n \le y_n$.

Задача. Проверить, что это действительно отношение частичного порядка. Привести примеры, показывающие, что это отношение не является отношением линейного порядка.

Функция $f(x_1, x_2, ...x_n)$ называется **монотонной**, если $f(x_1, x_2, ...x_n) \leq f(y_1, y_2, ...y_n)$ при $(x_1, x_2, ...x_n) \prec (y_1, y_2, ...y_n)$.

Для того, чтобы проверить является ли функция монотонной достаточно проанализировать таблицу ее значений.

Пример таблично заданной монотонной функции приведен в предыдущей таблице.

Пример таблично заданной функции, которая не является монотонной

x_1	x_2	x_3	f
0	0	0	0
0	0	1	1
0	1	0	0
0	1	1	1
1	0	0	0
1	0	1	0
1	1	0	0
1	1	1	1

При сравнении 2 и 6 строки мы видим, что *(0,0,1)* $\prec$ *(1,0,1)*, *однако f(0,0,1)=1>0=f(1,0,*1). На этих строках условие монотонности нарушается.

Задача. Проверить, что класс *M* является функционально замкнутым**.** Это значит, что при подстановке монотонных функций в монотонную функцию снова получается монотонная функция.

Класс всех монотонных функций, отличных от константы, имеет простой базис. Этот факт будет следовать из следующих нескольких теорем.

Теорема 3.7. (о разложении по переменной). *Произвольная функция алгебры логики может быть представлена в виде* $f(x_1, ...x_i ...x_n) = x_i \cdot f(x_1, ...1...x_n) \vee \overline{x_i} \cdot f(x_1, ...0...x_n)$ *для любого i.*

Это тождество доказывается прямой проверкой при $x_i = 0$ и $x_i = 1$.

Следствие. *Для любой монотонной функции имеет место представление*

$$f(x_1, ...x_i ...x_n) = x_i \cdot f(x_1, ...1...x_n) \vee f(x_1, ...0...x_n)$$

для любого i.

Доказательство. Так как для любой монотонной функции $f(x_1, ...x_i ...x_n)$ выполнено $f(x_1, ...0...x_n) \leq f(x_1, ...1...x_n)$ для любого i, множитель $\overline{x_i}$ в представлении теоремы можно опустить. Это доказывается прямой проверкой при $x_i = 0$ и $x_i = 1$.

Теорема 3.8. *Всякая монотонная функция, отличная от константы, может быть получена с помощью операции суперпозиции из функций* $x \wedge y$ *и* $x \vee y$.

Доказательство. Мы будем доказывать это утверждение с помощью математической индукции по числу *n* переменных. При *n =1* утверждение очевидно. При *n >1* каждая из функций $f(x_1,...1...x_n)$ и $f(x_1,...0...x_n)$ из представления $f(x_1,...x_i...x_n) = x_i \cdot f(x_1,...1...x_n) \vee f(x_1,...0...x_n)$ является монотонной и зависит от меньшего числа переменных. Если хотя бы одна из них была константой, то это представление также можно было бы упростить до функций с меньшим числом переменных. Поэтому утверждение следует из математической индукции по числу переменных.

5. **Класс *L* всех линейных функций.**

Функция называется **линейной**, если ее многочлен Жегалкина не содержит произведений переменных. Примеры линейных функций $\bar{x} = x + 1$, $x + y$, $x \leftrightarrow y = x + y + 1$. Нелинейными являются функции $x \wedge y = x \cdot y$, $x \vee y = x \cdot y + x + y$, $x \to y = x \cdot y + x + y + 1$.

Из определения следует, что линейные функции – это просто все функции вида *0* и $x_1 + x_2 + ... + x_n$ для *n=1,2.....*

Задача. Проверить, что класс *L* является функционально замкнутым**.** Это значит, что при подстановке линейных функций в линейную функцию снова получается линейная функция.

Классы функций T_0, T_1, *S, M, L* используются для определения критерии полноты системы функций.

3.7. Критерий функциональной полноты

Имеет место основная **теорема о функциональной полноте.**

Теорема 3.9. *Система функций является полной тогда и только тогда когда она не является подмножеством ни одного из пяти замкнутых классов* T_0, T_1, *S, M, L.*

Пример полной системы функций. Этот пример предлагает способ определения полноты системы функций. Для определения полноты системы функций надо заполнить подобную таблицу.

