ОГЛАВЛЕНИЕ

ГЛАВА 1. МНОЖЕСТВА. ОТНОШЕНИЯ. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ 5
1.1. Множества 5
1.2. Теоретико-множественные операции 10
1.3. Отношения 15
1.4. Отображения (функции). Биекции 20
1.5. Подстановки, перестановки 24
1.6. Алгебраические структуры 30
Задачи к главе 1 48
ГЛАВА 2. КОМБИНАТОРИКА 49
2.1. Предварительные определения. Метод математической индукции 49
2.2. Комбинаторные числа 50
2.3. Разбиения 60
2.4. Производящие функции 75
2.5. Формула включения-исключения 89
2.6. Теория Пойа 96
Задачи к главе 2 103
ГЛАВА 3. БУЛЕВЫ ФУНКЦИИ 106
3.1. Булевы функции, основные понятия 106
3.2. Операции над булевыми переменными (логические связки) 113
3.3. Дизъюнктивные и конъюнктивные нормальные формы булевой функции 119
3.4. Минимизация ДНФ 128
3.5. Самодвойственные, монотонные и линейные функции. Полиномы Жегалкина 133
3.6. Классы Поста 144
Задачи к главе 3 150
ГЛАВА 4. ГРАФЫ 152
4.1. Основные понятия и определения 152
4.2. Связность графа 157
4.3. Планарные графы 161
4.4. Эйлеровы и гамильтоновы графы 163

4.5. Описание классов графов с помощью запрещенных миноров 168
4.6. Раскраска графов 169
Задачи к главе 4 171
ЛИТЕРАТУРА 175

ГЛАВА 1. МНОЖЕСТВА. ОТНОШЕНИЯ. АЛГЕБРАИЧЕСКИЕ СТРУКТУРЫ

1.1. Множества

Теория множеств была создана в конце 19-го века усилиями немецких математиков Г. Кантора и Р. Дедекинда как исчисление бесконечных количеств.

Определение (Георга Кантора). *Множество – это собрание определенных и различимых между собой объектов нашей интуиции или интеллекта, мыслимых как единое цело.*

В центре внимания дискретной математики находятся множества, состоящие из конечного числа элементов - конечные множества.

Общий метод задания множества состоит в указании некоторого характеристического свойства, которым обладают элементы множества и только они.

Примеры:

1) множество всех четных натуральных чисел;

2) множество действительных корней уравнения $x^2 - x - 2 = 0$;

3) множество точек на плоскости, удаленных от точки O не более чем на 3 единицы расстояния.

Конечное множество может быть задано и простым перечислением его элементов, которое принято записывать в фигурных скобках.

Например: $A = \{a_1, \dots, a_n\}$.

Порядок перечисления элементов не существенен.

Например, множество простых чисел меньших 10 может быть задано различными перечислениями: $\{2; 3; 5; 7\} = \{7; 3; 2; 5\} = \{3; 7; 5; 2\}$ и другими (всего 24 варианта).

Множество, не содержащее элементов, называется *пустым множеством,* которое обозначается знаком: $\emptyset$.

Если каждый элемент множества B является элементом множества A, то B называют *подмножеством* множества A, обозначение: $B \subseteq A$. При этом, если $B \neq A$, то B называют *собственным подмножеством* множества A и обозначают $B \subset A$.

Теорема. У конечного множества, состоящего из n элементов, имеется ровно 2^n различных подмножеств.

Доказательство. Рассмотрим множество $A = \{a_1, \dots, a_n\}$. Рассмотрим

подмножество $B \subseteq A$. Поставим в соответствие подмножеству B упорядоченный двоичный набор длины n (*характеристический вектор*) $\chi(B) = (\beta_1, \dots, \beta_n)$, в котором $\beta_i = 1$, если $a_i \in B$, и $\beta_i = 0$, если $a_i \notin B$.

Например, если $A = \{a_1, a_2, a_3, a_4, a_5\}$ и $B = \{a_1, a_4, a_5\}$, то $\chi(B) = (1,0,0,1,1)$.

Пустому подмножеству соответствует набор из n нулей, а всему множеству $A \subseteq A$ соответствует набор из n единиц.

