МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
БУРЯТСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ МАТЕМАТИКИ И ИНФОРМАТИКИ

И. К. Шаранхаев

Элементы дискретной математики

*Рекомендовано Учебно-методическим
советом БГУ в качестве учебного пособия
для специальностей «Математика»,
«Прикладная математика и информатика»,
«Математическое обеспечение и админист-
рирование информационных систем».*

Улан-Удэ
Издательство Бурятского госуниверситета
2006

УДК 519.71, 519.17 (075.8)
ББК 22.174
Ш 25

Утверждено к печати
редакционно-издательским советом
Бурятского государственного университета

Рецензенты:

Б. М. Степанов, кандидат технических наук, доцент
И. Б. Юмов, кандидат физико-математ. наук, доцент

Шаранхаев И. К.
Ш 25 **Элементы дискретной математики:** Учеб. пособие. – Улан-Удэ: Издательство Бурятского госуниверситета, 2006. – 63 с.

Учебное пособие написано на основе курса лекций по дискретной математике, читаемого студентам Института математики и информатики БГУ. В нем рассмотрены такие разделы дискретной математики как комбинаторика, булевы функции, графы.

Предназначено для студентов, аспирантов и преподавателей математических специальностей вузов.

Содержание

Введение

В последние десятилетия дискретная математика является интенсивно развивающейся областью современной математической науки. В первую очередь связано это с бурным развитием компьютерной техники и новых информационных технологий. Не секрет, что в сравнении с непрерывной дискретная математика в настоящее время является не менее значимым звеном в прикладном математическом образовании. Поэтому изучение основ дискретной математики является обязательным при подготовке специалистов высокого уровня.

В данном учебном пособии рассмотрены несколько важных разделов дискретной математики.

В первой главе изучаются различные комбинаторные объекты и их свойства, комбинаторные тождества, а также некоторые методы комбинаторного анализа.

Вторая глава посвящена в основном различным вопросам представления булевых функций или функций алгебры логики термами (формулами).

В третьей главе рассмотрен ряд вопросов, касающихся теории графов: планарность, сети, деревья и т. д.

В основу книги положен материал курсов лекций, читаемых автором в Институте математики и информатики Бурятского государственного университета по специальностям «Математика», «Прикладная математика и информатика», «Математическое обеспечение и администрирование информационных систем».

Предложенный в конце книги список литературы несомненно поможет читателю в более глубоком изучении дискретной математики.

Автор благодарен коллективу кафедры алгебры ИМИ БГУ за содействие и поддержку, оказанные при подготовке этой книги.

1 Элементы комбинаторики

Комбинаторика — это раздел дискретной математики, изучающий объекты, порождаемые элементами из конечного множества $A = \{a_1, \ldots, a_n\}$, а также числовые характеристики этих объектов. В математике и нередко в практической деятельности приходится иметь дело с задачами комбинаторного характера, то есть в которых нужно подсчитать количество возможных комбинаций объектов, удовлетворяющих определенным условиям. Разнообразие комбинаторных задач очень велико, и для решения многих из них имеется развитый математический аппарат.

1.1 Размещения, перестановки, сочетания

Размещения без повторений. *Размещением без повторений* элементов из $A = \{a_1, \ldots, a_n\}$ по k (или размещением без повторений из n элементов по k) называется упорядоченное подмножество из k элементов множества A.

П р и м е р. $A = \{a_1, a_2, a_3\}$ и $k = 2$. Все размещения без повторений из 3 элементов по 2 выглядят следующим образом: $< a_1, a_2 >$, $< a_2, a_1 >$, $< a_1, a_3 >$, $< a_3, a_1 >$, $< a_2, a_3 >$, $< a_1, a_2 >$.

Обозначим число размещений без повторений из n по k через A_n^k.

Т е о р е м а 1. $A_n^k = n(n-1) \cdot \ldots \cdot (n-k+1)$ при $1 \le k \le n$.

Д о к а з а т е л ь с т в о проведем индукцией по k.

Базис индукции. При $k = 1$ имеем $A_n^1 = n$. Действительно, различных одноэлементных подмножеств множества A существует ровно n.

Шаг индукции. По предположению индукции $A_n^{k-1} = n(n-1) \cdot \ldots \cdot (n-k+2)$. Рассмотрим произвольное размещение из n по $k-1$, обозначим его $< a_{i_1}, a_{i_2}, \ldots, a_{i_{k-1}} >$ и построим с его помощью размещение из n по k $< a_{i_1}, a_{i_2}, \ldots, a_{i_{k-1}}, a_j >$. Очевидно, что $j \ne i_m$, где $1 \le m \le k-1$. Различных размещений из n по k таким способом можно построить ровно $n - k + 1$. Все размещения из n по k получим, перебирая все размещения из n по $k-1$, которых по предположению индукции имеется $n(n-1)\cdot\ldots\cdot(n-k+2)$. Отсюда, $A_n^k = n(n-1)\cdot\ldots\cdot(n-k+1)$. Теорема доказана.

С л е д с т в и е. $A_n^k = \dfrac{n!}{(n-k)!}$.

Напомним, что $n! = 1\cdot 2\cdot\ldots\cdot n$, а $0! = 1$.

Очевидно, что при $k > n$ размещений без повторений из n по k не существует, поэтому в этом случае считаем, что $A_n^k = 0$.

Кроме того полагаем, что $A_0^0 = A_n^0 = 1$, так как 0-элементным подмножеством является только пустое множество.

Легко заметить, что для чисел A_n^k имеют место следующие тождества

$$A_n^k = n\cdot A_{n-1}^{k-1} \text{ и } A_n^k = A_n^{k-1}\cdot(n-k+1).$$

Размещения с повторениями. *Размещением с повторениями* элементов из A по k (или размещением с повторениями из n элементов по k) называется упорядоченный набор из k элементов множества A, причем в наборе элементы могут повторяться.

П р и м е р. $A = \{a_1, a_2, a_3\}$ и $k = 2$. Все размещения с повторениями из 3 по 2 выглядят следующим образом: (a_1, a_1), (a_1, a_2), (a_1, a_3), (a_2, a_1), (a_2, a_2), (a_2, a_3), (a_3, a_1), (a_3, a_2), (a_3, a_3).

Обозначим число размещений с повторениями из n по k через $\tilde{A}_n^k$.

Т е о р е м а 2. $\tilde{A}_n^k = n^k$.

Д о к а з а т е л ь с т в о аналогично предыдущему, и оставляется читателю в качестве упражнения.

Перестановки. *Перестановкой* элементов множества A (или перестановкой из n элементов) называется упорядоченное множество из n элементов $a_1, \ldots, a_n$.

П р и м е р. $A = \{a_1, a_2, a_3\}$. Всевозможными перестановками из 3 элементов являются: $< a_1, a_2, a_3 >$, $< a_1, a_3, a_2 >$, $< a_2, a_1, a_3 >$, $< a_2, a_3, a_1 >$, $< a_3, a_1, a_2 >$, $< a_3, a_2, a_1 >$.

Обозначим число перестановок из n элементов через P_n. Очевидно, что перестановки из n элементов – частный случай размещений без повторений из n по k при $k = n$, т. е. $P_n = A_n^n$. Следовательно, имеет место следующая

Т е о р е м а 3. $P_n = n!$

Сочетания без повторений. *Сочетанием без повторений* элементов из A по k (или сочетанием без повторений из n элементов по

k) называется неупорядоченное подмножество из k элементов множества A.

П р и м е р. $A = \{a_1, a_2, a_3\}$ и $k = 2$. Всевозможными сочетаниями без повторений из 3 по 2 являются $\{a_1, a_2\}$, $\{a_1, a_3\}$, $\{a_2, a_3\}$.

Обозначим число сочетаний без повторений из n по k через C_n^k.

Т е о р е м а 4. $C_n^k = \dfrac{n!}{k!(n-k)!}$ при $0 \le k \le n$.

Д о к а з а т е л ь с т в о. В сочетании без повторений из n элементов по k в отличие от размещения без повторений из n по k порядок следования элементов не учитывается, поэтому из одного сочетания получается $k!$ размещений. Отсюда имеем $C_n^k = \dfrac{A_n^k}{k!} = \dfrac{n!}{k!(n-k)!}$. Теорема доказана.

С л е д с т в и е. $C_0^0 = C_n^0 = C_n^n = 1$ и $C_n^k = C_n^{n-k}$.

При $k > n$ сочетаний без повторений из n элементов по k не существует, поэтому в этом случае полагаем $C_n^k = 0$.

Сочетания с повторениями. *Сочетанием с повторениями* элементов из A по k (или сочетанием с повторениями из n элементов по k) называется неупорядоченный набор из k элементов множества A, в котором элементы могут повторяться.

П р и м е р. $A = \{a_1, a_2, a_3\}$ и $k = 2$. Всевозможными сочетаниями с повторениями из 3 по 2 являются (a_1, a_1), (a_1, a_2), (a_1, a_3), (a_2, a_2), (a_2, a_3), (a_3, a_3).

Обозначим число сочетаний с повторениями из n по k через $\tilde{C}_n^k$.

Т е о р е м а 5. $\tilde{C}_n^k = C_{n+k-1}^k$.

Д о к а з а т е л ь с т в о. Пусть $\tilde{a}$ – произвольное сочетание с повторениями элементов из A по k. Сочетанию $\tilde{a}$ поставим в соответствие набор $\sigma(\tilde{a})$ длины $n+k-1$ из $n-1$ нулей и k единиц следующим образом: в наборе $\sigma(\tilde{a})$ число единиц, находящихся между $(i-1)$-м и i-м нулями, равно числу элементов a_i, входящих в сочетание $\tilde{a}$ $(i = 2, \ldots, n-1)$, а число единиц, стоящих перед первым нулем (после последнего нуля), равно числу элементов a_1 (элементов a_n), входящих в $\tilde{a}$.

Например, сочетанию (a_1, a_1) из предыдущего примера соответствует набор 1100, а (a_2, a_3) – 0101.

Соответствие между сочетаниями $\tilde{a}$ и наборами $\sigma(\tilde{a})$ взаимно однозначно. Наборов длины $n+k-1$ из $n-1$ нулей и k единиц имеется ровно C_{n+k-1}^k, т. е. $\tilde{C}_n^k = C_{n+k-1}^k$. Теорема доказана.

1.2 Комбинаторные тождества

В предыдущем разделе были рассмотрены числа C_n^k и получена основная формула для подсчета таких чисел. Оказывается, что числа C_n^k, которые называются биномиальными коэффициентами, обладают целым рядом замечательных свойств.

1. $C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$.

Доказательство. Действительно, $C_{n-1}^{k-1} + C_{n-1}^k =$

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

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

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

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

2. $(x+y)^n = \sum\limits_{k=0}^{n} C_n^k x^k y^{n-k}$ (формула бинома Ньютона).

Доказательство проведем индукцией по n.

Базис индукции. $x + y = C_1^0 x^0 y^1 + C_1^1 x^1 y^0 = \sum\limits_{k=0}^{1} C_1^k x^k y^{1-k}$.

Шаг индукции. По предположению индукции

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

Используя равенство, получаем $(x+y)^n = (x+y)(x+y)^{n-1} =$

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

$$+\sum_{k=0}^{n-1} C_{n-1}^k x^k y^{n-k} = \sum_{k=0}^{n-2} C_{n-1}^k x^{k+1} y^{n-1-k} +$$

$$+\sum_{k=1}^{n-1} C_{n-1}^k x^k y^{n-k} + C_{n-1}^0 x^0 y^n + C_{n-1}^{n-1} x^n y^0 =$$

$$= \sum_{k=1}^{n-1} C_{n-1}^{k-1} x^k y^{n-k} + \sum_{k=1}^{n-1} C_{n-1}^k x^k y^{n-k} + C_n^0 x^0 y^n + C_n^n x^n y^0 =$$

$$= \sum_{k=1}^{n-1} (C_{n-1}^{k-1} + C_{n-1}^k) x^k y^{n-k} + C_n^0 x^0 y^n + C_n^n x^n y^0 =$$

$$= C_n^0 x^0 y^n + \sum_{k=1}^{n-1} C_n^k x^k y^{n-k} + C_n^n x^n y^0 = \sum_{k=0}^{n} C_n^k x^k y^{n-k}.$$

3. $\sum\limits_{k=0}^{n} C_n^k = 2^n$.

Д о к а з а т е л ь с т в о следует из предыдущего свойства при $x = y = 1$.

4. $\sum\limits_{k=0}^{n} (-1)^k C_n^k = 0$.

Д о к а з а т е л ь с т в о оставляем читателю в качестве упражнения.

5. $\sum\limits_{i=0}^{k} C_n^i \cdot C_m^{k-i} = C_{n+m}^k$ (тождество Коши).

Д о к а з а т е л ь с т в о. C_{n+m}^k – это число способов выбрать k человек из n мужчин и m женщин. Выбор можно осуществлять следующим образом: сначала выбрать i человек из n мужчин, а затем остальные $k-i$ человек из m женщин. Общее число же способов выбрать k человек равняется $\sum\limits_{i=0}^{k} C_n^i \cdot C_m^{k-i}$.

6. $\sum\limits_{k=1}^{n} kC_n^k = n2^{n-1}$.

Д о к а з а т е л ь с т в о. Построим последовательность из элементов множества $X = \{1, \ldots, n\}$ по следующему правилу: берется подмножество множества X, и выбирая в произвольном порядке элементы подмножества, записываем их в конец последовательности. Сначала рассматриваются все одноэлементные подмножества, затем двухэлементные и т. д. Имеется C_n^k различных подмножеств мощности k, поэтому всего в этой последовательности $\sum\limits_{k=1}^{n} kC_n^k$ чисел.

Например, при $n = 3$ такой последовательностью будет

$$1, 2, 3, 1, 2, 1, 3, 2, 3, 1, 2, 3.$$

Теперь подсчитаем, сколько раз каждое число входит в последовательность. Нетрудно заметить, что каждое число встречается среди членов последовательности, построенных с помощью подмножеств мощности k, ровно C_{n-1}^{k-1} раз, т. е. для всей последовательности эта величина равна $\sum\limits_{k=1}^{n} C_{n-1}^{k-1} = 2^{n-1}$. Остается отметить, что всего чисел n.

7. $\sum\limits_{k=1}^{n} k^2 C_n^k = n(n+1)2^{n-2}$.

Доказательство можно провести, опираясь на доказательство предыдущего свойства, и оставляется в качестве упражнения.

Треугольник Паскаля. На свойстве 1 основывается эффективный способ вычисления значений биномиальных коэффициентов C_n^k при малых n и k, который можно представить в виде треугольной таблицы, известной как треугольник Паскаля:

$$\begin{array}{ccccccccc}
 & & & & 1 & & & & \\
 & & & 1 & & 1 & & & \\
 & & 1 & & 2 & & 1 & & \\
 & 1 & & 3 & & 3 & & 1 & \\
1 & & 4 & & 6 & & 4 & & 1 \\
\ldots & & & & \ldots & & & & \ldots
\end{array}$$

В этом треугольнике каждое число (кроме единиц на боковых сторонах) есть сумма двух чисел, стоящих над ним. Число C_n^k расположено в $(n+1)$-м ряду на $(k+1)$-й позиции.

Полиномиальная теорема. Формула бинома Ньютона имеет следующее обобщение.

Теорема. $(x_1 + \ldots + x_m)^n = \sum\limits_{k_1+\ldots+k_m=n} \dfrac{n!}{k_1! \cdot \ldots \cdot k_m!} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m}$.

Д о к а з а т е л ь с т в о проведем индукцией по m.

Базис индукции. При $m = 2$ имеем формулу бинома Ньютона.

Шаг индукции. Разбив сумму на две части $x_1 + \ldots + x_{m-1}$ и x_m, воспользовавшись формулой бинома Ньютона и предположением индукции, получим

$$(x_1 + \ldots + x_{m-1} + x_m)^n = \sum_{i=0}^{n} C_n^i (x_1 + \ldots + x_{m-1})^i x_m^{n-i} =$$

$$= \sum_{i=0}^{n} C_n^i \Big(\sum_{k'_1+\ldots+k'_{m-1}=i} \frac{i!}{k'_1! \cdot \ldots \cdot k'_{m-1}!} x_1^{k'_1} \cdot \ldots \cdot x_{m-1}^{k'_{m-1}} \Big) x_m^{n-i} =$$

$$= \sum_{i=0}^{n} \sum_{k'_1+\ldots+k'_{m-1}=i} \frac{n!}{i!(n-i)!} \cdot \frac{i!}{k'_1! \cdot \ldots \cdot k'_{m-1}!} x_1^{k'_1} \cdot \ldots \cdot x_{m-1}^{k'_{m-1}} x_m^{n-i} =$$

$$= \sum_{k'_1+\ldots+k'_{m-1}=i} \sum_{i=0}^{n} \frac{n!}{(n-i)! k'_1! \cdot \ldots \cdot k'_{m-1}!} x_1^{k'_1} \cdot \ldots \cdot x_{m-1}^{k'_{m-1}} x_m^{n-i} =$$

$$= \sum_{k_1+\ldots+k_m=n} \frac{n!}{k_1! \cdot \ldots \cdot k_m!} x_1^{k_1} \cdot \ldots \cdot x_m^{k_m}.$$

Теорема доказана.