	T_0,	T_1	*S*	*M*	*L*
$x_1 + x_2$	+	-	-	-	+
$x_1 \vee x_2$	+	+	-	+	-
1	-	+	-	+	+

Данная таблица показывает, что система функций $\{x_1 + x_2, x_1 \vee x_2, 1\}$ является полной, так как не является подмножеством ни одного из пяти классов T_0, T_1, *S, M, L*. Это следует из того, что в каждом столбце стоит хотя бы один минус, который указывает, что соответствующая функция не принадлежит классу из этого столбца. Первые две строки таблицы показывают, что система функций $\{x_1 + x_2, x_1 \vee x_2\}$ не является полной, так как первый столбец сокращенной таблицы состоит из

одних плюсов, т.е. $\{x_1 + x_2, x_1 \vee x_2\} \subseteq T_0$. Эту систему достаточно дополнить единицей, для того чтобы она стала полной.

Прежде чем доказывать основную теорему, проверим, что все классы T_0, T_1, S, M, L - различные. Это показывает следующая таблица, которая выражает принадлежность трех функций – констант 0 и 1 и отрицания $\bar{x}$ к классам T_0, T_1, S, M, L. Все эти утверждения о принадлежности к классам или очевидны или ранее доказаны.

	T_0	T_1	S	M	L
0	+	-	-	+	+
1	-	+	-	+	+
$\bar{x}$	-	-		-	+

Поскольку в таблице все столбцы различные – никакие два класса из T_0, T_1, S, M, L не могут совпадать. Отсюда также следует, что ни один из этих классов не совпадает с классом P_2 всех функций алгебры логики.

Доказательство теоремы о функциональной полноте.

Доказательство необходимости. Пусть система функций Θ полна, т.е. $[\Theta] = P_2$. Допустим, что множество функций Θ является подмножеством одного из замкнутых классов T_0, T_1, S, M, L, например $\Theta \subseteq M$. Тогда будет $P_2 = [\Theta] \subseteq [M] = M$, т.е. класс монотонных функций совпадает с классом всех функций алгебры логики $M = P_2$. Как только что было замечено, это утверждение неверно. Полученное противоречие показывает, что $\Theta \not\subset M$. Аналогичным образом доказывается, что класс Θ не является подмножеством ни одного из остальных пяти замкнутых классов.

Доказательство достаточности. Так как класс Θ не содержится ни в одном из пяти классов, выберем какие-нибудь функции f_i, f_j, f_k, f_m, f_l так, что $\{f_i, f_j, f_k, f_m, f_l\} \subseteq \Theta$ и $f_i \notin T_0, f_j \notin T_1, f_k \notin S, f_m \notin M, f_l \notin L$. Используя эти функции, выразим конъюнкцию и отрицание через функции f_i, f_j, f_k, f_m, f_l. Мы ранее показали, что конъюнкция и отрицание образуют полную систему функций. Отсюда следует, что любую функцию алгебры логики можно выразить через функции f_i, f_j, f_k, f_m, f_l. Таким образом, уже эта система из пяти функций (а значит, и система Θ) будет обладать свойством полноты.

Выражать конъюнкцию и отрицание через функции f_i, f_j, f_k, f_m, f_l. будем в три этапа.

Этап 1. *Построение с помощью функций f_i, f_j, f_k констант 0 и 1.*

По выбору $f_i \notin T_0$, т.е. $f_i(0.,0,...0) = 1$. Возможны два случая.

1) $f_i(1,1,...1) = 1$. Тогда функция $\phi(x) = f_i(x,x,...x) = 1$ для всех x, т.е. является константой 1. По определению $f_j(1.,1,...1) = 0$. Вторая константа 0 получается в виде $\varphi(x) = f_j(\phi(x), \phi(x), ...\phi(x)) = 0$.

2) $f_i(1.1,...1) = 0$. Тогда $\phi(0) = f_i(0,0,...0) = 1$ по определению и $\phi(1) = f_i(1,1,...1) = 1$ по этому случаю. Значит $\phi(x) = \bar{x}$. Возьмем $f_k \notin S$. Предварительно докажем лемму 3.1.