Очевидно, что каждому подмножеству $B \subseteq A$ однозначно соответствует двоичный набор длины n, и разным подмножествам A соответствуют разные наборы. Поэтому различных подмножеств множества A столько же сколько различных двоичных наборов длины n.

Двоичный набор длины n можно понимать как двоичную запись целого числа, расположенного в диапазоне от 0 до $2^n - 1$. Таких целых чисел ровно 2^n штук.

Теорема доказана.

Определение. Количество элементов в конечном множестве назовем *мощностью* этого множества.

Обозначение: $|A|$ - мощность множества A (используется также обозначение $card(A)$).

Попытаемся теперь распространить понятие мощности на бесконечные множества.

Два множества назовем *равномощными,* если между элементами этих множеств можно установить взаимно однозначное соответствие, такое, что

1) каждому элементу первого множества соответствует какой-то элемент второго множества,

2) каждому элементу второго множества соответствует какой-то элемент первого множества,

3) разным элементам одного множества соответствуют разные элементы другого.

Очевидно, что два конечных множества будут равномощными в смысле данного определения только тогда, когда они имеют одинаковое количество элементов.

Определение. Множество, равномощное натуральному ряду $\mathbb{N} = \{1,2,3, \dots\}$ называется *счетным.* (Его элементы можно «пересчитать»,

выстроить в последовательность $A = \{a_1, a_2, a_3, \dots\}$.)

Утверждение. Бесконечное подмножество счетного множества является счетным множеством.

Доказательство. Упорядочим в последовательность элементы рассматриваемого счетного множества. Пусть $A = \{a_1, a_2, a_3, \dots\}$, и $B \subseteq A$, причем $B = \{a_{i_1}, a_{i_2}, a_{i_3}, \dots\}$. Множество B очевидно счетно.

Теорема. Объединение счетного набора счетных множеств является счетным множеством.

Доказательство. Мы имеем последовательность последовательностей. Выстроим в последовательность все элементы этого объединения способом, указанным на картинке (рис. 1.1).

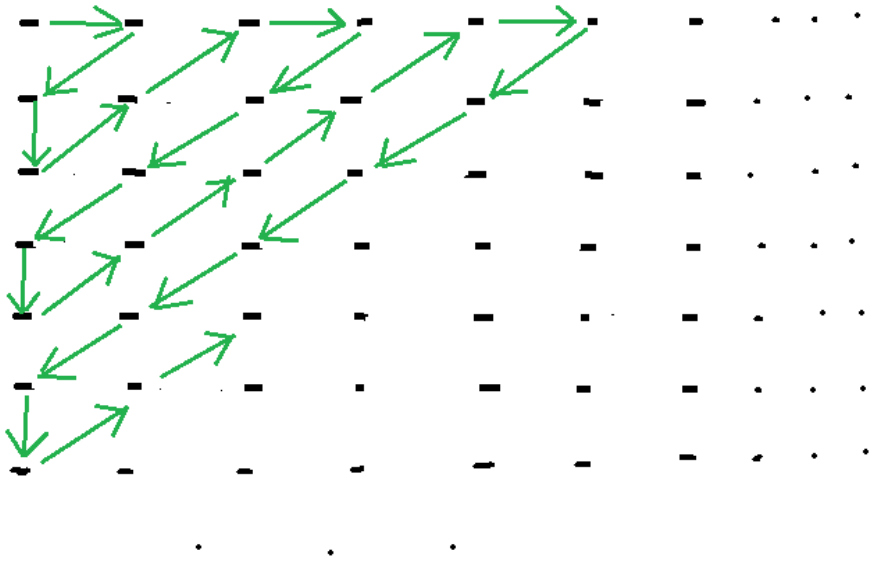


Рисунок 1.1

Эта же схема может быть применена для доказательства того, что объединение конечного числа счетных множеств счетно.

Совсем легко доказать, что объединение счетного и конечного множества будет счетным множеством.

Утверждение. Множество всех обыкновенных положительных дробей счетно.

Доказательство. Это множество является объединением счетного числа счетных множеств: дробей со знаменателем 1, дробей со знаменателем 2, дробей со знаменателем 3 и так далее.