1.3 Производящие функции. Принцип включения и исключения.

Производящие функции. Пусть даны две последовательности комбинаторных чисел $\{a_i\}$ и функций $\{\varphi_i(x)\}$ $(i = 0, 1, 2 \ldots)$. Рассмотрим ряд $\sum\limits_{i=0}^{\infty} a_i \varphi_i(x)$. При определенных ограничениях данный ряд будет задавать функцию $F(x) = \sum\limits_{i=0}^{\infty} a_i \varphi_i(x)$. Эта функция называется *производящей* функцией для заданной последовательности чисел $\{a_i\}$ относительно заданной последовательности функций $\{\varphi_i(x)\}$. Обычно используются $\varphi_i(x) = x^i$ или $\varphi_i(x) = \dfrac{x^i}{i!}$.

П р и м е р. Из формулы бинома Ньютона при $y = 1$ следует, что $(1+x)^n = \sum\limits_{k=0}^{n} C_n^k x^k$. Функция $(1+x)^n$ является производящей функцией для биномиальных коэффициентов.

Для начала покажем, как с помощью производящих функций можно получить более простое доказательство тождества Коши. Для этого возьмем равенство $(1+x)^{n+m} = (1+x)^n(1+x)^m$. Воспользовавшись формулой бинома Ньютона, имеем

$$\sum_{k=0}^{n+m} C_{n+m}^k x^k = \sum_{k=0}^{n} C_n^k x^k \cdot \sum_{k=0}^{m} C_m^k x^k = \sum_{k=0}^{n+m} (\sum_{i=0}^{k} C_n^i C_m^{k-i}) x^k.$$

Таким образом, $C_{n+m}^k = \sum\limits_{i=0}^{k} C_n^i C_m^{k-i}$.

Применим аппарат производящих функций для доказательства еще одного комбинаторного тождества.

Т е о р е м а 1. $C_{2n}^n = \sum\limits_{k=0}^{n} (C_n^k)^2$.

Д о к а з а т е л ь с т в о. Имеем $(1+x)^{2n} = (1+x)^n(1+x)^n$. Это тождество эквивалентно следующему $\sum\limits_{k=0}^{2n} C_{2n}^k x^k = (\sum\limits_{k=0}^{n} C_n^k x^k)(\sum\limits_{k=0}^{n} C_n^k x^k)$. Приравнивая коэффициенты при x^n, получим

$$C_{2n}^n = \sum_{k=0}^{n} C_n^k C_n^{n-k} = \sum_{k=0}^{n} (C_n^k)^2.$$

Теорема доказана.

Разнообразие приемов, используемых в методе производящих функций, настолько велико, что детальное его изложение выходит за рамки данного курса. Для более глубокого изучения производящих функций подойдет, например, книга [3].

Принцип включения и исключения. Пусть $A_1, \ldots, A_n$ – система подмножеств конечного множества A. Тогда имеет место следующая

Т е о р е м а 2. $|A_1 \cup \ldots \cup A_n| = \sum\limits_{i=1}^{n} |A_i| - \sum\limits_{1 \le i < j \le n} |A_i \cap A_j| + {}$
$+ \sum\limits_{1 \le i < j < k \le n} |A_i \cap A_j \cap A_k| + \ldots + \sum\limits_{1 \le i_1 < i_2 \ldots < i_k \le n} |A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}| + {}$
$+ \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|$.

Д о к а з а т е л ь с т в о проведем индукцией по n.

Базис индукции. При $n = 2$ теорема верна, так как очевидно $|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$.

Шаг индукции. По предположению индукции $|A_1 \cup \ldots \cup A_{n-1}| = \sum\limits_{i=1}^{n-1} |A_i| - \sum\limits_{1 \le i < j \le n-1} |A_i \cap A_j| + \ldots + (-1)^{n-2} |A_1 \cap \ldots \cap A_{n-1}|$. Заметим, что $(A_1 \cup \ldots \cup A_{n-1}) \cap A_n = (A_1 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)$. Далее в силу индуктивного предположения $|(A_1 \cap A_n) \cup \ldots \cup (A_{n-1} \cap A_n)| =$

$$= \sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j \cap A_n| + \ldots +$$

$+(-1)^{n-2} |A_1 \cap \ldots \cap A_{n-1} \cap A_n|$.

Окончательно, $|A_1 \cup \ldots \cup A_n| = |(A_1 \cup \ldots \cup A_{n-1}) \cup A_n| =$

$$= |A_1 \cup \ldots \cup A_{n-1}| + |A_n| - |(A_1 \cup \ldots \cup A_{n-1}) \cap A_n| =$$

$$= (\sum_{i=1}^{n-1} |A_i| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \ldots + (-1)^{n-2} |A_1 \cap \ldots \cap A_{n-1}|) +$$

$$+ |A_n| - (\sum_{i=1}^{n-1} |A_i \cap A_n| - \sum_{1 \le i < j \le n-1} |A_i \cap A_j \cap A_n| + \ldots +$$

$$+ (-1)^{n-2} |A_1 \cap \ldots \cap A_{n-1} \cap A_n|) = (\sum_{i=1}^{n-1} |A_i| + |A_n|) -$$

$$- (\sum_{1 \le i < j \le n-1} |A_i \cap A_j| + \sum_{i=1}^{n-1} |A_i \cap A_n|) + \ldots - |(-1)^{n-2} |A_1 \cap \ldots \cap$$

$$\cap A_{n-1} \cap A_n| = \sum_{i=1}^{n} |A_i| - \sum_{1 \le i < j \le n} |A_i \cap A_j| + \ldots + (-1)^{n-1} |A_1 \cap \ldots \cap A_n|.$$

Теорема доказана.

С л е д с т в и е. $|A \setminus (A_1 \cup \ldots \cup A_n)| = |A| - \sum\limits_{i=1}^{n} |A_i| + \sum\limits_{1 \le i < j \le n} |A_i \cap A_j| - \ldots + (-1)^n |A_1 \cap \ldots \cap A_n|$.

Д о к а з а т е л ь с т в о следует из $|A \setminus (A_1 \cup \ldots \cup A_n)| = |A| - |A_1 \cup \ldots \cup A_n|$.

П р и м е р. Сколько всего натуральных чисел, меньших 100, которые не делятся ни на одно из чисел 3 и 5.

Чисел, меньших 100, имеется 99. Легко заметить, что $[99 : 3] = 33$ числа делятся на 3, $[99 : 5] = 19$ делятся на 5 и $[99 : 15] = 6$ делятся одновременно на 3 и 5. Таким образом, количество чисел, удовлетворяющих нашему условию, равно $99 - (33 + 19) + 6 = 53$.

2 Введение в теорию булевых функций

Булевы функции получили свое название в честь английского математика Джорджа Буля. Долгое время они были востребованы лишь в основаниях математики, однако в настоящее время несомненно булевы функции – основной аппарат для изучения дискретных преобразователей информации. Функционирование современных компьютеров поддается описанию средствами теории булевых функций. Теория кодирования, теория конечных автоматов, теория игр, языки программирования — области применения булевых функций.

2.1 Определение и формы представления булевых функций

Пусть $E = \{0, 1\}$ и $\sigma_i \in E$, где $i \in \{1, \dots, n\}$. Тогда выражение $(\sigma_1, \dots, \sigma_n)$ будем называть *двоичным набором*, а σ_i – *i-ой компонентой* двоичного набора. Обозначим этот двоичный набор через $\tilde{\sigma}$. Далее под набором будем понимать двоичный набор.

Длиной набора $\tilde{\sigma} = (\sigma_1, \dots, \sigma_n)$ называют число n и обозначают через $|\tilde{\sigma}|$. Очевидно, что множество всех наборов длины n есть E^n. Набор, все компоненты которого нули, называют *нулевым* и обозначают через $\tilde{0}$, а набор, все компоненты которого единицы, называют *единичным* и обозначают через $\tilde{1}$.

Л е м м а 1. Число всех наборов длины n равно 2^n.

Д о к а з а т е л ь с т в о проведем индукцией по n.

Базис индукции. При $n = 1$ существует всего два набора (0) и (1), что соответствует формулировке леммы.

Шаг индукции. Разобьем E^n на два множества A_0 и A_1 следующим образом: $A_0 = \{\tilde{\sigma} |\ \tilde{\sigma} \in E^n$ и $\sigma_n = 0\}$ и $A_1 = \{\tilde{\sigma} |\ \tilde{\sigma} \in E^n$ и $\sigma_n = 1\}$. Между A_0 и E^{n-1} установим взаимно однозначное соответствие $\varphi : (\sigma_1, \dots, \sigma_{n-1}, 0) \to (\sigma_1, \dots, \sigma_{n-1})$. Аналогичная ситуация с A_1 и E^{n-1}. Таким образом, $|A_0| = |A_1| = |E^{n-1}|$. По предположению индукции $|E^{n-1}| = 2^{n-1}$. Отсюда следует, что $|E^n| = 2 \cdot 2^{n-1} = 2^n$. Лемма 1 доказана.

Введем на E^n линейный порядок. Будем считать, что наборы $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_m$ $(m = 2^n)$ *упорядочены по натуральному порядку*, если для всех $s \in \{1, \ldots, m\}$ выполняется условие $s = 1 + \sum\limits_{i=1}^{n} 2^{n-i} \cdot \sigma_{s,i}$, где $\tilde{\sigma}_s = (\sigma_{s,1}, \ldots, \sigma_{s,n})$.

Заметим, что наборы $\tilde{\sigma}_1, \ldots, \tilde{\sigma}_m$ $(m = 2^n)$, упорядоченные по натуральному порядку, представляют натуральные числа $0, \ldots, 2^n - 1$, записанные в двоичном исчислении.

Функция $f : E^n \to E$ называется *булевой* или *функцией алгебры логики*. При этом n называется *размерностью* булевой функции f и обозначается через $dim f$. Множество всех булевых функций обозначается через F, размерности n – через F^n. Далее на протяжении всей главы булеву функцию будем называть просто функцией.

П р и м е р ы.

1. Функции размерности нуль – это константы 0 и 1, называемые соответственно *нулевой* и *единичной* функциями.

2. Функций размерности один всего четыре:

$f_1(0) = 0, \quad f_2(0) = 1, \quad f_3(0) = 0, \quad f_4(0) = 1,$
$f_1(1) = 0, \quad f_2(1) = 1, \quad f_3(1) = 1, \quad f_4(1) = 0.$

Функцию $f_3(x)$ называют *тождественной*, а $f_4(x)$ – *отрицанием*, и пишут соответственно $f_3(x) = x$, $f_4(x) = \bar{x}$. Тождественную функцию будем также обозначать через e.

Функция от n переменных может быть задана *таблицей*, в которой перечислены всевозможные наборы длины n по натуральному порядку и для каждого набора указано значение функции на этом наборе (табл. 1).

Таблица 1.

x_1	x_2	$\ldots$	x_n	$f(x_1, x_2, \ldots, x_n)$
0	0	$\ldots$	0	$f(0, 0, \ldots, 0)$
0	0	$\ldots$	1	$f(0, 0, \ldots, 1)$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	1	$\ldots$	0	$f(1, 1, \ldots, 0)$
1	1	$\ldots$	1	$f(1, 1, \ldots, 1)$

Остаточными функциями от функции $f(x_1, \ldots, x_n)$ по переменной x_i называются функции размерности на единицу меньше, чем размерность f, обозначаемые и определяемые следующим образом:

$$f_{x_i}^{\sigma_i}(\tau_1, \ldots, \tau_{n-1}) = f(\tau_1, \ldots, \tau_{i-1}, \tau_{i+1}, \ldots, \tau_{n-1})$$

для любого набора $(\tau_1, \ldots, \tau_{n-1}) \in E^{n-1}$.

Индуктивно понятие остаточной функции распространяется на множество переменных $x_{i_1}, \ldots, x_{i_s}$ по набору $\sigma_{i_1}, \ldots, \sigma_{i_s}$ $(s \leq n)$: $f^{\sigma_{i_1},\ldots,\sigma_{i_s}}_{x_{i_1},\ldots,x_{i_s}} = (f^{\sigma_{i_1},\ldots,\sigma_{i_{s-1}}}_{x_{i_1},\ldots,x_{i_{s-1}}})^{\sigma_{i_s}}_{x_{i_s}}$, где s называется *порядком* остаточной функции.

Переменная x_i функции $f(x_1, \ldots, x_n)$ называется *существенной*, если существуют значения $\sigma_1, \ldots, \sigma_{i-1}, \sigma_{i+1}, \ldots, \sigma_n$ для переменных $x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n$ такие, что $f(\sigma_1, \ldots, \sigma_{i-1}, 0, \sigma_{i+1}, \ldots, \sigma_n) \neq$ $\neq f(\sigma_1, \ldots, \sigma_{i-1}, 1, \sigma_{i+1}, \ldots, \sigma_n)$. В противном случае она называется *фиктивной*.

Пусть для функции $f(x_1, \ldots, x_n)$ переменная x_i является фиктивной. Возьмем таблицу, задающую $f(x_1, \ldots, x_n)$, вычеркнем из нее все строки, где в двоичных наборах на i-ой позиции встречается 1, а также столбец, отвечающий за x_i. Полученная таблица определяет некоторую булеву функцию $g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$. Говорят, что функция $g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ получается из функции $f(x_1, \ldots, x_n)$ путем удаления фиктивной переменной x_i, а функция $f(x_1, \ldots, x_n)$ получается из $g(x_1, \ldots, x_{i-1}, x_{i+1}, \ldots, x_n)$ путем введения фиктивной переменной x_i.

Функции f_1 и f_2 называются *равными*, если f_1 можно получить из f_2 путем введения и (или) удаления фиктивных переменных.

Далее рассмотрим векторное представление функций. Вектор $\tilde{\sigma}$ *представляет* функцию $f(\tilde{x})$, если $|\tilde{\sigma}| = 2^{|\tilde{x}|}$ и $\sigma_i = f(\tilde{\alpha}_i)$, где $\tilde{\alpha}_i$ является i-м набором при натуральном упорядочении наборов. Записываем так: $f(\tilde{x}) = \tilde{\sigma}$.

Для функции $f(\tilde{x})$ *нулевым характеристическим* множеством называется множество $H_0(f) = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $f^{\tilde{\sigma}}_{\tilde{x}} = 0\}$, а *единичным характеристическим* множеством – $H_1(f) = \{\tilde{\sigma} | \tilde{\sigma} \in E^n$ и $f^{\tilde{\sigma}}_{\tilde{x}} = 1\}$.

П р и м е р. Пусть $f = (10000010)$. Тогда $H_1(f) = \{(000), (110)\}$ и $H_0(f) = \{(001), (010), (011), (100), (101), (111)\}$.

Введем названия и обозначения для часто используемых функций размерности 2.

$f_1 = (0001)$ - *конъюнкция*, $f_1(x, y) = x \cdot y$;

$f_2 = (0111)$ - *дизъюнкция*, $f_2(x, y) = x \vee y$;

$f_3 = (0110)$ - *сложение по* mod 2, $f_3(x, y) = x \oplus y$;

$f_4 = (1101)$ - *импликация*, $f_4(x, y) = x \rightarrow y$;

$f_5 = (1001)$ - *эквивалентность*, $f_5(x, y) = x \leftrightarrow y$;

$f_6 = (1110)$ - *штрих Шеффера*, $f_6(x,y) = x|y$;
$f_7 = (1000)$ - *стрелка Пирса*, $f_7(x,y) = x \downarrow y$.

Л е м м а 2. Число функций размерности n равно 2^{2^n}.

Д о к а з а т е л ь с т в о следует из векторного представления булевых функций и леммы 1.

2.2 Представление булевых функций термами

Представление функций термами (формулами) является наиболее широко используемым в теории булевых функций.

Пусть $B \subseteq F$ и X – некоторое множество символов, называемых переменными. Индукцией определим понятие *терма над* B от множества переменных X:

1) переменная $x \in X$ есть терм;

2) если $f \in B$, $dim f = m$ и $\Phi_1, \ldots, \Phi_m$ – термы, то $f(\Phi_1, \ldots, \Phi_m)$ есть терм.

Для графического равенства термов Φ и Ψ используем обозначение $\Phi \equiv \Psi$.

С определением терма связано несколько сопутствующих понятий: *подтерм* терма Φ, глубина $d(\Phi)$, *множество* $\chi(\Phi)$ *переменных* терма Φ.

1) если $\Phi \equiv x$, то единственным подтермом терма Φ является x; $d(\Phi) = 0$; $\chi(\Phi) = \{x\}$;

2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$, то подтермами Φ являются сам терм Φ и все подтермы термов $\Phi_1, \ldots, \Phi_m$; $d(f(\Phi_1, \ldots, \Phi_m)) = 1 + \max\limits_{1 \leq i \leq m} d(\Phi_i)$; $\chi(\Phi) = \chi(\Phi_1) \cup \ldots \cup \chi(\Phi_m)$;

Если $\tilde{x} = \chi(\Phi)$, то будем использовать запись $\Phi(\tilde{x})$.