Лемма 3.1. *Если $f_k \notin S$, то, подставляя вместо ее переменных переменные x или $\bar{x}$, можно получить функцию - константу - 0 или 1.*

Доказательство. Так как $f_k \notin S$ найдется набор битов $(\alpha_1,\alpha_2..\alpha_k)$, число которых равно числу переменных функции f_k, на котором нарушается условие самодвойственности. Из определения следует, что это нарушение должно иметь вид $f(\bar{\alpha}_1,\bar{\alpha}_2,..\bar{\alpha}_k) = f(\alpha_1,\alpha_2..\alpha_k)$. Обозначим $x^0 = \bar{x}$ и $x^1 = x$. Тогда можно заметить, что $0^\alpha = \bar{\alpha}$ и $1^\alpha = \alpha$ для всех $\alpha = 0,1$. Эти равенства нетрудно проверить непосредственно $0^0 = \bar{0}$ и $0^1 = 0 = \bar{1}$ и $1^0 = \bar{1} = 0$, $1^1 = 1$.

Рассмотрим функцию $\phi(x) = f(x^{\alpha_1},x^{\alpha_2}...x^{\alpha_k})$. Для этой функции имеем $\phi(0) = f(0^{\alpha_1},0^{\alpha_2}...0^{\alpha_k}) = f(\bar{\alpha}_1,\bar{\alpha}_2,..\bar{\alpha}_k)$ и $\phi(1) = f(1^{\alpha_1},1^{\alpha_2}...1^{\alpha_k}) = f(\alpha_1,\alpha_2..\alpha_k)$. По выбору набора битов $f(\bar{\alpha}_1,\bar{\alpha}_2,..\bar{\alpha}_k) = f(\alpha_1,\alpha_2..\alpha_k)$. Значит $\phi(0) = \phi(1)$, т.е. функция $\phi(x)$ - это константа, тождественно равная 0 или 1. Лемма доказана. Заметим, что конкретное значение константы -0 или 1, зависит от конкретного вида функции $f_k \notin S$.

Возвращаемся к доказательству этапа 2 теоремы. Мы уже получили функцию $\phi(x) = \bar{x}$. По лемме 1 из этой функции и $f_k \notin S$ получим константу α, равную 0 или 1. Так как мы уже получили отрицание, то противоположную константу получим в виде $\beta = \phi(\alpha)$.

Этап 1) завершен – мы построили с помощью функций f_i, f_j, f_k константы 0 и 1.

Этап 2. Построение с помощью констант 0, 1 и функции $f_m \notin M$ отрицания $\bar{x}$.

Этот этап будет реализован в виде следующей леммы.

Лемма 3.2. *Если $f_m \notin M$, то из нее можно путем подстановки переменной x и констант 0 и 1 получить функцию отрицания $\bar{x}$.*

Доказательство. Так как функция f_m не монотонная, найдутся два набора переменных $(\alpha_1,\alpha_2..\alpha_k) \prec (\beta_1,\beta_2...\beta_k)$, для которых $f_m(\alpha_1,\alpha_2..\alpha_k) > f_m(\beta_1,\beta_2...\beta_k)$. Двигаясь согласно порядку $\prec$ от нулевого набора $(0,0,...0)$ в сторону увеличения, найдем два таких набора вида $(\alpha_1,...0,..\alpha_k) \prec (\alpha_1,...1,..\alpha_k)$, которые являются соседними относительно данного порядка и на которых нарушается условие монотонности. Нарушение заключается в том, что выполнено $f_m(\alpha_1,...0,..\alpha_k) > f_m(\alpha_1,...1,..\alpha_k)$. Рассмотрим функцию $\phi(x) = f_m(\alpha_1,...x,..\alpha_k)$. Для нее выполнено $\phi(0) = f_m(\alpha_1,...0,..\alpha_k) > f_m(\alpha_1,...1,..\alpha_k) = \phi(1)$. Значит $\phi(0) = 1 > 0 = \phi(1)$, т.е. $\phi(x) = \bar{x}$. Лемма доказана.

Этап 3. Построение при помощи констант 0 и 1 и функций $\bar{x}$ и $f_l \notin L$ конъюнкции $x_1 \cdot x_2 = x_1 \wedge x_2$. Этот этап мы оформим в виде леммы 3.3.