Утверждение. Множество $\mathbb{Q}$ всех рациональных чисел счетно.

Доказательство. Каждое положительное рациональное число однозначно представляется в виде несократимой дроби, поэтому множество положительных

рациональных чисел является подмножеством множества всех дробей, которое счетно.

Итак, множество всех положительных рациональных чисел счетно, аналогично множество всех отрицательных рациональных чисел счетно.

Все множество $\mathbb{Q}$, поэтому, также будет счетным.

Теорема (Г. Кантор). Множество $\mathbb{R}$ всех действительных чисел *несчетно.*

Доказательство. Предположим, что $\mathbb{R}$ - счетное множество. Рассмотрим множество A всех бесконечных десятичных дробей вида: $0, d_1 d_2 d_3 \ldots$, где каждая из цифр d_i равна нулю или единице.

Различные элементы A будут задавать различные действительные числа, поэтому мы можем считать, что A является подмножеством $\mathbb{R}$. По нашему предположению $\mathbb{R}$ счетно, поэтому и его подмножество A также счетно.

Выстроим всё это множество A в последовательность:

$$0, \boxed{d_{1;1}} d_{1;2} d_{1;3} \ldots$$
$$0, d_{2;1} \boxed{d_{2;2}} d_{2;3} \ldots$$
$$0, d_{3;1} d_{3;2} \boxed{d_{3;3}} \ldots$$
$$\ldots$$

Эта последовательность бесконечных десятичных дробей должна по нашему предположению содержать все элементы множества A.

Рассмотрим дробь $0, c_1 c_2 c_3 \ldots$, в которой $c_i = 0$, если $d_{i;i} = 1$ и, наоборот, $c_i = 1$, если $d_{i;i} = 0$.

Эта дробь является элементом множества A, но не может присутствовать в указанной последовательности элементов множества поскольку она отличается от i-ой дроби этой последовательности i-ой цифрой после запятой.

Таким образом, указанная последовательность не может содержать всех элементов множества A, то есть множество A не является счетным, а поэтому и все множество $\mathbb{R}$ не является счетным.

Определение. *Мощность* – это обобщение понятия *количества* на бесконечные множества. Будем говорить, что равномощные множества имеют одинаковую мощность.

Мощность счетных множеств будем обозначать $\aleph_0$ (алеф-нуль).

Мощность множеств равномощных $\mathbb{R}$ будем называть *мощностью континуума,* и обозначать буквой C.

Можно доказать, что множество $\mathbb{R}$ равномощно множеству всех подмножеств натурального ряда. Этот факт, по аналогии с конечной ситуацией, записывают в виде равенства $2^{\aleph_0} = \mathfrak{C}$.

Континуум-гипотеза $\aleph_1 = \mathfrak{C}$

Является ли $\mathfrak{C}$ следующей за $\aleph_0$ бесконечной мощностью? Иначе говоря, существует ли мощность промежуточная между $\aleph_0$ и $\mathfrak{C}$?

Этот вопрос был поставлен еще Кантором в конце 19 века. Вопрос оказался неразрешимым в рамках «наивной теории множеств».

В начале 20-го века (в частности, для преодоления парадоксов теории множеств) были созданы аксиоматические варианты теории множеств. Общепринятой аксиоматикой стала аксиоматика Цермело-Френкеля (ZF).

В 30-е годы 20-го века немецкий математик Гёдель доказал, что континуум-гипотеза не противоречит аксиомам системы ZF.

В 60-е годы 20-го века американский математик Коэн доказал, что и отрицание континуум-гипотезы не противоречит аксиомам системы ZF.

Таким образом, континуум-гипотеза является утверждением, не зависящим от аксиом системы ZF.

Теорема. Для любого множества A мощность множества всех подмножеств множества A больше мощности множества A ($2^{|A|} > |A|$).

Доказательство. Предположим, что существует взаимно однозначное соответствие f между элементами множества A и элементами $P(A)$ −множества все подмножеств множества A. Обозначим буквой D множество всех таких $x \in A$, для которых $x \notin f(x)$. Пусть $d \in A$ - элемент, соответствующий множеству D при соответствии f, то есть $f(d) = D$.