Множество B называется *базисным множеством*, а функции из B *базисными функциями*. При этом говорят, что терм является *термом над базисным множеством* B.

Запись $\Phi[f_1, \ldots, f_k]$ используем для того, чтобы показать, какие функциональные символы входят в построение терма Φ. Это означает, что в Φ есть подтермы вида $f_i(\Phi_{i_1}, \ldots, \Phi_{i_s})$, $i \in \{1, \ldots, k\}$ и $f_i \neq f_j$ для $i \neq j$, а все остальные подтермы являются переменными.

Если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$, то f – внешняя функция терма Φ.

Определим *значение терма* Φ *при заданных значениях переменных* $\tilde{x}$, где $\chi(\Phi) \subseteq \tilde{x}$:

1) если Φ – переменная, то значение Φ совпадает со значением этой переменной;

2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$ и значения термов $\Phi_1, \ldots, \Phi_m$ есть $\sigma_1, \ldots, \sigma_m$ соответственно, то значение терма Φ есть $f(\sigma_1, \ldots, \sigma_m)$.

Функция g *представима термом* $\Phi(x_1, \ldots, x_n)$, если $dimg = n$ и для любого набора $\alpha_1, \ldots, \alpha_n$, задающего значения переменных, значение терма $\Phi(x_1, \ldots, x_n)$ при этом значении переменных совпадает с $g(\alpha_1, \ldots, \alpha_n)$.

Если g представима термом $\Phi[f_1, \ldots, f_n]$, то говорят, что g есть суперпозиция функций $f_1, \ldots, f_n$.

П р и м е р. Пусть даны функции $f_1 = (0001)$, $f_2 = (0111)$ и терм $\Phi(x_1, x_2, x_3) \equiv f_1(x_1, f_2(x_2, x_3))$. Тогда $f = (00000111)$ – функция, представимая термом Φ.

Пусть Φ, Ψ – термы и $\tilde{x} = \chi(\Phi) \cup \chi(\Psi)$. Если при любых значениях переменных $\tilde{x}$ значения термов Φ и Ψ совпадают, то такие термы называются *эквивалентными* и обозначаются $\Phi = \Psi$. Очевидно, что для эквивалентных термов представимые ими функции равны.

Введем обозначение $\Phi^{\Psi}_{\Phi_1}$ для терма, получаемого из Φ заменой подтерма Φ_1 на терм Ψ. Будем считать, что если Φ_1 не является подтермом Φ, то $\Phi^{\Psi}_{\Phi_1} \equiv \Phi$.

Л е м м а 1. (о замене) Пусть Φ, Ψ – термы и Υ подтерм Φ. Тогда если $\Upsilon = \Psi$, то $\Phi = \Phi^{\Psi}_{\Upsilon}$.

Д о к а з а т е л ь с т в о проведем индукцией по глубине терма Φ.

Базис индукции. Пусть $d(\Phi) = 0$. Тогда Φ является переменной, и у него единственный подтерм – сама переменная, то есть $\Phi \equiv \Upsilon$. Поэтому $\Phi = \Phi^{\Psi}_{\Upsilon}$.

Шаг индукции. Пусть $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)(\tilde{x})$. Тогда Υ – это либо сам Φ, либо подтерм некоторого Φ_i. В первом случае доказательство аналогично доказательству базиса индукции. Во втором случае, так как $d(\Phi_i) < d(\Phi)$, то по предположению индукции $\Phi_i = \Psi_i$, где $\Psi_i \equiv$ $\equiv (\Phi_i)^{\Psi}_{\Upsilon}$. Тогда для любого набора $\tilde{\sigma}$ получаем, что

$f((\Phi_1)^{\tilde{\sigma}}_{\tilde{x}}, \ldots, (\Phi_i)^{\tilde{\sigma}}_{\tilde{x}}, \ldots, (\Phi_m)^{\tilde{\sigma}}_{\tilde{x}}) = f((\Phi_1)^{\tilde{\sigma}}_{\tilde{x}}, \ldots, (\Psi_i)^{\tilde{\sigma}}_{\tilde{x}}, \ldots, (\Phi_m)^{\tilde{\sigma}}_{\tilde{x}})$, поэтому $f(\Phi_1, \ldots, \Phi_i, \ldots, \Phi_m) = f(\Phi_1, \ldots, \Phi_{i-1}, \Psi_i, \Phi_{i+1}, \ldots, \Phi_m)$. Отсюда $\Phi = \Phi^{\Psi_i}_{\Phi_i} \equiv \Phi^{\Psi_i}_{(\Phi_i)^{\Psi}_{\Upsilon}} \equiv \Phi^{\Psi}_{\Upsilon}$. Лемма 1 доказана.

Л е м м а 2. (о подстановке) Пусть $\Phi(\tilde{x})$, $\Psi(\tilde{y})$, Υ – термы. Если $\Phi = \Psi$, то $\Phi_x^\Upsilon = \Psi_x^\Upsilon$.

Д о к а з а т е л ь с т в о проведем индукцией по глубине терма Υ.

Базис индукции. Пусть $d(\Upsilon) = 0$. Тогда $\Upsilon \equiv z$ и $\Phi_x^\Upsilon = \Psi_x^\Upsilon$, так как только изменилось имя переменной.

Шаг индукции. Пусть $\Upsilon(\tilde{z}) \equiv f(\Phi_1, \ldots, \Phi_m)$. Очевидно, имеет место $\Phi_x^\Upsilon \equiv (\Phi_x^{f(u_1,\ldots,u_m)})_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m}$ и $\Psi_x^\Upsilon \equiv (\Psi_x^{f(u_1,\ldots,u_m)})_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m}$.

Так как $d(f(u_1, \ldots, u_m)) < d(f(\Phi_1, \ldots, \Phi_m))$, то по предположению индукции $\Phi_x^{f(u_1,\ldots,u_m)} = \Psi_x^{f(u_1,\ldots,u_m)}$. Затем в силу того, что $d(\Phi_i) < d(f(\Phi_1, \ldots, \Phi_m))$, применив m раз предположение индукции, получим $(\Phi_x^{f(u_1,\ldots,u_m)})_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m} = (\Psi_x^{f(u_1,\ldots,u_m)})_{u_1,\ldots,u_m}^{\Phi_1,\ldots,\Phi_m}$, то есть $\Phi_x^\Upsilon = \Psi_x^\Upsilon$. Лемма 2 доказана.

Функции $f(x_1, \ldots, x_n)$ и $g(x_1, \ldots, x_n)$ называются *двойственными*, если $f(x_1, \ldots, x_n) = \bar{g}(\bar{x}_1, \ldots, \bar{x}_n)$. Для двойственных функций введем обозначения $g = f^*$ и $f = g^*$. Очевидно, что $(f^*)^* = f$.

Определим терм Φ^* *двойственный* к терму Φ:

1) если $\Phi \equiv x$, то $\Phi^* \equiv x$;

2) если $\Phi \equiv f(\Phi_1, \ldots, \Phi_m)$, то $\Phi^* \equiv f^*(\Phi_1^*, \ldots, \Phi_m^*)$.

Очевидно, если $\Phi[f_1, \ldots, f_k]$, то $\Phi^* \equiv \Phi[f_1^*, \ldots, f_k^*]$.

Т е о р е м а 1. Пусть f представима термом Φ, тогда f^* представима термом Φ^*.

Д о к а з а т е л ь с т в о проведем индукцией по глубине терма Φ.

Базис индукции. Пусть $d(\Phi) = 0$. Тогда $\Phi \equiv x$ и $f = x$. Отсюда следует, что $f^* = \bar{\bar{x}} = x$ представима термом $\Phi^* \equiv \Phi$.

Шаг индукции. Пусть $\Phi \equiv g(\Phi_1, \ldots, \Phi_m)$. В силу того, что $d(\Phi_i) < < d(\Phi)$, используя предположение индукции для термов $\Phi_1, \ldots, \Phi_m$, получим $f^* = \bar{g}(\overline{\Phi_1, \ldots, \Phi_m})(\bar{x}_1, \ldots, \bar{x}_k) = \bar{g}(\bar{\bar{\Phi}}_1, \ldots, \bar{\bar{\Phi}}_m)(\bar{x}_1, \ldots, \bar{x}_k) =$ $= \bar{g}(\overline{\bar{\Phi}_1(\bar{x}_1, \ldots, \bar{x}_k)}, \ldots, \overline{\bar{\Phi}_m(\bar{x}_1, \ldots, \bar{x}_k)}) = \bar{g}(\bar{g}_1^*, \ldots, \bar{g}_m^*) =$ $= g^*(g_1^*, \ldots, g_m^*) = g^*(\Phi_1^*, \ldots, \Phi_m^*) = \Phi^*$, где g_i представима термом Φ_i, $i = 1, \ldots, m$. Теорема 1 доказана.

С л е д с т в и е. (принцип двойственности) Пусть Φ и Ψ – термы. Тогда если $\Phi = \Psi$, то $\Phi^* = \Psi^*$.

Д о к а з а т е л ь с т в о. Из $\Phi = \Psi$ следует, что $f = g$, где f и g представимы Φ и Ψ соответственно. Это означает, что $f^* = g^*$.

По теореме 1 f^* и g^* представимы Φ^* и Ψ^*, т. е. $\Phi^* = \Psi^*$. Следствие доказано.

Парами двойственных функций являются

$$\begin{array}{cc} 0 & 1 \\ e & e \\ - & - \\ \cdot & \vee \\ \oplus & \leftrightarrow \\ | & \downarrow \end{array}$$

Для упрощения записи термов (уменьшения числа скобок) договоримся о приоритете функций. Итак, установим следующий порядок: $-$, $\cdot$, $\vee$, $\oplus$ и все остальные функции. Символ «$\cdot$» будем часто опускать.

Т е о р е м а 2. Выполняются следующие тождества:

1) $x \cdot y = y \cdot x$; $x \vee y = y \vee x$; $x \oplus y = y \oplus x$;

2) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$; $x \vee (y \vee z) = (x \vee y) \vee z$; $x \oplus (y \oplus z) = (x \oplus y) \oplus z$;

3) $1 \cdot x = x$; $0 \cdot x = x$; $1 \vee x = 1$; $0 \vee x = x$; $1 \oplus x = \bar{x}$;

4) $x \cdot x = x$; $x \vee x = x$; $x \oplus x = 0$;

5) $\bar{\bar{x}} = x$;

6) $\overline{x \cdot y} = \bar{x} \vee \bar{y}$; $\overline{x \vee y} = \bar{x} \cdot \bar{y}$; $\overline{x \oplus y} = \bar{x} \oplus y = x \oplus y \oplus 1$;

7) $x \cdot (y \vee z) = x \cdot y \vee x \cdot z$; $x \vee (y \cdot z) = (x \vee y) \cdot (x \vee z)$; $x \cdot (y \oplus z) = x \cdot y \oplus x \cdot z$; $x \vee (y \oplus z) = x \vee y \oplus x \vee z \oplus x$; $x \vee (y \oplus z \oplus u) = x \vee y \oplus x \vee z \oplus x \vee u$;

8) $x \oplus y = \bar{x} \cdot y \vee x \cdot \bar{y}$; $x \leftrightarrow y = x \cdot y \vee \bar{x} \cdot \bar{y} = \bar{x} \oplus y$; $x \to y = \bar{x} \vee y$; $x \vee y = x \cdot y \oplus x \oplus y$;

9) $x \cdot \bar{x} = 0$; $x \vee \bar{x} = 1$; $x \oplus \bar{x} = 1$.

Д о к а з а т е л ь с т в о. Непосредственно проверяется, что термы в обеих частях тождеств эквивалентны.

В сочетании лемм о замене и подстановке, а также полученных тождеств, можно доказывать эквивалентность термов над базисным множеством F^2, не пользуясь определением эквивалентности.

П р и м е р.

1) $x_1 \vee x_1 x_2 = x_1 \cdot 1 \vee x_1 x_2 = x_1(1 \vee x_2) = x_1 \cdot 1 = x_1$;

2) $x_1 x_2 \vee \bar{x}_1 x_2 = (x_1 \vee \bar{x}_1) x_2 = 1 \cdot x_2 = x_2$.

2.3 Разложение булевых функций по переменным. Совершенные нормальные формы. Полином Жегалкина

Будем использовать следующие обозначения:
$\bigvee\limits_{i=1}^{n} x_i = x_1 \vee \ldots \vee x_n$, $\mathop{\&}\limits_{i=1}^{n} x_i = x_1 \cdot \ldots \cdot x_n$, $\sum\limits_{i=1}^{n} x_i = x_1 \oplus \ldots \oplus x_n$,

$$x^\sigma = \begin{cases} x, \text{ если } \sigma = 1; \\ \bar{x}, \text{ если } \sigma = 0. \end{cases}$$

Очевидно, что $x^\sigma = 1$ тогда и только тогда, когда $x = \sigma$.

Т е о р е м а 1. Любую функцию $f(x_1, \ldots, x_n)$ при любом m $(1 \le m \le n)$ можно представить в следующем виде

$f(x_1, \ldots, x_n) = \bigvee\limits_{(\sigma_1, \ldots, \sigma_m)} x_1^{\sigma_1} \cdot \ldots \cdot x_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, x_{m+1}, \ldots, x_n)$,

где дизъюнкция берется по всевозможным наборам значений переменных $x_1, \ldots, x_m$.

Д о к а з а т е л ь с т в о. Возьмем произвольный набор $(\alpha_1, \ldots, \alpha_n)$ и покажем, что левая и правая части принимают на нем одно и то же значение.

$f(\alpha_1, \ldots, \alpha_n) = \bigvee\limits_{(\sigma_1, \ldots, \sigma_m)} \alpha_1^{\sigma_1} \cdot \ldots \cdot \alpha_m^{\sigma_m} \cdot f(\sigma_1, \ldots, \sigma_m, \alpha_{m+1}, \ldots, \alpha_n) =$
$= \alpha_1^{\alpha_1} \cdot \ldots \cdot \alpha_m^{\alpha_m} \cdot f(\alpha_1, \ldots, \alpha_m, \alpha_{m+1}, \ldots, \alpha_n) = f(\alpha_1, \ldots, \alpha_n)$.

Теорема 1 доказана.

В качестве следствий из теоремы получаем два специальных случая разложения.

1) Разложение по переменной (Шеннона):

$$f(x_1, \ldots, x_n) = x_i f_{x_i}^1 \vee \bar{x}_i f_{x_i}^0.$$

2) Разложение по всем переменным:

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

Если $f(x_1, \ldots, x_n) \neq 0$, то $f(x_1, \ldots, x_n) = \bigvee\limits_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}$.

Это разложение называется *совершенной дизъюнктивной нормальной формой* (СДНФ). Здесь терм вида $x_1^{\sigma_{i_1}} \cdot \ldots \cdot x_n^{\sigma_{i_n}}$ называется *полной элементарной конъюнкцией.*

П р и м е р. Пусть $f(x_1, x_2) = (1001)$. Тогда СДНФ для функции f имеет следующий вид: $f(x_1, x_2) = \bar{x}_1\bar{x}_2 \vee x_1\bar{x}_2 \vee x_1x_2$.

Т е о р е м а 2. Любая функция может быть представлена термом над $B = \{-, \cdot, \vee\}$.

Д о к а з а т е л ь с т в о. Если $f(x_1, \ldots, x_n) = 0$, то $f(x_1, \ldots, x_n) = x_1 \cdot \bar{x}_1$. Иначе f представима в виде СДНФ. Теорема 2 доказана.

Т е о р е м а 3. Любая ненулевая функция имеет единственную СДНФ (с точностью до перестановки полных элементарных конъюнкций).

Д о к а з а т е л ь с т в о следует из того, что любая функция однозначно определяется своим единичным характеристическим множеством.

Запишем СДНФ для функции $\bar{f}(x_1, \ldots, x_n)$ и рассмотрим ее отрицание.

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

$$\overline{\overline{f}}(x_1, \ldots, x_n) = \overline{\bigvee_{\substack{(\sigma_1, \ldots, \sigma_n) \\ \bar{f}(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}} = \mathop{\&}_{\substack{(\sigma_1, \ldots, \sigma_n) \\ \bar{f}(\sigma_1, \ldots, \sigma_n) = 1}} (x_1^{\bar{\sigma}_1} \vee \ldots \vee x_n^{\bar{\sigma}_n})$$

согласно закону де Моргана. Отсюда в силу $\overline{\overline{f}} = f$ имеем

$$f(x_1, \ldots, x_n) = \mathop{\&}_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 0}} (x_1^{\bar{\sigma}_1} \vee \ldots \vee x_n^{\bar{\sigma}_n}).$$

Это разложение называется *совершенной конъюнктивной нормальной формой* (СКНФ). Здесь терм вида $x_1^{\sigma_{i_1}} \vee \ldots \vee x_n^{\sigma_{i_n}}$ называется *полной элементарной дизъюнкцией*.