Лемма 3.3. *Если $f_l \notin L$, то из нее, функций x, $\bar{x}$ и констант 0 и 1 можно получить функцию $x_1 \cdot x_2 = x_1 \wedge x_2$.*

Доказательство. Функция $f_l \notin L$ является полиномом не менее чем 2-го порядка. Выделим из него произведение двух переменных $x_1 \cdot x_2$ и фиксируем все остальные переменные так, чтобы наш полином имел вид $f(x_1, x_2) = x_1 \cdot x_2 + \alpha \cdot x_1 + \beta \cdot x_2 + \gamma$. Рассмотрим функцию

$$\varphi(x_1 + \beta, x_2 + \alpha) + \alpha \cdot \beta + \gamma =$$
$$(x_1 + \beta) \cdot (x_2 + \alpha) + \alpha \cdot (x_1 + \beta) + \beta \cdot (x_2 + \alpha) + \gamma + \alpha \cdot \beta + \gamma =$$
$$x_1 \cdot x_2 + \alpha \cdot x_1 + \beta \cdot x_2 + \alpha \cdot \beta + \alpha \cdot x_1 + \alpha \cdot \beta + \beta \cdot x_2 +$$
$$\alpha \cdot \beta + \gamma + \alpha \cdot \beta + \gamma = x_1 \cdot x_2.$$

Лемма доказана.

Таким образом, мы доказали, что функции $\bar{x}$ и $x_1 \cdot x_2$ могут быть выражены через набор функций f_i, f_j, f_k, f_m, f_l. Теорема доказана.

Следствие. *Всякий замкнутый класс функций алгебры логики совпадает с классом P_2 или является подмножеством одного из пяти замкнутых классов T_0, T_1, S, M, L.*

Доказательство. Пусть для некоторого замкнутого класса функций алгебры логики Θ выполнено $\Theta \not\subset T_0, \Theta \not\subset T_1, \Theta \not\subset S, \Theta \not\subset M, \Theta \not\subset L$. Тогда по основной теореме о полноте этот класс является полным и $\Theta = [\Theta] = P_2$.

Класс функций Θ называется **предполным**, (или максимальным) если он неполный и для любой функции $f \notin \Theta$ класс $\Theta \cup \{f\}$ является полным.

Теорема 3.10. *Всякий предполный класс является замкнутым.*

Допустим, что класс Θ предполный и незамкнутый. Тогда существует функция g, которая выражается через функции класса Θ, но не принадлежит ему. По определению предполного класса $[\Theta \cup \{g\}] = P_2$. С другой стороны замыкания классов Θ и $\Theta \cup \{g\}$ должны совпадать. Поэтому $[\Theta] = P_2$, т.е. класс Θ - полный. Полученное противоречие доказывает теорему.

Следствие. *В классе P_2 имеется только пять предполных классов, а именно, это классы T_0, T_1, S, M, L.*

Доказательство. Пусть класс Θ предполный. Так как он неполный, он должен быть подмножеством одного из пяти замкнутых классов. Пусть, например, $\Theta \subseteq M$. Если эти два класса не совпадают, то существует функция $f \in M \div \Theta$. Тогда $[\Theta \cup \{f\}] = P_2$ и $[\Theta \cup \{f\}] \subseteq M \subseteq P_2$. Отсюда следует $M = P_2$, что невозможно.

Задача. Проверить на полноту следующие системы функций. Если система не полна, то добавить к ней наиболее простую функцию, так чтобы она стала полной

$\{x_1 \to x_2, \overline{x_1 \to x_2}\}$, $\{x_1 \to x_2, x_1 + x_2\}$, $\{x_1 \to x_2, 1\}$,

$\{x_1 \leftrightarrow x_2, x_1 \vee x_2, 0\}$, $\{\bar{x}, x_1 \cdot x_2 + x_1 \cdot x_3 + x_2 \cdot x_3\}$.

Список литературы

1. Виленкин Н.Я., Виленкин А.Н., Виленкин П.А. Комбинаторика. ФИМА, МЦНМО, 2006.

2. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по курсу дискретной математики. М.: Наука. 1992.

3. Марченков С.С. Замкнутые классы булевых функций. М.: Физматлит. 2000.

4. Яблонский С.В. Введение в дискретную математику. М.: Наука. - 1986.