Будет ли этот элемент принадлежать множеству D?

Если $d \notin D$, то по определению множества D будет выполнено $d \in D$.
И наоборот: если $d \in D$, то $d \notin D$. Получили противоречие. Следовательно, не существует взаимно-однозначного соответствия f.

Теорема доказана.

1.2. Теоретико-множественные операции

Объединение множеств

Определение. Множество, состоящее из элементов, входящих хотя бы в одно из множеств A или B называется *объединением* этих множеств и обозначается $A \cup B$ (рис. 1.2).

Значок ∪ - это стилизованная латинская буква U – первая буква в слове UNION. До середины 20-го века для объединения множеств использовался термин «сумма множеств» и значок «+».

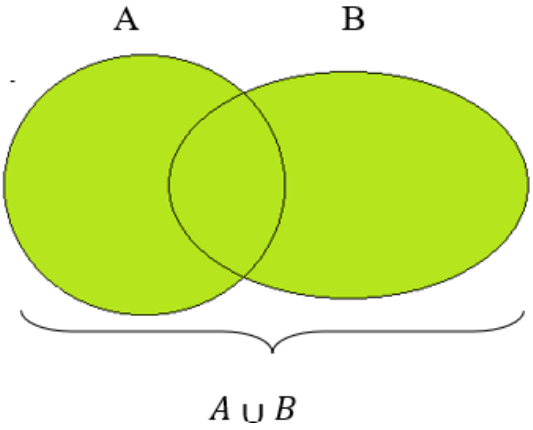


Рисунок 1.2

Пересечение множеств

Определение. Множество, состоящее из элементов, входящих в каждое из множеств A и B, называется *пересечением* этих множеств и обозначается $A \cap B$ (рис. 1.3).

Значок ∩ - это перевернутый значок ∪. До середины 20-го века для пересечения множеств использовался термин «произведение множеств» и значок «•». Новые обозначения для объединения и пересечения подчеркивают *двойственность* этих операций (это обсудим позже).

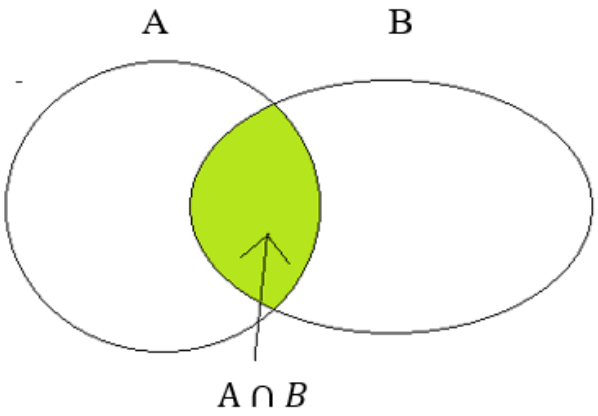


Рисунок 1.3

Разность множеств

Определение. Множество, состоящее из элементов множества A, не входящих в множество B, называется *разностью* этих множеств и обозначается $A \backslash B$ (рис. 1.4).

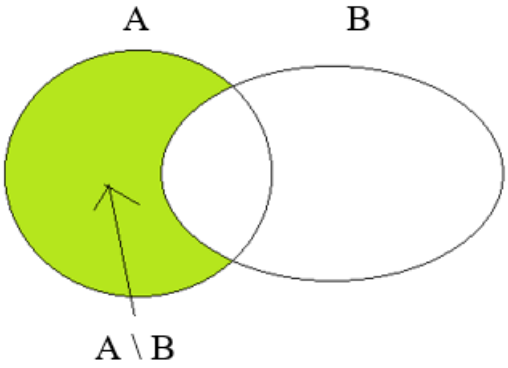


Рисунок 1.4

Симметрическая разность множеств

Определение. Множество, состоящее из элементов, входящих ровно в одно из множеств A или B, называется *симметрической разностью* этих множеств и обозначается $A \triangle B$ или $A \oplus B$.