П р и м е р. Пусть $f(x_1, x_2) = (0001)$. Тогда СКНФ для функции f имеет следующий вид: $f(x_1, x_2) = (x_1 \vee x_2)(x_1 \vee \bar{x}_2)(\bar{x}_1 \vee x_2)$.

Т е о р е м а 4. Любая неединичная функция имеет единственную СКНФ (с точностью до перестановки полных элементарных дизъюнкций).

Д о к а з а т е л ь с т в о следует из того, что любая функция однозначно определяется своим нулевым характеристическим множеством.

Рассмотрим СДНФ функции $f(x_1, \ldots, x_n) \neq 0$. На каждом наборе $(\alpha_1, \ldots, \alpha_n)$ в 1 обращается не более одной из полных элементарных конъюнкций, входящих в СДНФ. Поэтому внешняя функция $\vee$ может быть заменена на $\oplus$. Тогда

$$f(x_1, \ldots, x_n) = \sum_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} x_1^{\sigma_1} \cdot \ldots \cdot x_n^{\sigma_n}.$$

Это разложение называется *совершенной полиномиальной конъюнктивно-нормальной формой* (СПКНФ).

Т е о р е м а 5. Любая ненулевая функция имеет единственную СПКНФ (с точностью до перестановки полных элементарных конъюнкций).

Д о к а з а т е л ь с т в о аналогично доказательству теоремы 3.

Поскольку $x \oplus \bar{\sigma} = x^{\sigma}$, то

$$f(x_1, \ldots, x_n) = \sum_{\substack{(\sigma_1, \ldots, \sigma_n) \\ f(\sigma_1, \ldots, \sigma_n) = 1}} (x_1 \oplus \bar{\sigma}_1) \cdot \ldots \cdot (x_n \oplus \bar{\sigma}_n).$$

Раскрыв скобки и приведя подобные члены по правилу $\Phi \oplus \Phi = 0$, придем к представлению функции в виде полинома по mod 2:

$$f(x_1, \ldots, x_n) = \sum_{i_1, \ldots, i_s} c_{i_1, \ldots, i_s} x_{i_1} \cdot \ldots \cdot x_{i_s},$$

где $c_{i_1, \ldots, i_s} \in E$, $0 \leq s \leq n$ и $i_j \in \{1, \ldots, n\}$. Это разложение называется *полиномом Жегалкина*.

Т е о р е м а 6. Любая функция представима в виде полинома Жегалкина единственным образом.

Д о к а з а т е л ь с т в о. Существование полинома для любой функции очевидно (для функции, равной 0, в качестве полинома берется 0).

Подсчитаем количество полиномов от переменных $x_1, \ldots, x_n$. Число различных конъюнкций $x_{i_1} \cdot \ldots \cdot x_{i_s}$ совпадает с числом подмножеств множества $\{1, \ldots, n\}$ и равно $\sum\limits_{s=0}^{n} C_n^s = 2^n$. Перед каждой конъюнкцией стоит коэффициент 0 или 1, поэтому различных полиномов 2^{2^n}. Всего же функций от n переменных также 2^{2^n}, то есть любой функции соответствует ровно один полином, иначе если найдется функция, которая представима двумя полиномами, то для какой-то функции полинома просто не хватит, что невозможно. Теорема 6 доказана.

2.4 Некоторые замкнутые множества булевых функций

Замыканием множества функций T называется множество всех функций, представимых термами над T. Замыкание множества T обозначается через $[T]$.

Множество функций T называется *замкнутым*, если $T = [T]$.

Л е м м а 1. Для любого множества T выполняется:

1) $T \subseteq [T]$;

2) $[T] = [[T]]$;

3) если $T \subseteq R$, то $[T] \subseteq [R]$.

Д о к а з а т е л ь с т в о следует непосредственно из определения замкнутости.

Множество B называется *базисом* для замкнутого множества функций T, если $[B] = T$. В этом случае также говорят, что B *полно в множестве* T. При $T = F$ говорят, что B – *полное множество.*

Т е о р е м а 1. (о сводимости базисов) Пусть R – базис для замкнутого множества T. Если $R \subseteq [B]$ и $B \subseteq T$, то B – базис для T.

Д о к а з а т е л ь с т в о. Так как R – базис для T, то $[R] = T$. По лемме 1 из $R \subseteq [B]$ следует, что $[R] \subseteq [B]$, то есть $T \subseteq [B]$. Также в силу того, что $B \subseteq T$ имеем $[B] \subseteq [T] = T$. Таким образом, $T = [B]$. Теорема 1 доказана.

С л е д с т в и е. Пусть $B_1 = \{f_1, \ldots, f_n\}$, $B_2 = \{g_1, \ldots, g_k\}$. Если для любого i функция f_i представима термом над B_2, и B_1 – полное множество, то B_2 также полно.

Таким образом, вопрос о полноте множеств можно решать с помощью уже известных полных множеств.

П р и м е р ы.

1) $B_0 = \{-, \cdot, \vee\}$ полно по теореме 2 из п. 2.3;

2) $B_1 = \{-, \cdot, \oplus\}$ и $B_2 = \{\cdot, \oplus, 1\}$ полны в силу теорем 5 и 6 из п. 2.3;

3) $B_3 = \{-, \cdot\}$, $B_4 = \{-, \vee\}$, $B_5 = \{|\}$, $B_6 = \{\downarrow\}$, $B_7 = \{\rightarrow, 0\}$ полны в силу теоремы 1 и следующих эквивалентностей: $x \vee y = \overline{\bar{x} \cdot \bar{y}}$, $\bar{x} = x|x$, $x \cdot y = (x|y)|(x|y)$, $\bar{x} = x \downarrow y$, $x \vee y = (x \downarrow y) \downarrow (x \downarrow y)$, $\bar{x} = x \rightarrow 0$, $x \vee y = (x \rightarrow 0) \rightarrow y$.

Функция $f(\tilde{x})$ называется *сохраняющей нуль*, если $f_{\tilde{x}}^{\tilde{0}} = 0$, и *сохраняющей единицу*, если $f_{\tilde{x}}^{\tilde{1}} = 1$.

Т е о р е м а 2. Множество F_0 всех функций, сохраняющих нуль, является замкнутым, и множество F_1 всех функций, сохраняющих единицу, также является замкнутым.

Д о к а з а т е л ь с т в о. Докажем замкнутость F_0 (для F_1 аналогично). Для этого покажем, что суперпозиция функций из F_0 принадлежит F_0.

Пусть функции $f, g_1, \ldots, g_n \in F_0$ и $dimf = n$. Тогда

$$f(g_1(\tilde{0}), g_2(\tilde{0}), \ldots, g_n(\tilde{0})) = f(0, 0, \ldots, 0) = 0.$$

Теорема 2 доказана.

Набор $\tilde{\sigma} \leq \tilde{\tau}$, если $\sigma_i \leq \tau_i$ для любого $i \in \{1, \ldots n\}$.

Функция $f(\tilde{x})$ называется *монотонной*, если для любых наборов $\tilde{\sigma}$ и $\tilde{\tau}$ из $\tilde{\sigma} \leq \tilde{\tau}$ следует, что $f(\tilde{\sigma}) \leq f(\tilde{\tau})$. Например, функции $\cdot, \vee$ являются монотонными, а $-, \oplus$ – немонотонные.

Т е о р е м а 3. Множество M всех монотонных функций является замкнутым.

Д о к а з а т е л ь с т в о. Для доказательства замкнутости M нужно показать, что суперпозиция монотонных функций есть функция монотонная.

Пусть функции $f, g_1, \ldots, g_n \in M$ и $dimf = n$. Тогда если $\tilde{\sigma} \leq \tilde{\tau}$, то $g_i(\tilde{\sigma}) \leq g_i(\tilde{\tau})$. Поэтому $(g_1(\tilde{\sigma}), \ldots, g_n(\tilde{\sigma})) \leq (g_1(\tilde{\tau}), \ldots, g_n(\tilde{\tau}))$. В силу монотонности f имеем $f(g_1(\tilde{\sigma}), \ldots, g_n(\tilde{\sigma})) \leq f(g_1(\tilde{\tau}), \ldots, g_n(\tilde{\tau}))$, то есть $f(g_1, \ldots, g_n) \in M$. Теорема 3 доказана.

Функция $f(\tilde{x})$ называется *самодвойственной*, если $f^* = f$.

Т е о р е м а 4. Множество S всех самодвойственных функций является замкнутым.

Д о к а з а т е л ь с т в о. Для доказательства замкнутости S нужно показать, что суперпозиция самодвойственных функций есть функция самодвойственная.

Пусть $f, g_1, \ldots, g_n \in S$, $dimf = n$ и $h(\tilde{x}) = f(g_1(\tilde{x}), \ldots, g_n(\tilde{x}))$. Тогда $h^*(\tilde{x}) = \bar{h}(\bar{\tilde{x}}) = \bar{f}(g_1(\bar{\tilde{x}}), \ldots, g_n(\bar{\tilde{x}})) = f(g_1(\tilde{x}), \ldots, g_n(\tilde{x})) = h(\tilde{x})$.

Теорема 4 доказана.

Функция $f(\tilde{x})$ называется *линейной*, если она представима полиномом Жегалкина степени не выше первой (содержит конъюнкции длины не более 1), то есть $f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n$. Легко заметить, что коэффициенты c_i связаны со значениями функции следующим образом:

$c_0 = f(0, 0, \ldots, 0)$,
$c_1 = f(0, 0, \ldots, 0) \oplus f(1, 0, 0, \ldots, 0)$,
$c_2 = f(0, 0, \ldots, 0) \oplus f(0, 1, 0, \ldots, 0)$,
— — — — — — — — — — — — — — —
$c_n = f(0, 0, \ldots, 0) \oplus f(0, 0, 0, \ldots, 1)$.

На основе этого для любой функции можно определить, является она линейной или нет. По приведенным формулам нужно вычислить коэффициенты $c_0, c_1, \ldots, c_n$ и проверить, реализуется ли данная функция полиномом $c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n$.

Производной функции f по переменной x называется функция $f'_x = f^0_x \oplus f^1_x$.

Л е м м а 2. Функция f линейна тогда и только тогда, когда для любой переменной $x \in \chi(f)$ производная f'_x является константой.

Д о к а з а т е л ь с т в о. Необходимость. Функция f линейна, то есть $f(x_1, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n$. В силу симметричности переменных достаточно рассмотреть производную по любой переменной. Итак, $f'_{x_1} = c_1$.

Достаточность. От противного. Пусть f нелинейна. Тогда в полиноме Жегалкина $p(x_1, \ldots, x_n)$ для функции f найдется конъюнкция, содержащая не менее двух переменных. Без ограничения общности можно считать, что среди них есть x_1 и x_2. Таким образом, $p(x_1, \ldots, x_n) = x_1 x_2 p_1(x_3, \ldots, x_n) \oplus x_1 p_2(x_3, \ldots, x_n) \oplus x_2 p_3(x_3, \ldots, x_n) \oplus$ $\oplus p_4(x_3, \ldots, x_n)$. Поскольку $p_1(x_3, \ldots, x_n) \neq 0$, $f'_{x_1} = x_2 p_1(x_3, \ldots, x_n) \oplus$ $\oplus p_2(x_3, \ldots, x_n)$ неравна константе. Противоречие. Лемма 2 доказана.

Т е о р е м а 5. Множество L всех линейных функций является замкнутым.

Д о к а з а т е л ь с т в о. Для доказательства замкнутости L нужно показать, что суперпозиция линейных функций есть функция линейная. Пусть $f, g_1, \ldots, g_n \in L$ и $dim f = n$. Тогда

$f = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_n x_n$,
$g_1 = c^1_0 \oplus c^1_1 y_1 \oplus \ldots \oplus c^1_k y_k$,
— — — — — — — — — — —

$g_n = c_0^n \oplus c_1^n y_1 \oplus \ldots \oplus c_k^n y_k$.

Таким образом, $f(g_1(x_1, \ldots, x_k), \ldots, g_n(x_1, \ldots, x_k)) = c_0 \oplus c_1(c_0^1 \oplus \oplus c_1^1 y_1 \oplus \ldots \oplus c_k^1 y_k) \oplus \ldots \oplus c_n(c_0^n \oplus c_1^n y_1 \oplus \ldots \oplus c_k^n y_k) = d_0 \oplus d_1 y_1 \oplus \ldots \oplus d_k y_k$. Теорема 5 доказана.

Для того, чтобы показать, что все 5 замкнутых множеств попарно различны, непусты и не совпадают с F, достаточно рассмотреть следующую таблицу.

Таблица 2.

	F_0	F_1	M	S	L
0	+	−	+	−	+
1	−	+	+	−	+
$\bar{x}$	−	−	−	+	+
$x \cdot y$	+	+	+	−	−

2.5 Критерий полноты множества булевых функций

Через $\bar{\tilde{\sigma}}$ будем обозначать набор $(\bar{\sigma}_1, \ldots, \bar{\sigma}_n)$.

Л е м м а 1. (о несамодвойственной функции) Если $f \notin S$, то $\{0, 1\} \subseteq [\{f, -\}]$.

Д о к а з а т е л ь с т в о. Функция $f \notin S$, значит найдется набор $\tilde{\sigma}$ такой, что $\bar{f}(\tilde{\sigma}) \neq f(\bar{\tilde{\sigma}})$, то есть $f(\tilde{\sigma}) = f(\bar{\tilde{\sigma}})$. Определим $g(x) = f(x^{\sigma_1}, \ldots, x^{\sigma_n})$. Очевидно, что $g(x) \in [\{f, -\}]$. Тогда $g(0) = = f(0^{\sigma_1}, \ldots, 0^{\sigma_n}) = f(\bar{\sigma}_1, \ldots, \bar{\sigma}_n) = f(\sigma_1, \ldots, \sigma_n) = f(1^{\sigma_1}, \ldots, 1^{\sigma_n}) = = g(1)$. Отсюда следует, что $g(x) = \sigma$. Если $\sigma = 0$, то $\bar{g}(x) = 1$, а если $\sigma = 1$, то $\bar{g}(x) = 0$. Лемма 1 доказана.

Л е м м а 2. (о немонотонной функции) Если $f \notin M$, то $- \subseteq \subseteq [\{f, 0, 1\}]$.

Д о к а з а т е л ь с т в о. Функция $f \notin M$, значит найдутся наборы $\tilde{\sigma}$ и $\tilde{\tau}$ такие, что $\tilde{\sigma} \leq \tilde{\tau}$ и $f(\tilde{\sigma}) > f(\tilde{\tau})$, то есть $f(\tilde{\sigma}) = 1$, $f(\tilde{\tau}) = 0$. Определим $g(x) = f(a_1, \ldots, a_n)$, где $a_i = \begin{cases} \sigma_i, \text{ если } \sigma_i = \tau_i; \\ x, \text{ если } \sigma_i < \tau_i. \end{cases}$ Очевидно, что $g(x) \in [\{f, 0, 1\}]$. Имеем $g(0) = f(\tilde{\sigma}) = 1$ и $g(1) = f(\tilde{\tau}) = 0$, то есть $g(x) = \bar{x}$. Лемма 2 доказана.

Л е м м а 3. (о нелинейной функции) Если $f \notin L$, то $\cdot \subseteq [\{f, -, 0, 1\}]$.

Д о к а з а т е л ь с т в о. Пусть $f(x_1,\dots,x_n)\notin L$. Значит в полиноме Жегалкина $p(x_1,\dots,x_n)$ для функции f найдется член, содержащий не менее двух переменных. Без ограничения общности можно считать, что среди них есть переменные x_1 и x_2. Тогда $p(x_1,\dots,x_n) =$ $= x_1x_2p_1(x_3,\dots,x_n)\oplus x_1p_2(x_3,\dots,x_n)\oplus x_2p_3(x_3,\dots,x_n)\oplus p_4(x_3,...,x_n)$. Поскольку $p_1(x_3,\dots,x_n)\neq 0$ найдется набор $(\alpha_3,\dots,\alpha_n)$ такой, что $p_1(\alpha_3,\dots,\alpha_n)=1$. Тогда $\varphi(x_1,x_2)=f(x_1,x_2,\alpha_3,\dots,\alpha_n)=x_1x_2\cdot 1\oplus$ $\oplus x_1p_2(\alpha_3,\dots,\alpha_n)\oplus x_2p_3(\alpha_3,\dots,\alpha_n)\oplus p_4(\alpha_3,\dots,\alpha_n)=x_1x_2\oplus\alpha x_1\oplus$ $\oplus\beta x_2\oplus\gamma=(x_1\oplus\beta)(x_2\oplus\alpha)\oplus\alpha\beta\oplus\gamma=x_1^{\bar\beta}x_2^{\bar\alpha}\oplus\alpha\beta\oplus\gamma$.

Если $\alpha\beta\oplus\gamma=0$, то $\varphi(x_1^{\bar\beta},x_2^{\bar\alpha})=x_1x_2$.

Если $\alpha\beta\oplus\gamma=1$, то $\bar\varphi(x_1^{\bar\beta},x_2^{\bar\alpha})=x_1x_2$. Лемма 3 доказана.

Т е о р е м а. (критерий полноты Поста) Множество B является полным, тогда и только тогда, когда оно целиком не содержится ни в одном из пяти замкнутых множеств F_0, F_1, M, S и L, то есть $B\not\subseteq F_0$, $B\not\subseteq F_1$, $B\not\subseteq M$, $B\not\subseteq S$, $B\not\subseteq L$.

Д о к а з а т е л ь с т в о. Необходимость. От противного. Пусть B принадлежит одному из перечисленных множеств. В силу замкнутости множеств термами над B могут быть реализованы лишь функции из данного множества. Противоречие.

Достаточность. Пусть $B\not\subseteq F_0$, $B\not\subseteq F_1$, $B\not\subseteq M$, $B\not\subseteq S$, $B\not\subseteq L$. Установим сначала, что термами над B могут быть реализованы константы 0 и 1. Пусть $g\in B$ и $g\notin F_0$, то есть $g(0,\dots,0)=1$.

а) Если $g(1,\dots,1)=1$, то $\varphi(x)=g(x,\dots,x)=1$. Возьмем $h\notin F_1$. Тогда $h(\varphi(x),\dots,\varphi(x))=h(1,\dots,1)=0$.

б) Если $g(1,\dots,1)=0$, то $\varphi(x)=g(x,\dots,x)=\bar x$. На основании леммы 1 с помощью $f_1\notin S$ и $-$ получим обе константы.

Имея константы, с помощью $f_2\notin M$ получим $-$ по лемме 2, а по лемме 3 с помощью $f_3\notin L$ и $-$ получим $\cdot$. Полнота B вытекает из полноты $\{-,\cdot\}$. Теорема доказана.

П р и м е р. Пусть $B=\{f\}$, где $f=(1000)$.

$f\notin F_0$, так как $f(00)=1$.

$f\notin F_1$, так как $f(11)=0$.

$f\notin M$, так как $f(00)>f(11)$.

$f\notin S$, так как $f(01)=f(10)$.

$f\notin L$, так как $f'_x=(10)$.

Таким образом, множество B полно.

2.6 Представление о функциях к-значной логики

Пусть $E_k = \{0, 1, \dots, k-1\}$. Функция $f : E_k^n \to E_k$ называется *функцией к-значной логики.*

Как и в случае булевых функций, любую функцию к-значной логики можно задать с помощью таблицы (табл. 3). В этой таблице наборы являются разложениями в к-ичной системе счисления чисел от 0 до $k^n - 1$.

Таблица 3.

x_1	x_2	$\dots$	x_{n-1}	x_n	$f(x_1, x_2, \dots, x_{n-1}, x_n)$
0	0	$\dots$	0	0	$f(0, 0, \dots, 0, 0)$
0	0	$\dots$	0	1	$f(0, 0, \dots, 0, 1)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
0	0	$\dots$	0	$k-1$	$f(0, 0, \dots, 0, k-1)$
0	0	$\dots$	1	0	$f(0, 0, \dots, 1, 0)$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$k-1$	$k-1$	$\dots$	$k-1$	$k-1$	$f(k-1, \dots, k-1)$

Л е м м а 1. Число всех к-ичных наборов длины n равно k^n.

Д о к а з а т е л ь с т в о легко проводится индукцией по n и оставляется читателю в качестве упражнения.

Л е м м а 2. Число всех функций к-значной логики размерности n равно k^{k^n}.

Д о к а з а т е л ь с т в о следует из леммы 1.

Рассмотрим некоторые элементарные функции:

1) $min(x_1, x_2)$ – обобщение конъюнкции;

2) $max(x_1, x_2)$ – обобщение дизъюнкции;

3) $x_1 \oplus x_2$ (mod k) – обобщение сложения по mod 2;

4) $\bar{x} = x \oplus 1$ (mod k) – обобщение отрицания (Поста) в смысле "циклического сдвига"значений;

5) $Nx = k - 1 - x$ – обобщение отрицания (Лукашевича) в смысле "зеркального отражения"значений;

6) $J_\sigma(x) = \begin{cases} k-1 \text{ при } x = \sigma, \\ 0 \text{ при } x \neq \sigma; \end{cases} \quad (\sigma = 0, 1, \dots, k-1).$

7) $V_k(x_1, x_2) = max(x_1, x_2) \oplus 1$ (mod k) – функция Вебба.

Аналогично двузначному случаю вводится понятие терма над некоторым множеством функций к-значной логики.

Для функций $min(x_1, x_2)$ и $max(x_1, x_2)$ также используются обозначения $x_1 \cdot x_2$ и $x_1 \vee x_2$. Тогда $\mathop{\&}\limits_{i=1}^{n} x_i = x_1 \cdot \ldots \cdot x_n = min(x_1, \ldots, x_n)$ и $\bigvee\limits_{i=1}^{n} x_i = x_1 \vee \ldots \vee x_n = max(x_1, \ldots, x_n)$.

Т е о р е м а. Любую функцию к-значной логики $f(x_1, \ldots, x_n)$ можно представить в виде

$$f(x_1, \ldots, x_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n)} J_{\sigma_1}(x_1) \cdot \ldots \cdot J_{\sigma_n}(x_n) \cdot f(\sigma_1, \ldots, \sigma_n).$$

Д о к а з а т е л ь с т в о. Возьмем произвольный набор $(\alpha_1, \ldots, \alpha_n)$ и покажем равенство левой и правой частей.

$$f(\alpha_1, \ldots, \alpha_n) = \bigvee_{(\sigma_1, \ldots, \sigma_n)} J_{\sigma_1}(\alpha_1) \cdot \ldots \cdot J_{\sigma_n}(\alpha_n) \cdot f(\sigma_1, \ldots, \sigma_n) =$$

$= J_{\alpha_1}(\alpha_1) \cdot \ldots \cdot J_{\alpha_n}(\alpha_n) \cdot f(\alpha_1, \ldots, \alpha_n) = (k-1) \cdot \ldots \cdot (k-1) \cdot f(\alpha_1, \ldots, \alpha_n) =$ $= f(\alpha_1, \ldots, \alpha_n)$. Теорема доказана.

С л е д с т в и е. Множество $\{0, 1, \ldots, k-1, J_0(x), J_1(x), \ldots, J_{k-1}(x), min(x_1, x_2), max(x_1, x_2)\}$ является полным.

3 Основы теории графов

Начало теории графов как математической дисциплине было положено великим математиком Леонардом Эйлером, решившим в 1736 году задачу о Кенигсбергских мостах. Однако в течение почти ста лет его статья была единственной в этой области. Интерес к проблемам теории графов возродился около середины XIX века. Имелось много причин такого оживления изучения графов: исследование электрических сетей, моделей кристаллов, структур молекул и т. д. На современном этапе заметно влияние запросов новых областей приложений: теории игр и программирования, теории передачи сообщений, а также проблем биологии и психологии.

3.1 Основные понятия и способы задания графов

Пусть V – непустое конечное множество, R – набор неупорядоченных пар элементов из V. Если $V = \{a_1, \ldots, a_n\}$, то R содержит пары вида (a_i, a_j). В общем случае в R могут встречаться пары с одинаковыми элементами, а также одинаковые пары.

Множество V и набор R определяют *псевдограф* $G = (V, R)$. Элементы множества V называются *вершинами*, а элементы набора R – *ребрами* псевдографа. Ребро вида (a_i, a_i) называется *петлей*.

Графом называется псевдограф без кратных ребер и петель. Граф $G = (V, R)$ называется *ориентированным* или *орграфом*, если множество R состоит из упорядоченных пар.

П р и м е р. Пусть $V = \{1, 2, 3, 4\}$, $R_1 = ((1, 2), (2, 1), (1, 3), (3, 3))$, $R_2 = \{(1, 2), (1, 3), (2, 4)\}$, $R_3 = \{(1, 2), (2, 1), (2, 3), (4, 3)\}$. Тогда $G_1 = (V, R_1)$ — псевдограф, $G_2 = (V, R_2)$ — граф, $G_3 = (V, R_3)$ — ориентированный граф.

Подграфом графа G называется граф, все вершины и ребра которого содержатся среди вершин и ребер графа G.

Удобным оказывается задание графов с помощью *диаграмм*, где вершины графа изображаются точками, а ребра – линиями.

Т е о р е м а. Любой граф можно задать пространственной диаграммой без пересечения ребер.

Д о к а з а т е л ь с т в о. Пусть граф имеет G имеет n вершин и r ребер. Проведем в пространстве произвольным образом некоторую прямую. Отметим на ней n вершин. Проведем через прямую r различных плоскостей. Каждое ребро графа G изобразим, например, в виде дуги окружности на отдельной плоскости. Очевидно, что все дуги попарно не пересекаются. Теорема доказана.

Легко заметить связь графов с бинарными отношениями. *Бинарным отношением* множеств A и B называется подмножество $R \subseteq A \times B$. Если $A = B$, то R называется *отношением на множестве* A. Любой ориентированный граф $G = (V, R)$ с петлями задает бинарное отношение R на множестве V, и обратно. Граф с петлями соответствует симметрическому отношению.

Пусть u и v – вершины, $x = (u, v)$ – соединяющее их ребро. Тогда говорят, что вершина u и ребро x *инцидентны*, вершина v и ребро x также инцидентны. Вершины u и v называются *смежными*, если существует ребро, их соединяющее. Два ребра называются *смежными*, если они имеют общую вершину.

Степенью вершины v называется число $d(v)$ ребер графа, инцидентных вершине v. Очевидно, что если p – число вершин графа, то для любой вершины v этого графа $0 \leq d(v) \leq p - 1$. Вершина v называется *изолированной*, если $d(v) = 0$.

Представление графа с помощью квадратной матрицы A, отражающей смежность вершин, называется *матрицей смежности*, где

$$a_{ij} = \begin{cases} 1, \text{ если вершина } v_i \text{ смежна с } v_j; \\ 0, \text{ в противном случае.} \end{cases}$$

Представление графа с помощью матрицы A, отражающей инцидентность вершин и ребер, называется *матрицей инциденций*, где для неориентированного графа

$$a_{ij} = \begin{cases} 1, \text{ если вершина } v_i \text{ инцидентна ребру } x_j; \\ 0, \text{ в противном случае;} \end{cases},$$

а для орграфа

$$a_{ij} = \begin{cases} 1, \text{ если } v_i \text{ инцидентна } x_j \text{ и является его концом;} \\ 0, \text{ если } v_i \text{ и } x_j \text{ не инцидентны;} \\ -1, \text{ если } v_i \text{ инцидентна } x_j \text{ и является его началом.} \end{cases}$$

Графы $G_1 = (V_1, R_1)$ и $G_2 = (V_2, R_2)$ называются *изоморфными*, если существует взаимно однозначное отображение $\varphi : V_1 \to V_2$ такое, что $(u_1, v_1) \in R_1$ тогда и только тогда, когда $(\varphi(u_1), \varphi(v_1)) \in R_2$. Очевидно, что изоморфизм графов есть отношение эквивалентности.

Поэтому графы рассматриваются с точностью до изоморфизма, то есть изоморфные графы не различаются.

Граф, в котором каждая пара вершин смежна, называется *полным.* Полный граф с p вершинами обозначают через K_p.

Маршрутом в графе называется чередующаяся последовательность вершин и ребер v_1, x_1, v_2, $x_2, \ldots, v_n$, в которой любые два соседних элемента инцидентны, то есть $x_i = (v_i, v_{i+1})$. Если $v_1 = v_n$, то маршрут называется *замкнутым.* Маршрут, в котором все ребра попарно различны называется *цепью.* Маршрут, в котором все вершины (а значит и ребра) попарно различны, называется *простой цепью.* Замкнутая цепь называется *циклом*, а замкнутая простая цепь – *простым циклом.*

Операция подразбиения ребра (u, v) в графе $G = (V, R)$ состоит в удалении из R ребра (u, v), добавлении к V новой вершины w и добавлении к $R \setminus \{(u, v)\}$ двух ребер (u, w) и w, v. Граф G_1 называется *подразбиением графа* G_2, если G_1 может быть получен из G_2 путем последовательного применения конечного числа раз операции подразбиения ребер.

Графы называются *гомеоморфными*, если существуют такие их подразбиения, которые изоморфны.

Т е о р е м а. Сумма степеней вершин графа равна удвоенному количеству ребер.

Д о к а з а т е л ь с т в о оставляется читателю в качестве упражнения.

3.2 Планарные графы

Граф *укладывается* на некоторой поверхности, если его можно нарисовать на этой поверхности так, чтобы ребра графа при этом не пересекались. Граф называется *планарным*, если его можно уложить на плоскости. *Плоский граф* – это граф, уже уложенный на плоскости.

Область, ограниченная ребрами в плоском графе и не содержащая внутри себя вершин и ребер, называется *гранью* (внешняя часть плоскости также образует грань).

Две вершины в графе *связаны*, если существует соединяющая их цепь. Граф, в котором все вершины связаны, называется *связным.*

Отношение связанности вершин является отношением эквивалентности. Классы эквивалентности по отношению связанности называются *компонентами связности* графа. Очевидно, что граф является связным тогда и только тогда, когда число компонент связности графа равно 1.

Т е о р е м а 1. (Эйлера) В связном планарном графе, имеющем p вершин, q ребер и r граней, справедливо следующее соотношение $p - q + r = 2$.

Д о к а з а т е л ь с т в о проведем индукцией по q.

Базис индукции. Пусть $q = 0$. Тогда $p = 1$ и $q = 1$, то есть $p - q + r = 2$.

Шаг индукции. Пусть теорема верна для всех графов с q ребрами. Добавим еще одно ребро. Если оно соединяет существующие вершины, то в новом графе число ребер $q' = q + 1$, число вершин $p' = p$ и число граней $r' = r + 1$. Тогда $p' - q' + r' = p - q - 1 + r + 1 = 2$.

Если добавляемое ребро соединяет существующую вершину с новой, то $p' = p + 1$, $q' = q + 1$ и $r' = r$. Таким образом, $p' - q' + r' = p + 1 - q - 1 + r = 2$. Теорема 1 доказана.

С л е д с т в и е 1. Если $p > 3$, то $q \leq 3p - 6$.

Д о к а з а т е л ь с т в о. Каждая грань ограничена по крайней мере тремя ребрами, каждое ребро ограничивает не более двух граней. Отсюда, $3r \leq 2q$. Имеем $2 = p - q + 2 \leq p - q + \dfrac{2q}{3}$, то есть $3p - 3q + 2q \geq 6$. Значит, $q \leq 3p - 6$. Следствие 1 доказано.

С л е д с т в и е 2. Графы K_5 и $K_{3,3}$ непланарны.

Д о к а з а т е л ь с т в о. 1. Рассмотрим K_5. Имеем $p = 5$ и $q = 10$. Если K_5 планарен, то по следствию 1 $q = 10 \leq 3p - 6 = 9$. Противоречие.

2. Рассмотрим $K_{3,3}$. Имеем $p = 6$ и $q = 9$. В этом графе нет треугольников, а значит если этот граф планарен, то в его плоской укладке каждая грань ограничена не менее чем четырьмя ребрами и, следовательно, $4r \leq 2q$ или $2r \leq q$. По теореме 1 имеем $6 - 9 + r = 2$, то есть $r = 5$. Значит, $2r = 10 \leq q = 9$. Противоречие. Следствие 2 доказано.

С л е д с т в и е 3. В любом планарном графе существует вершина, степень которой не больше 5.

Д о к а з а т е л ь с т в о. От противного. Пусть $d(v) \geq 6$ для любой вершины $v \in V$. Тогда $6p \leq \sum\limits_{v \in V} d(v) = 2q$, то есть $3p \leq q$. По следствию 1 имеем $q \le 3p - 6$, противоречие. Следствие 3 доказано.

Т е о р е м а 2. (Понтрягина-Куратовского) Граф является планарным тогда и только тогда, когда он не содержит ни одного подграфа, гомеоморфного графам K_5 и $K_{3,3}$.

Без доказательства.

Операция удаления вершины v из графа $G = (V, R)$ заключается в удалении из V элемента v, а из R всех ребер, инцидентных v. Подграф $G' = (V', R')$ графа $G = (V, R)$ называется *правильным*, если для любых u, $v \in V'$ из того, что $(u, v) \in R$ следует $(u, v) \in R'$.

Раскраской графа называется такое приписывание цветов его вершинам, что никакие две смежные вершины не получают одинаковый цвет. Наименьшее возможное число цветов в раскраске называется *хроматическим числом* и обозначается $\chi(G)$. Очевидно, что $\chi(G) \le p$, где p – число вершин графа G, и $\chi(K_p) = p$.

Т е о р е м а 3. (о пяти красках) Всякий планарный граф можно раскрасить пятью красками.

Д о к а з а т е л ь с т в о. Достаточно рассматривать связные графы, потому что $\chi(G)$ равно максимальному из хроматических чисел компонент связности графа G.

Далее доказательство проведем индукцией по числу вершин p.

Базис индукции. Если $p \le 5$, то $\chi(G) \le p \le 5$.