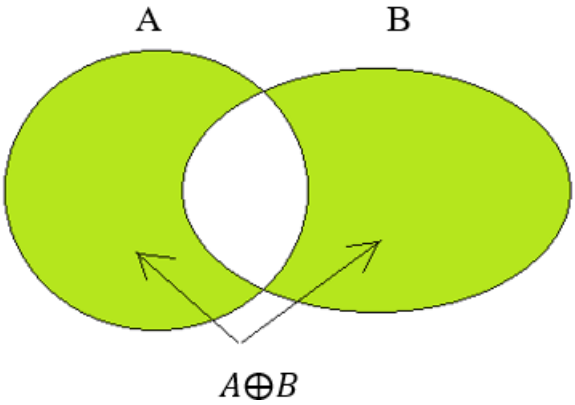


Рисунок 1.5

Операция дополнения

Очень часто мы работаем с множествами, являющимися подмножествами какого-то общего для них объемлющего множества («универсума») U.

Дополнением к множеству A в этом универсуме называется множество $\overline{A} = U \backslash A$. Оно состоит из всех элементов U, не принадлежащих A (рис. 1.6).

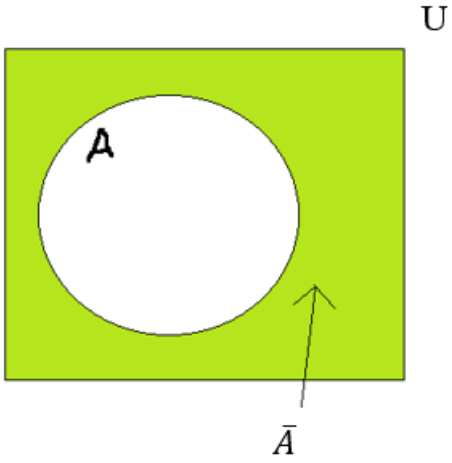


Рисунок 1.6

Свойства теоретико-множественных операций

1) Коммутативность объединения и пересечения

$$A \cup B = B \cup A,$$

$$A \cap B = B \cap A;$$

2) Ассоциативность объединения и пересечения

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

$$(A \cap B) \cap C = A \cap (B \cap C);$$

3) Дистрибутивность пересечения относительно объединения и объединения относительно пересечения

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

4) Формулы де Моргана

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

Здесь мы можем увидеть *двойственность* операций объединения и пересечения: во всяком из тождеств мы можем подменить объединение на пересечение и пересечение на объединение – тождество сохранит свою силу.

Такой двойственности нет у операций сложения и умножения чисел. Например, $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$, но $a + (b \cdot c) \neq (a + b) \cdot (a + c)$.

Рассмотренные свойства легко доказываются. Чтобы «прочувствовать» эти свойства можно использовать «диаграммы Эйлера». Например, прочувствуем дистрибутивность пересечения относительно объединения (рис. 1.7):

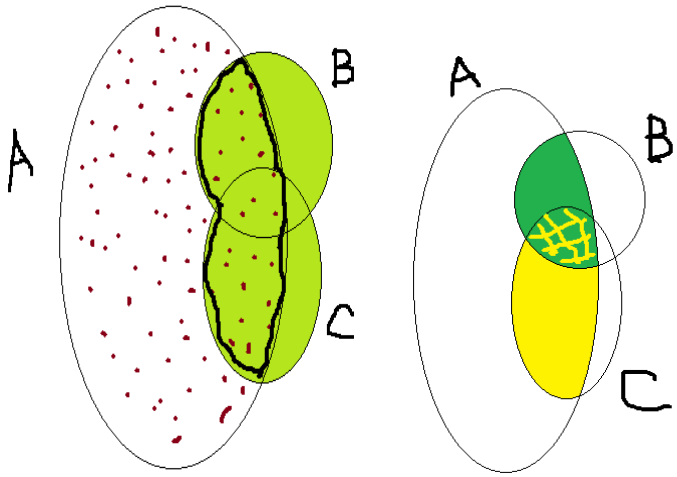


Рисунок 1.7

Заметим, что использование диаграмм Эйлера (Эйлера - Венна) ограничено случаем рассмотрения 3-х множеств. Для случая 4-х множеств здесь придется использовать объемные тела в пространстве (что уже неудобно), а при рассмотрении большего числа множеств моделирование придется производить в 4-х (и более) –мерном пространстве ☺!