Шаг индукции. Пусть теорема верна для всех графов с p вершинами. Рассмотрим граф G с $p+1$ вершиной. По следствию 3 теоремы 1 существует вершина v, для которой $d(v) \le 5$.

Пусть G' получается из G удалением вершины v. Тогда по индуктивному предположению $\chi(G') \le 5$. Раскрасим теперь вершину v в графе G.

1 случай. Если $d(v) < 5$, то в 5-раскраске графа G' существует цвет, свободный для v.

2 случай. Если $d(v) = 5$ и найдутся две смежные с v вершины одинакового цвета в 5-раскраске графа G', то существует цвет, свободный для v.

3 случай. Если $d(v) = 5$ и все 5 цветов использованы для раскраски смежных с v вершин. Пусть смежная с v вершина v_i окрашена в цвет i. И пусть G_{13} – правильный подграф графа G', порожденный всеми вершинами, покрашенными в цвета 1 или 3 в 5-раскраске графа G'.

Если v_1 и v_3 принадлежат разным компонентам связности графа G_{13}, то в той компоненте, в которой находится v_1, произведем перекраску $1 \leftrightarrow 3$. При этом получится 5-раскраска графа G', но цвет 1 будет свободен для v.

Если же v_1 и v_3 принадлежат одной компоненте связности, то существует простая цепь, соединяющая v_1 и v_3 и состоящая из вершин, покрашенных в цвета 1 и 3. В этом случае вершины v_2 и v_4 принадлежат разным компонентам связности подграфа G_{24} графа G', так как граф G – планарный. Перекрасим вершины $2 \leftrightarrow 4$ в той компоненте связности графа G_{24}, которой принадлежит v_2, и получим 5-раскраску графа G', в которой цвет 2 свободен для v. Теорема 3 доказана.

3.3 Сети. Потоки в сетях

На протяжении всего параграфа будем рассматривать только связные графы.

Направленным графом $G = (V, R)$ называется орграф, который не имеет симметричных пар ориентированных ребер, то есть набор R не может содержать одновременно ребра (u, v) и (v, u). Ориентированное ребро далее будем называть *дугой.*

Для орграфа *полустепенью исхода* вершины v называется число дуг, исходящих из вершины v, а *полустепенью захода* – число дуг, входящих в вершину v. Обозначаются эти числа соответственно, $d^-(v)$ и $d^+(v)$.

Вершина v в орграфе называется *источником*, если $d^+(v) = 0$, и *стоком*, если $d^-(v) = 0$.

Направленный граф с одним источником и одним стоком называется *сетью.*

Пусть $G = (V, R)$ – сеть, s и t – соответственно источник и сток сети. Дуги сети нагружены неотрицательными действительными числами, $c : R \to \mathbf{R}^+$. Число $c(u, v)$ называется *пропускной способностью* дуги (u, v).

Пусть задана функция $f : R \to \mathbf{R}^+$. *Дивергенцией* функции f в вершине u называется число $div(f, u)$, которое определяется следующим образом:

$$div(f,u) = \sum_{\{v|(u,v)\in R\}} f(u,v) - \sum_{\{v|(v,u)\in R\}} f(v,u).$$

Функция $f : R \to \mathbf{R}$ называется *потоком* в сети G, если:

1) для любой $(u,v) \in R \quad 0 \leq f(u,v) \leq c(u,v)$;

2) для любой $u \in V \setminus \{s,t\}$ $div(f,u) = 0$.

Число $w(f) = div(f,s)$ называется *величиной потока* f.

Дадим определение *разреза*. Разобьем множество вершин V произвольным образом на два подмножества S и T, так что $S \subset V$, $T \subset V$, $S \cup T = V$, $S \cap T = \emptyset$, $s \in S$, $t \in T$. Тогда множество $P = \{(u,v) \in R | u \in S, v \in T$ или $u \in T, v \in S\}$ называется *(s,t)-разрезом.* Таким образом, разрез разбивает граф на две связные компоненты. $P = P^+ \cup P^-$, где P^+ – множество дуг от S к T, а P^- – от T к S.

Сумма потоков через дуги разреза P обозначается $F(P)$, то есть $F(P) = \sum\limits_{e\in P} f(e)$. Сумма пропускных способностей дуг разреза P называется *пропускной способностью* разреза и обозначается $C(P)$, то есть $C(P) = \sum\limits_{e\in P} c(e)$.

Л е м м а 1. $w(f) = F(P^+) - F(P^-)$.

Д о к а з а т е л ь с т в о. Рассмотрим сумму $W = \sum\limits_{v\in S} div(f,v)$. Пусть дуга $(u,v) \in R$. Если $u,v \in S$, то в сумму W попадают два слагаемых для этой дуги: $f(u,v)$ при вычислении $div(f,u)$ и $-f(u,v)$ при вычислении $div(f,v)$, итого 0. Если $u \in S$, $v \in T$, то в сумму W попадает одно слагаемое $f(u,v)$, все такие слагаемые дают $F(P^+)$. Если $u \in T$, $v \in S$, то в сумму W попадает одно слагаемое $-f(u,v)$, все такие слагаемые дают $F(P^-)$. Таким образом, $F(P^+) - F(P^-) = W$. С другой стороны, $W = \sum\limits_{v\in S} div(f,v) = div(f,s) = w(f)$, так как $div(f,v) = 0$ для всех $v \in V \setminus \{s,t\}$. Лемма 1 доказана.

Л е м м а 2. $div(f,s) = -div(f,t)$.

Д о к а з а т е л ь с т в о. Рассмотрим (s, t) – разрез P. Пусть $S = V \setminus \{t\}$, а $T = \{t\}$. Имеем $div(f,s) = w(f) = F(P^+) - F(P^-) = $ $= F(P^+) = \sum\limits_{v} f(v,t) = -div(f,t)$. Лемма 2 доказана.

Л е м м а 3. $w(f) \leq F(P)$.

Д о к а з а т е л ь с т в о. $w(f) = F(P^+) - F(P^-) \leq F(P^+) \leq F(P)$. Лемма 3 доказана.

Л е м м а 4. $\underset{f}{max}\, w(f) \leq \underset{P}{min}\, C(P)$.

Д о к а з а т е л ь с т в о. По лемме 3 $w(f) \leq F(P) \leq F(P)$. Отсюда, $\underset{f}{max}\, w(f) \leq \underset{P}{min}\, F(P)$. По определению $F(P) \leq C(P)$, а значит $\underset{P}{min}\, F(P) \leq \underset{P}{min}\, C(P)$. Итак, $\underset{f}{max}\, w(f) \leq \underset{P}{min}\, C(P)$. Лемма 4 доказана.

Т е о р е м а. (Форда-Фалкерсона) Максимальный поток в сети равен минимальной пропускной способности разреза, то есть существует поток f^* такой, что $w(f^*) = \underset{f}{max}\, w(f) = \underset{P}{min}\, C(P)$.

Д о к а з а т е л ь с т в о. Пусть f – некоторый максимальный поток. Покажем, что существует разрез P такой, что $w(f) = C(P)$.

Рассмотрим граф G', полученный из G отменой ориентации ребер. Цепь, соединяющую u и v, обозначим $< u, v >$. Построим множество вершин S следующим образом: $S = \{u \in V|$ существует $< s, u > \in G'$; для любой $(u_i, u_{i+1}) \in < s, u >$ если $(u_i, u_{i+1}) \in R$, то $f(u_i, u_{i+1}) < c(u_i, u_{i+1})$ и если $(u_{i+1}, u_i) \in R$, то $f(u_{i+1}, u_i) > 0\}$. Такая цепь $< s, u >$ называется *аугментальной*. Имеем $s \in S$ по построению. Покажем, что $t \in T$. От противного. Пусть $t \in S$, тогда существует аугментальная цепь $< s, t >$. Примем $\delta = \underset{e \in < s,t >}{min}\, \alpha(e)$, где $\alpha(e) = \begin{cases} c(e) - f(e) > 0, \text{ если } e \text{ ориентировано вдоль } < s, t >; \\ f(e) > 0, \text{ если } e \text{ ориентировано против } < s, t > . \end{cases}$
В этом случае можно увеличить величину потока на δ, изменив поток для всех дуг аугментальной цепи:

$f'(e) = \begin{cases} f(e) + \delta, \text{ если } e \text{ ориентировано вдоль } < s, t >; \\ f(e) - \delta, \text{ если } e \text{ ориентировано против } < s, t > . \end{cases}$ При этом условия потока выполняются $0 \leq f'(e) \leq c(e)$ и $div(f', v) = 0$. Получили противоречие максимальности f.

Итак, $t \in T$. Следовательно, множества S и T определяют разрез $P = P^+ \cup P^-$. В этом разрезе для всех дуг e^+ имеем $f(e^+) = c(e^+)$, а для e^- имеем $f(e^-) = 0$, иначе S можно было бы расширить. Таким образом, $w(f) = F(P^+) - F(P^-) = C(P^+)$, а P – искомый разрез. Теорема доказана.

3.4 Деревья

Будем рассматривать неориентированные графы.

Л е м м а 1. Если $G = (V, R)$ – связный граф, то при добавлении к G любого ребра (u, v), где $u, v \in V$, то в полученном графе будет простой цикл.

Д о к а з а т е л ь с т в о. Так как граф G является связным, то существует цепь S из u в v. Если эта цепь не является простой, то в ней повторяется некоторая вершина v_i, то есть цепь имеет вид $S = uS_1v_iS_2v_iS_3v$. Тогда цепь S сократима, выбросив из нее S_2, получим $S' = uS_1v_iS_3v$. Поскольку S – конечная цепь, то повторяя при необходимости эту операцию сокращения, получим простую цепь Z из u в v. После добавления к Z отсутствовавщего в G ребра (u, v) получим простой цикл. Лемма 1 доказана.

Л е м м а 2. Граф из p вершин и q ребер содежит не менее $p - q$ связных компонент, а если в этом графе нет циклов, то он содержит ровно $p - q$ связных компонент.

Д о к а з а т е л ь с т в о. При добавлении к произвольному графу, содержащему вершины u и v, одного ребра (u, v) число связных компонент может только уменьшиться, но не более чем на 1. При добавлении q ребер число связных компонент в графе может уменьшиться не более чем на q.

Граф $G = (V, R)$ с p вершинами и q ребрами получается из графа $G' = (V, \emptyset)$, имеющего p изолированных вершин, то есть p связных компонент, добавлением q ребер, и согласно вышесказанному в G будет не менее $p - q$ связных компонент.

Пусть теперь в G нет циклов. Допустим, что в процессе получения G из G' добавляется ребро (u, v). Если бы вершины u и v принадлежали одной связной компоненте, то в G по лемме 1 появился бы цикл. Значит, u и v принадлежат разным компонентам связности и при добавлении ребра (u, v) число связных компонент уменьшается ровно на 1. Поэтому в G окажется ровно $p - q$ связных компонент. Лемма 2 доказана.

С л е д с т в и е. Любой граф G с p вершинами и q ребрами при $q \leq p - 2$ несвязен.

Д о к а з а т е л ь с т в о. По лемме 2 и из условия $q \leq p-2$ следует, что в G не менее двух связных компонент. Следствие доказано.

Граф $G = (V, R)$ называется *деревом*, если он является связным и не содержит циклов.

Если $G = (V, R)$ – связный граф, $x \in R$ и входит в некоторый цикл, то есть x – циклическое ребро, то граф G_1, полученный из G удалением ребра x остается, как нетрудно заметить, связным. Удаляя из G в произвольной последовательности циклические ребра, можно получить связный подграф графа G с множеством вершин V, но без циклов, то есть дерево. Это дерево называется *остовным деревом* или *остовом* графа G. Таким образом, всякий связный граф $G = (V, R)$ содержит хотя бы один подграф $G' = (V, R')$ с тем же множеством вершин, являющийся деревом.

Т е о р е м а 1. Пусть $G = (V, R)$ – граф с p вершинами и q ребрами. Тогда следующие условия эквивалентны:

1) G – дерево;

2) любые две вершины графа G связаны ровно одной простой цепью;

3) G не содержит циклов и $q = p - 1$;

4) G – связный граф и $q = p - 1$;

5) G – связный граф, но при удалении любого ребра становится несвязным;

6) G не содержит циклов, но при добавлении любого нового ребра с концами из V у него появляется цикл.

Д о к а з а т е л ь с т в о. Покажем переход $1 \Rightarrow 2$. От противного. Пусть в дереве G существуют две простые цепи Z_1 и Z_2, связывающие вершины u и v. В этом случае существует ребро x, которое принадлежит Z_1 и не принадлежит Z_2. Пойдем в обе стороны от ребра x до первой встречи с цепью Z_2 в вершинах v_i и v_j. Эту подцепь цепи Z_1, содержащую ребро x, обозначим через Z_1'. Подцепь Z_1' вместе с подцепью Z_2' цепи Z_2', ведущей из v_i и v_j, образует цикл. Противоречие. Переход $1 \Rightarrow 2$ доказан.

Покажем переход $2 \Rightarrow 3$. Условие 2) означает, что в G отсутствуют циклы, поскольку концы любого ребра из цикла связаны, по крайней мере, двумя простыми цепями. Из условия 2) следует также, что граф G – связный, то есть имеет одну связную компоненту. Из леммы 2 получаем $q = p - 1$. Переход $2 \Rightarrow 3$ доказан.

Покажем переход $3 \Rightarrow 4$. Из условия 3) и леммы 2 следует, что число компонент связности в G равно $p - q = 1$, то есть G – связный граф. Переход $3 \Rightarrow 4$ доказан.

Покажем переход $4 \Rightarrow 5$. Этот переход вытекает из следствия к лемме 2.

Покажем переход $5 \Rightarrow 6$. Если бы в G был цикл, то при удалении ребра из этого цикла граф G остался бы связным, что противоречит условию 5). Так как G – связный граф, то по лемме 1 при добавлении любого нового ребра с концами из V появляется простой цикл. Переход $5 \Rightarrow 6$ доказан.

Покажем переход $6 \Rightarrow 1$. От противного. Пусть G – несвязный граф, а вершины u и v принадлежат разным компонентам связности графа G. Тогда добавление ребра (u, v) не порождает циклов, что противоречит условию 6). Таким образом, G – связный граф, не содержащий циклов, то есть дерево. Переход $6 \Rightarrow 1$ доказан. Теорема 1 доказана.

Выделим в дереве какую-нибудь одну вершину, которую назовем *корнем*. Полученное дерево с выделенной вершиной называется *корневым деревом*.

Т е о р е м а 2. Число неизоморфных корневых деревьев с q ребрами не превосходит 4^q.

Д о к а з а т е л ь с т в о. Будем кодировать корневые деревья наборами из нулей и единиц по следующему индуктивному правилу:

1. Кодом дерева из одного ребра является набор 01;

2. а) Если дерево имеет одно корневое ребро (ребро, инцидентное корню), то его кодом будет набор $0A1$, где A – код дерева, получающегося при удалении корневого ребра и объявлении корнем его второго конца;

б) Если корневых ребер $k > 1$, то дерево получается склеиванием в корне k поддеревьев с меньшим числом ребер. Если $A_1, \ldots, A_k$ – коды этих поддеревьев, то набор $A_1 \ldots A_k$ является кодом всего дерева.

Очевидно, что код дерева с q ребрами есть набор длины $2q$, содержащий поровну нулей и единиц. Далее заметим, что в случае применения правила б) из пункта 2 в коде $A_1 \ldots A_k$ набор A_1 является наименьшим непустым начальным отрезком, содержащим поровну нулей и единиц. То же самое верно и для A_2 в коде $A_2 \ldots A_k$ и т. д. Таким образом, по своему коду дерево восстанавливается однозначно. Поэтому число неизоморфных корневых деревьев с q ребрами не превосходит числа наборов длины $2q$ из нулей и единиц, то есть $2^{2q} = 4^q$. Теорема 2 доказана.

3.5 Эйлеровы и гамильтоновы графы

Если граф имеет цикл, содержащий все ребра графа по одному разу, то такой цикл называется *эйлеровым циклом*, а граф называется *эйлеровым*. Ясно, что эйлеровым может быть только связный граф.

Т е о р е м а 1. Если граф $G = (V, R)$ является связным и нетривиальным, то следующие утверждения эквивалентны:

1) G – эйлеров граф;

2) каждая вершина графа G имеет четную степень;

3) множество ребер графа G можно разбить на простые циклы.

Д о к а з а т е л ь с т в о. Покажем переход $1 \Rightarrow 2$. Пусть Z – эйлеров цикл. Двигаясь по Z, будем подсчитывать степени вершин, полагая их до начала прохождения нулевыми. Прохождение каждой вершины добавляет 2 в степень этой вершины. Поскольку Z содержит все ребра, когда обход Z будет закончен, будут учтены все ребра, а степени всех вершин – четные. Переход $1 \Rightarrow 2$ доказан.

Покажем переход $2 \Rightarrow 3$. Граф G – связный и нетривиальный, для любой верщины v из V $d(v) > 0$. Степени вершин четные, следовательно $d(v) \geq 2$ для любой v. Имеем $2q = \sum\limits_{v \in V} d(v) \geq 2p$, а значит $q \geq p$ или $q > p - 1$. Отсюда следует, что G – не дерево, а значит G содержит простой цикл Z_1. Пусть G_1 получается из G удалением Z_1 и всех изолированных вершин, появившихся после удаления ребер. Нетрудно заметить, что все степени вершин графа G_1 опять четные. Таким образом, в G_1 также существует простой цикл Z_2. Далее выделяем все циклы Z_i, пока граф не будет пуст. Имеем $R = \bigcup\limits_i Z_i$ и $\bigcap\limits_i Z_i = \emptyset$. Переход $2 \Rightarrow 3$ доказан.

Покажем переход $3 \Rightarrow 1$. Возьмем какой-либо цикл Z_1 из данного разбиения. Если $Z_1 = R$, то теорема доказана. Если нет, то существует цикл Z_2 такой, что найдется вершина v_1, принадлежащая как Z_1, так и Z_2 в силу связности G. Маршрут $Z_1 \cup Z_2$ является циклом и содержит все свои ребра по одному разу. Если $Z_1 \cup Z_2 = R$, то теорема доказана. Иначе существует цикл Z_3 такой, что найдется вершина v_2, принадлежащая $Z_1 \cup Z_2$ и Z_3. Далее будем аналогично наращивать эйлеров цикл, пока он не исчерпает разбиения. Переход $3 \Rightarrow 1$ доказан. Теорема 1 доказана.

Пусть $S(p)$ – множество всех графов с p вершинами, а $E(p)$ – множество всех эйлеровых графов с p вершинами.

Т е о р е м а 2. $\lim\limits_{p\to\infty} \dfrac{|E(p)|}{|S(p)|} = 0$, то есть количество эйлеровых графов существенно мало по сравнению общим количеством графов.

Д о к а з а т е л ь с т в о. Пусть $E'(p)$ - множество графов с p вершинами, степень каждой из которых четна. Тогда по теореме 1 $E(p) \subseteq E'(p)$ и $|E(p)| \leq |E'(p)|$. По лемме в любом графе число вершин нечетной степени четно, поэтому любой граф из $E'(p)$ можно получить с помощью графа из множества $S(p-1)$, если добавить новую вершину и соединить ее со всеми старыми вершинами нечетной степени. Значит, $|E'(p)| \leq |S(p-1)|$. Мощность $|S(p)| = 2^{C_p^2}$, где C_p^2 – число всевозможных ребер. Заметим, что $C_{p-1}^1 + C_{p-1}^2 = C_p^2$. Итак, $|E(p)| \leq |E'(p)| \leq |S(p-1)| = 2^{C_{p-1}^2} = 2^{C_p^2-(p-1)} = |S(p)| \cdot 2^{-(p-1)}$, то есть $\dfrac{|E(p)|}{|S(p)|} \leq \dfrac{1}{2^{p-1}}$. Отсюда, $\lim\limits_{p\to\infty} \dfrac{|E(p)|}{|S(p)|} = 0$. Теорема 2 доказана.

Если граф имеет простой цикл, содержащий все вершины графа, то такой цикл называется *гамильтоновым циклом*, а сам граф называется *гамильтоновым.* Очевидно, что гамильтоновым может быть только связный граф.

Любой граф G можно превратить в гамильтонов, добавив достаточное количество вершин. Для этого, например, достаточно к вершинам $v_1, \ldots, v_p$ графа G добавить вершины $u_1, \ldots, u_p$ и множество ребер $\{(v_i, u_i)\} \cup \{(u_i, v_{i+1})\}$.

Т е о р е м а 3. (Дирака) Если в графе $G = (V, R)$ для любой вершины v выполняется $d(v) \geq \dfrac{p}{2}$, то граф G является гамильтоновым.

Д о к а з а т е л ь с т в о. От противного. Пусть граф G не является гамильтоновым. Добавим к G минимальное количество новых вершин $u_1, \ldots, u_n$, соединяя их со всеми вершинами графа G так, чтобы новый граф $G' = (V', R')$ был гамильтоновым, где $V' = V \cup \{u_1, \ldots, u_n\}$.

Пусть $v, u_1, w, \ldots, v$ – гамильтонов цикл в графе G', причем $v \in V$, $u_1 \in V'$, $u_1 \notin V$. Такая пара вершин v и u_1 в гамильтоновом цикле обязательно найдется, иначе граф G был бы гамильтоновым. Тогда $w \in V$ и $w \notin \{u_1, \ldots, u_n\}$, иначе вершина u_1 была бы не нужна. Более того вершина v несмежна с w, иначе опять вершина u_1 была бы не нужна.

Далее, если в цикле $v, u_1, w, \ldots, v', w', \ldots, v$ есть вершина w', смежная с вершиной w, то вершина v' несмежна с вершиной v, так как иначе можно было бы построить гамильтонов цикл $v, v', \ldots, w, w', \ldots, v$ без вершины u_1, взяв последовательность вершин $w, \ldots, v'$ в обратном порядке. Отсюда следует, что число вершин графа G', несмежных с v, не менее числа вершин, смежных с w.

По построению $d(w) \geq \dfrac{p}{2} + n$ и $d(v) \geq \dfrac{p}{2} + n$. Общее число вершин, смежных и несмежных с v составляет $n + p - 1$. Тогда выполняется $n + p - 1 \geq d(w) + d(v) \geq \dfrac{p}{2} + n + \dfrac{p}{2} + n = 2n + p$, то есть $0 \geq n + 1$. Противоречие. Теорема 3 доказана.

Задачи к разделу I.

1. Бросают две игральные кости. Сколькими способами они могут упасть так, что либо на каждой грани выпадет четное число очков, либо на каждой грани выпадет нечетное число очков?

2. Бросают три игральные кости. Сколькими способами они могут упасть так, что либо все оказавшиеся вверху грани одинаковы, либо все попарно различны?

3. Сколькими способами из 28 костей домино можно выбрать две кости так, чтобы их можно было приложить друг к другу?

4. У англичан принято давать детям несколько имен. Сколькими способами можно назвать ребенка, если ему дают не более трех имен, а общее число имен равно 300. (Два способа, различающиеся лишь порядком имен, считаются различными).

5. Найти число векторов $\tilde{\alpha} = (\alpha_1, \ldots, \alpha_n)$, координаты которых удовлетворяют условиям:

а) $\alpha_i \in \{0, \ldots, k-1\}$, $i = \overline{1,n}$;

б) $\alpha_i \in \{0, \ldots, k_i - 1\}$, $i = \overline{1,n}$;

в) $\alpha_i \in \{0,1\}$, $i = \overline{1,n}$, $\sum\limits_{i=1}^{n} \alpha_i = r$.

6. Каково число матриц из n строк и m столбцов с элементами из множества $\{0,1\}$. То же при условии, что строки матрицы попарно различны.

7. Дано m предметов одного сорта и n другого. Найти число вариантов одновременного выбора r предметов одного сорта и s другого.

8. Сколькими способами можно распределить три билета среди 20 студентов, если:

а) распределяются билеты в разные театры, а каждый студент может получить не более одного билета;

б) распределяются билеты в разные театры и на разные дни, а каждый студент может получить любое (не превосходящее трех) число билетов;

в) распределяются равноценные билеты на вечер и каждый студент может получить не более одного билета?

9. Выяснить, сколькими способами можно выстроить девять человек:

а) в колонну по одному;

б) в колонну по три, если в каждой шеренге люди выстраиваются по росту и нет людей одинакового роста?

10. Доказать следующие тождества:

а) $C_n^k \cdot C_k^r = C_{n-r}^{k-r} \cdot C_n^r$;

б) $\dfrac{C_n^{k-r}}{C_n^k} = \dfrac{A_k^r}{A_{n-k+r}^r}$;

в) $\dfrac{C_{n+1}^k}{C_n^k} = \dfrac{n+1}{n-k+1}$;

г) $\dfrac{C_{n-r}^{k-r}}{C_n^k} = \dfrac{A_k^r}{A_n^r}$;

д) $C_n^k = \sum\limits_{r=0}^{k} C_{n-r-1}^{k-r}$;

е) $\sum\limits_{k=0}^{n} (2k+1)C_n^k = (n+1) \cdot 2^n$.

11. Доказать, что

а) C_n^k возрастает по n при фиксированном k;

б) C_{n-r}^{k-r} убывает по r при фиксированных n и k.

12. Пусть $n = p_1^{\alpha_1}, \dots, p_k^{\alpha_k}$ – разложение числа n в произведение простых попарно различных чисел. Найти:

а) число всех натуральных делителей числа n;

б) число всех делителей, не делящихся на квадрат никакого целого числа, отличного от 1;

в) сумму делителей числа n.

13. Сколькими способами можно представить число n в виде суммы k неотрицательных слагаемых? (Представления, отличающиеся

лишь порядком слагаемых, считаются различными).

14. а) Найти число целых положительных чисел, не превосходящих 1000 и не делящихся ни на одно из чисел 3, 5 и 7;

б) Найти число целых положительных чисел, не превосходящих 1000 и не делящихся ни на одно из чисел 6, 10 и 15.

15. Найти число простых чисел, не превосходящих 250.

16. На одной из кафедр университета работают 13 человек, причем каждый из них знает хотя бы один иностранный язык. Десять человек знают английский, семеро – немецкий, шестеро – французский. Пятеро знают английский и немецкий, четверо – английский и французский, трое – немецкий и французский.

а) Сколько человек знают все три языка?

б) Сколько человек знают ровно два языка?

в) Сколько человек знают только английский?

17. Дисциплина состоит из трех разделов. Каждый из 40 экзаменационных билетов содержит по 3 вопроса из любого раздела. Известно, что в 14-ти билетах есть вопросы из всех трех разделов. Вопросы по первому разделу имеются в 34 билетах, из них один билет полностью посвящен первому разделу, 8 билетов содержат вопросы по первому и второму разделам. Вопросы из второго раздела содержатся в 28 билетах, и только в два из них целиком посвящены второму разделу. Сколько экзаменационных билетов состоят лишь из вопросов третьего раздела?

Задачи к разделу II.

1. Найти двоичный набор длины k, являющийся разложением числа n, если

а) $k = 3$, $n = 6$;

б) $k = 4$, $n = 11$;

в) $k = 5$, $n = 30$.

2. Найти номера следующих двоичных наборов:

а) (100);

б) (111011);

в) $(1\underbrace{0\ldots0}_{\text{m раз}}1)$, где $m \geq 1$;

г) $(\underbrace{1\ldots1}_{\text{m раз}}0\underbrace{1\ldots1}_{\text{m раз}}\ \underbrace{0\ldots0}_{\text{m раз}})$, где $m \geq 1$.

3. Выписать все двоичные наборы длины 5 по натуральному порядку.

4. Записать табличное и векторное представления для функции $f(x_1, x_2, x_3, x_4)$, принимающей значение 1 на наборах веса 3.

5. Пусть $f = (0011101100001111)$. Найти представление функции f через характеристические множества.

6. Функция $f(x_1, x_2, x_3)$ определяется следующим образом: она равна 1 либо при $x_1 = 1$, либо если переменные x_2 и x_3 принимают разные значения, а значение переменной x_1 меньше значения переменной x_3; в противном случае функция обращается в нуль. Составить таблицу функции f и выписать характеристические множества.

7. Найти остаточные функции от функции f по каждой переменной, если

а) $f = (00111000)$;

б) $f = (1111010100011100)$;

в) $f(x_1, x_2, x_3)$ принимает значение 1 только на наборах веса 1;

г) $H_0(f) = \{(010), (101), (110), (001)\}$;

д) $H_1(f) = \{(1100), (0001), (1110)\}$.

8. Функция $f(x_1, x_2, x_3, x_4)$ задается так: она равна нулю только на таких наборах $\tilde{\sigma} = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$, для которых справедливо неравенство $\sigma_1 + \sigma_2 > \sigma_3 + 2\sigma_4$. Построить таблицу функции f и найти характеристические множества.

9. Перечислить все фиктивные и существенные переменные следующих функций:

а) $f = (1100001100111100)$;

б) $g = (0101101001011010)$;

в) $h = (0011110000111100)$;
г) $H_0(t) = \{(000), (100)\}$.

10. Каково число функций размерности n, принимающих значение 1 менее, чем на k наборах из E^n?

11. Какие из следующих выражений являются термами над множеством $B = \{-, \vee, \leftrightarrow, |, \downarrow\}$?
а) $(x\bar{y}z \vee (y \leftrightarrow xz)$;
б) $(x \vee xy)|(x \vee y\bar{z})$;
в) $(\downarrow y \vee (z \downarrow z) \vee \bar{x})$;
г) $((x|z) \vee (y \leftrightarrow y))$;
д) $((y) \downarrow (xz))$.

12. По функциям $f = (1011)$ и $g = (1001)$ найти векторное представление функции h, если
а) $h(x_1, x_2, x_3, x_4) = f(x_1, x_2) \vee g(x_3, x_4)$;
б) $h(x_2, x_3, x_4) = f(g(x_3, x_4), x_2)$.

13. Найти векторное представление функции φ, заданной термом Φ над множеством $B = \{f_1, f_2, g\}$, если функциональным символам f_1, f_2, g сопоставлены булевы функции, заданные соответственно векторами (10), (1011) и (1000), где
а) $\Phi \equiv f_2(f_1(g(x, f_1(y))), y)$;
б) $\Phi \equiv g(f_1(f_2(x, y)), g(x, f_1(y)))$;
в) $\Phi \equiv f_1(f_2(x, g(f_2(x, y), f_1(y))))$.

14. Построить таблицы функций, реализуемых следующими термами:
а) $(x \to y) \oplus ((y \to z) \oplus (z \to x))$;
б) $\overline{\bar{x} \vee y \vee x \cdot \bar{z}} \downarrow (x \leftrightarrow y)$;
в) $\bar{x} \to (\bar{z} \leftrightarrow (y \oplus xz))$;
г) $(((x|y) \downarrow z)|y) \downarrow z$.

15. Для следующих термов найти глубину, множество переменных, множество графически неравных подтермов:
а) $(x \vee y)(y \vee x) \oplus \overline{x \to z}((y \to x) \vee (\bar{y} \vee x))$;
б) $(x \leftrightarrow z) \vee (x \vee (x \leftrightarrow (z \oplus \overline{x \leftrightarrow z})))$.

16. Выяснить эквивалентны ли термы Φ и Ψ, если

а) $\Phi \equiv x\bar{z} \vee \bar{x}\bar{z} \vee \bar{x}y$, $\Psi \equiv \bar{x}\overline{yz} \vee x\bar{z}$;

б) $\Phi \equiv ((x \to y) \vee z)((z \to y) \vee \bar{x}) \to (x\bar{y} \oplus (x \leftrightarrow \bar{y}))$, $\Psi \equiv (x \vee y)(\bar{x} \vee \bar{y})$;

в) $\Phi \equiv (x \to y) \oplus (z \to y)$, $\Psi \equiv (x \oplus z) \to y$.

17. Представить функцию f термом над B, если

а) $f = x \to y$, $B = \{-, \vee\}$;

б) $f = x \vee y$, $B = \{\to\}$;

в) $f = x \leftrightarrow y$, $B = \{\cdot, \to\}$;

г) $f = x|y$, $B = \{\downarrow\}$.

18. Доказать, что функцию f нельзя представить термом над B, если

а) $f = x \oplus y$, $B = \{\cdot\}$;

б) $f = x \cdot y$, $B = \{\to\}$;

в) $f = x \vee y$, $B = \{\leftrightarrow\}$.

19. Можно ли реализовать функцию f термом глубины $k+1$ над множеством B, если она реализуема термом глубины k над тем же множеством B?

20. Выяснить, является ли функция g двойственной к функции f, если

а) $f = (10001001)$, $g = (01110110)$;

б) $H_0(f) = \{(000), (011), (110)\}$, $H_1(g) = \{(000), (011), (111)\}$;

в) $f = xy \oplus xz \oplus yz$, $g = xy \vee xz \vee yz$;

г) $f = (x|\bar{y}) \vee (z \oplus x)$, $g = (x \downarrow \bar{y})(\bar{x} \leftrightarrow \bar{z})$.

21. Используя принцип двойственности, построить терм, представляющий функцию, двойственную функции f, если

а) $f = xy \vee y\bar{z} \vee \bar{y}z$;

б) $f = (\bar{x} \vee \bar{y} \vee (yz \oplus 1)) \downarrow x$;

в) $f = ((x \to y) \vee \bar{z})(x \leftrightarrow yz)$.

22. Для функции f найти представление в виде СДНФ, СКНФ, СПКНФ и полинома Жегалкина, если

а) $f = (0100)$;

б) $f = (11101001)$;
в) $f = (0001011000100100)$;
д) $H_0(f) = \{(001), (010), (110)\}$;
е) $f = (x_1 \to x_2) \oplus (x_1 | x_2 x_3)$;
ж) $f = (x_1 \leftrightarrow x_2)(x_3 \to \bar{x}_2 x_4)$.

23. Используя эквивалентные преобразования, привести терм Φ к СДНФ и СКНФ, если
а) $\Phi \equiv (x_1 \leftrightarrow x_3)(x_1 \to x_2)$;
б) $\Phi \equiv (\bar{x}_1 \to \bar{x}_2) \oplus (x_3 \leftrightarrow (\bar{x}_2 \vee x_1))$;
в) $\Phi \equiv ((x_2 \leftrightarrow \bar{x}_3) \to x_1) \oplus x_1 \bar{x}_2$.

24. Методом неопределенных коэффициентов построить полином Жегалкина для функции f, если
а) $f = (0001)$;
б) $f = (00010111)$;
в) $f = x_1 \downarrow x_2$;
г) $f = (x_1 \bar{x}_2 \oplus x_3) \to x_2$.

25. Выяснить, принадлежит ли функция f множествам F_0, F_1, M, S и L, если
а) $f = (1011)$;
б) $f = (00010111)$;
в) $f = x_1 x_2 \vee \bar{x}_3$;
г) $f = x_1 \downarrow ((x_1 \to \bar{x}_2) \vee \bar{x}_3)$;
д) $f = (x_1 \to \bar{x}_2 x_3) \leftrightarrow (x_3 \oplus x_1 \vee x_4)$.

26. Сведением к заведомо полному множеству показать, что множество B полно, если
а) $B = \{-, \cdot\}$;
б) $B = \{|\}$;
в) $B = \{\downarrow\}$;
г) $B = \{xy \oplus z, (x \to y) \oplus z\}$;
д) $B = \{xy \oplus zt \oplus 1, (101101110)\}$.

27. Построить множество всех функций, зависящих от переменных x_1 и x_2 и принадлежащих замыканию A, если
а) $A = \{x_1 \oplus x_2\}$;

б) $A = \{0, \bar{x}\}$;
в) $A = \{x_1 x_2\}$;
г) $A = \{\bar{x}_1 \vee x_2\}$;
д) $A = \{0, x_1 \leftrightarrow x_2\}$.

28. Выяснить, полно ли множество B, если
а) $B = \{1110\}$;
б) $B = \{xy, x \vee y, x \oplus y, xy \vee yz \vee zx\}$;
в) $B = \{f = (1001), g = (11101000)\}$;
г) $B = \{\bar{x}, x(y \leftrightarrow z) \leftrightarrow yz, x \oplus y \oplus z\}$;
д) $B = \{\cdot, \rightarrow, (00010111), 1\}$.

29. Выяснить, полно ли множество $B = \{f_1, f_2\}$, если
а) $f_1 \in S \setminus M,\ f_2 \notin L \cup S,\ f_1 \rightarrow f_2 = 1$;
б) $f_1 \notin L \cup F_0 \cup F_1,\ f_2 \in M \cap L,\ f_1 \rightarrow f_2 = 1$;
в) $f_1 \notin F_0 \cup L,\ f_2 \notin S,\ f_1 \rightarrow f_2 = 1$;
г) $f_1 \in (S \cap L) \setminus F_0,\ f_2 \in M \setminus (F_0 \cap L),\ f_1 \rightarrow f_2 = 1$.

Задачи к разделу III.

1. Показать, что в любом графе, имеющем не менее двух вершин, найдутся две вершины с одинаковыми степенями.

2. Существует ли 6-вершинный граф, имеющий такой набор степеней вершин $2, 2, 2, 4, 5, 5$?

3. Пусть $i_k(G)$ – число вершин степени k в графе G. Найти число попарно неизоморфных графов G, у которых:
а) $i_2(G) = i_3(G) = i_4(G) = 2,\ i_k(G) = 0$ при $k \neq 2, 3, 4$;
б) $i_2(G) = i_3(G) = i_4(G) = 3,\ i_k(G) = 0$ при $k \neq 2, 3, 4$.

4. Пусть $d_0(G)$ – минимальная из степеней графа G, имеющего n вершин.
а) Доказать, что если $d_0(G) \geq \dfrac{n-1}{2}$, то граф связен;
б) Можно ли в а) заменить $\dfrac{n-1}{2}$ на $\left[\dfrac{n-1}{2}\right]$?

5. Доказать, что связный граф с n вершинами содержит не менее $n-1$ ребер.

6. Доказать, что если в графе имеется ровно две вершины с нечетными степенями, то найдется цепь, соединяющая эти вершины.

7. Доказать, что если в графе степень каждой вершины больше единицы, то в нем есть цикл.

8. Доказать, что для всякого $n \geq 3$ существует n-вершинный связный граф, содержащий $n-1$ вершин с неравными друг другу степенями.

9. По заданному коду $\tilde{\alpha}$ построить корневое дерево:
а) $\tilde{\alpha} = (001010011011)$;
б) $\tilde{\alpha} = (0100011001101011)$;
в) $\tilde{\alpha} = (0001010110011011)$.

10. Доказать, что во всяком дереве с $n \geq 2$ вершинами содержится не менее двух висячих вершин.

4 Литература

1. Гаврилов Г. П., Сапоженко А. А. Задачи и упражнения по дискретной математике. — М.: Физматлит, 2004.
2. Гиндикин С. Г. Алгебра логики в задачах. — М.: Наука, 1972.
3. Грэхем Р., Кнут Д., Паташник О. Конкретная математика. — М.: Мир, 1998.
4. Дискретная математика и математические вопросы кибернетики. Т. 1. / Под ред. С. В. Яблонского и О. Б. Лупанова. — М.: Наука, 1974.
5. Зыков А. А. Теория конечных графов. — Новосибирск: Наука, 1969.
6. Избранные вопросы теории булевых функций. / Под ред. С. Ф. Винокурова и Н. А. Перязева. — М.: Физматлит, 2001.
7. Матросов В. Л., Стеценко В. Н. Лекции по дискретной математике. — М.: МПГУ, 1997.
8. Новиков Ф. А. Дискретная математика для программистов. — Спб.: Питер, 2002.
9. Оре О. Теория графов. — М.: Наука, 1980.
10. Редькин Н. П. Дискретная математика. — Спб.: Лань, 2003.
11. Сачков В. Н. Введение в комбинаторные методы дискретной математики. — М.: Наука, 1972.
12. Харари Ф. Теория графов. — М.: Мир, 1973.
13. Холл М. Комбинаторика. — М.: Мир, 1970.
14. Шоломов Л. А. Основы теории дискретных логических и вычислительных устройств. — М.: Наука, 1980.
15. Яблонский С. В. Введение в дискретную математику. — М.: Высшая школа, 2001.
16. Яблонский С. В., Гаврилов Г. П., Кудрявцев В. Б. Функции алгебры логики и классы Поста. — М.: Наука, 1966.

Методические указания по изучению курса

Учебное пособие рассчитано для студентов математических специальностей университета.

Цель изучения курса заключается в формировании прочной теоретической базы, необходимой будущему специалисту в его профессиональной деятельности, воспитании общей математической культуры.

Задачи курса:

- изучение основных разделов дискретной математики;
- выявление особенностей и связей, как между разделами дискретной математики, так и с другими математическими дисциплинами;
- формирование представления об основных дискретных структурах и функциональных системах;
- овладение основными методами дискретной математики.

Данное пособие предназначено для реализации поставленной цели и задач, особое внимание обращается на:

- самостоятельную работу студентов;
- практические занятия;
- контроль знаний, умений и навыков, приобретенных студентами в процессе работы над курсом.

При изучении курса используются материалы дисциплины «Математический анализ»: сведения о множествах, отношения, отображения и функции.

Пособие призвано помочь студентам в более глубоком, детальном усвоении сложного теоретического материала, поэтому доказательства теорем, лемм, следствий тщательно разобраны и изложены.

Также в пособии дается список необходимой для изучения литературы, задачи для самостоятельного решения, список вопросов к экзамену, контрольная работа, примерная тематика рефератов и курсовых работ, рабочая программа курса.

После изучения курса студент должен знать:

- основные комбинаторные объекты и комбинаторные числа, их свойства;
- основы теории графов: способы представления, виды графов, их свойства;

- основы теории булевых функций: способы задания булевых функций, разложение функций по переменным, совершенные нормальные формы, замкнутые классы булевых функций, критерий полноты множества булевых функций;

Программа курса

Пояснительная записка

Программа курса «Дискретная математика» предназначена для студентов 4 курса очного отделения, обучающихся по специальности «Математика».

Курс «Дискретная математика» читается студентам четвертого курса и обеспечивает освоение ими основных понятий, идей и методов дискретной математики, а также приобретение студентами практических навыков формализации прикладных задач.

Курс опирается на курс «Математический анализ». Он используется при изучении курсов «Основы программирования», «Базы данных», «Интеллектуальные системы», а также в спецкурсах и спецсеминарах.

Курс «Дискретная математика» читается в седьмом семестре. Общий объем курса - 90 ч., из них лекции - 36 ч., практические (лабораторные) занятия - 18 ч., самостоятельная работа студентов - 36 ч.

В течение обучения проводятся контрольная работа и экзамен.

Кроме этого студентам предлагаются темы для рефератов и курсовых работ.

Содержание

Тема 1. Элементы комбинаторики. Размещения, перестановки, сочетания. Треугольник Паскаля. Биномиальные коэффициенты и их свойства. Полиномиальная теорема. Принцип включения-исключения.

Тема 2. Определение и методы представления булевых функций. Упорядочение двоичных наборов. Определение и методы представления булевых функций. Число булевых функций фиксированной размерности. Унарные и бинарные булевы функции. Определение термов. Функция, представимая термом. Эквивалентность термов.

Остаточные функции. Существенные и фиктивные переменные. Леммы о подстановке и замене. Двойственные функции и двойственные термы. Принцип двойственности. Основные эквивалентности термов над множеством бинарных функций.

Тема 3. Разложение и канонические формы булевых функций. Теорема о разложении функций по переменным. Канонические формы булевых функций: совершенная дизъюнктивная нормальная форма, совершенная конъюнктивная нормальная форма, совершенная полиномиальная конъюнктивно-нормальная форма, полином Жегалкина. Методы нахождения канонических форм.

Тема 4. Замкнутость и полнота множеств булевых функций. Замыкание множества булевых функций. Замкнутые множества. Лемма о сводимости базисов. Замкнутость множеств, сохраняющих 0 и сохраняющих 1. Монотонные функции. Замкнутость множества монотонных функций. Самодвойственные функции. Замкнутость множества самодвойственных функций. Линейные функции. Замкнутость множества линейных функций. Леммы о немонотонной функции, о несамодвойственной функции, о нелинейной функции. Полные множества булевых функций. Критерий Поста полноты множества булевых функций.

Тема 5. Определение и способы задания графов. Псевдографы, графы. Способы задания. Операции над графами. Изоморфизм графов. Ориентированные графы. Связность графов. Задание графов пространственной диаграммой без пересечения ребер.

Тема 6. Планарность и раскраска графов. Плоские и планарные графы. Теорема Эйлера. Гомеоморфизм графов. Теорема Понтрягина-Куратовского. Раскраска графов. Хроматическое число графа. Лемма о существовании вершины степени не более 5. Теорема о пяти красках.

Тема 7. Сети. Потоки в сетях. Двудольные графы. Теорема Холла о паросочетании в двудольном графе. Направленные графы. Определение сети. Потоки в сетях. Теорема Форда-Фалкерсона о максимальной величине потока в сети.

Тема 8. Деревья. Теорема об эквивалентных условиях понятия дерева. Нумерованные деревья. Теорема Кюли о числе деревьев с занумерованными вершинами.

Тема 9. Обходы графов. Эйлеровы циклы и эйлеровы графы. Критерий эйлеровости графа. Гамильтоновы циклы и гамильтоновы графы. Признак гамильтоновости графа.

Название тем, объем в часах

№	Название тем	лекции	практ	сам. раб.	всего
1	Элементы комбинаторики	4	2	4	10
2	Определение и методы представления булевых функций	4	2	4	10
3	Разложения и канонические формы булевых функций	4	2	4	10
4	Замкнутость и полнота множеств булевых функций	4	2	4	10
5	Определение и способы задания графов	4	2	4	10
6	Планарность и раскраска графов	4	2	4	10
7	Сети. Потоки в сетях	4	2	4	10
8	Деревья	4	2	4	10
9	Обходы графов	4	2	4	10
	Всего	36	18	36	90

Список тем рефератов и курсовых работ.

Темы рефератов:

1. Графы
2. Деревья
3. Асимптотическая оценка сложности булевых функций в базисе $\{\&, \vee, -\}$. Метод Лупанова
4. Числа Стирлинга
5. Числа Эйлера
6. Числа Белла
7. Метод производящих функций

8. Дискретные экстремальные задачи

Темы курсовых работ:

1. Дифференциальное исчисление булевых функций
2. Реализация булевых функций бесповторными термами
3. Замкнутые классы булевых функций
4. Минимизация булевых функций в классе ДНФ
5. Разложение булевых функций в ряды и канонические полиномиальные формы
6. Методы синтеза схем из функциональных элементов

Вопросы к экзамену

1. Размещения, перестановки, сочетания - основные комбинаторные формулы.
2. Треугольник Паскаля. Биномиальные тождества.
3. Основные комбинаторные тождества.
4. Принцип включения - исключения.
5. Упорядочение двоичных наборов. Определение и методы представления булевых функций. Число булевых функций фиксированной размерности.
6. Унарные и бинарные булевы функции.
7. Определение термов. Значение, глубина, множество переменных термов. Множество подтермов. Функция, представляющаяся термом, эквивалентность термов. Упорядоченные термы.
8. Остаточные функции. Существенные и фиктивные аргументы. Лемма о существенном аргументе.
9. Леммы о подстановке и замене.
10. Двойственные функции и двойственные термы. Принцип двойственности.
11. Основные эквивалентности термов над множеством бинарных функций.
12. Теорема о разложении функции по переменным. Конъюнктивные, дизъюнктивные и полиномиальные разложения функций по переменным.
13. Канонические формы булевых функций: СДНФ и СКНФ.
14. Канонические формы булевых функций: СПКНФ и ПЖ.
15. Замкнутые множества булевых функций. Предложения и леммы для множеств, сохраняющих 0 и сохраняющих 1.

16. Замкнутые множества булевых функций. Предложения и леммы для множества линейных функций.

17. Замкнутые множества булевых функций. Предложения и леммы для множества самодвойственных функций.

18. Замкнутые множества булевых функций. Предложения и леммы для множества монотонных функций.

19. Критерий полноты множества булевых функций.

20. Псевдографы, графы. Способы задания. Изоморфизм графов. Ориентированные графы.

21. Задание графов диаграммами. Задание пространственной диаграммой без пересечения ребер.

22. Плоские и планарные графы. Теорема Эйлера.

23. Два примера не планарных графа. Гомеоморфизм графов. Теорема Понтрягина - Куратовского (без доказательства).

24. Лемма о существовании вершины степени не более 5.

25. Теорема о пяти красках.

26. Сети. Потоки в сетях. Теорема Форда-Фалкерсона.

27. Деревья. Теорема о эквивалентных условиях понятия дерева.

28. Нумерованные деревья. Теорема Кэли .

29. Эйлеровы графы. Критерий.

30. Гамильтоновы графы. Признак.

Контрольная работа

Вариант 1.

1. Сколькими способами из 28 костей домино можно выбрать две кости так, чтобы их можно было приложить друг к другу?

2. Найти число целых положительных чисел, не превосходящих 1000 и не делящихся ни на одно из чисел 6, 10 и 15.

3. Для функции $f = (01000111)$ найти СДНФ, СКНФ и полином Жегалкина.

4. Используя критерий полноты, установить, является ли следующее множество булевых функций $\{\&, \rightarrow, (01110001)\}$ полным.

5. Доказать, что если в графе степень каждой вершины больше единицы, то в нем есть цикл.

Вариант 2.

1. Бросают три игральные кости. Сколькими способами они могут упасть так, что либо все оказавшиеся вверху грани одинаковы, либо все попарно различны?

2. Найти число целых положительных чисел, не превосходящих 1000 и не делящихся ни на одно из чисел 3, 5 и 7.

3. Для функции $f = (01000111)$ найти СДНФ, СКНФ и полином Жегалкина.

4. Используя критерий полноты, установить, является ли следующее множество булевых функций $\{\vee, \rightarrow, (11100010)\}$ полным.

5. Доказать, что во всяком дереве с $n \geq 2$ вершинами содержится не менее двух висячих вершин.

Учебное издание

Шаранхаев Иван Константинович
e-mail: goran5@mail.ru, тел. 21-97-57

ЭЛЕМЕНТЫ ДИСКРЕТНОЙ МАТЕМАТИКИ

Учебное пособие

Редактор И.Х. Оширова
Компьютерный набор и верстка автора

Свидетельство РПУ-У №1020300970106 от 18.10.02.

Подписано в печать 15.12.05. Формат 60×84 1/16.
Уч.-изд. л. Усл. п. л. Заказ №1544.
Тираж 50 экз.

Издательство Бурятского госуниверситета
670000, г. Улан-Удэ, ул. Смолина, 24а.