Для доказательства теоретико-множественных тождеств с большим числом множеств можно использовать теорию булевых функций. К этому вопросу мы вернемся позже в нашем курсе.

Декартово произведение множеств

Определение. *Декартовым произведением* множеств A и B называется множество упорядоченных пар: $A \times B = \{(a; b): a \in A, b \in B\}$.

Пример:

$A = \{Петя; Вася\}$, $B = \{Маша; Лена\}$,

$A \times B = \{(Петя; Маша), (Петя; Лена), (Вася; Маша), (Вася; Лена)\}$.

Множество $\mathbb{R}^n$

Определение. $\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x; y): x \in \mathbb{R}, y \in \mathbb{R}\}$ - множество всех упорядоченных пар действительных чисел, которое можно отождествить с множеством всех точек плоскости, на которой введена декартова система координат. (Отсюда и термин *декартово произведение*).

$\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x; y; z): x \in \mathbb{R}, y \in \mathbb{R}, z \in \mathbb{R}\}$ - множество всех упорядоченных троек действительных чисел, которое можно отождествить с множеством всех точек геометрического пространства, в котором введена декартова система координат.

$\mathbb{R}^n = \mathbb{R} \times \mathbb{R} \times \ldots \times \mathbb{R} = \{(x_1; x_2; \ldots, x_n): x_i \in \mathbb{R}\}$ - множество всех упорядоченных n-ок действительных чисел, которое можно отождествить с множеством всех точек геометрического n-мерного пространства.

Бинарный куб $\mathbf{B^n}$

Пусть $\mathbf{B} = \{0; 1\}$.

$\mathbf{B^n} = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n): x_i \in \mathbf{B}\}$ - множество упорядоченных наборов длины n, состоящих из нулей и единиц.

Если считать эти наборы координатами точек в пространстве, то элементы $\mathbf{B}^n$ являются вершинами n-мерного куба (рис. 1.8. а, 1.8. б).

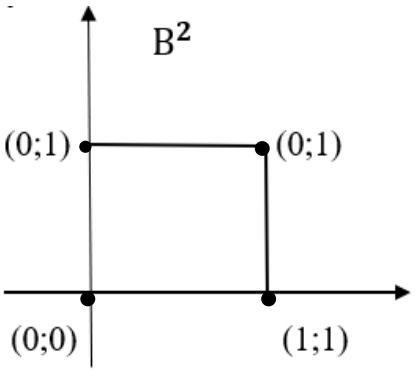


Рисунок 1.8. а

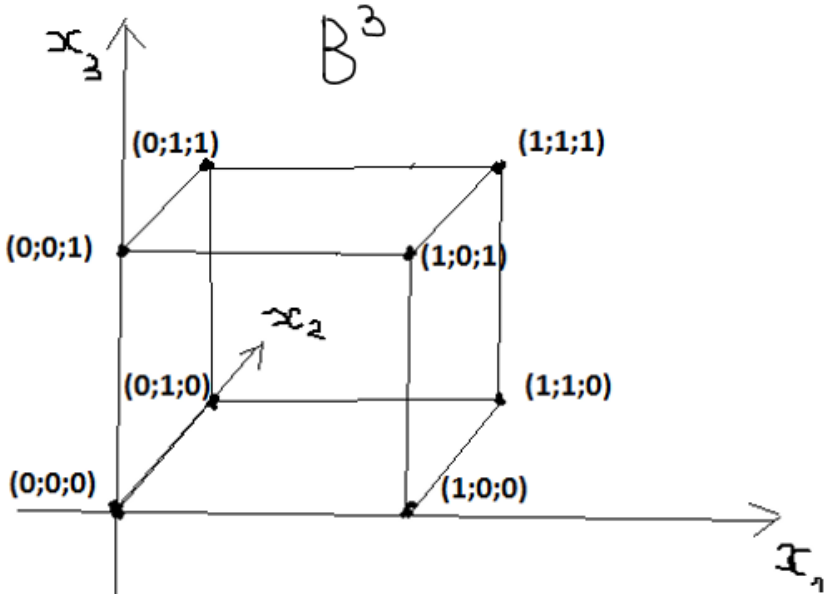


Рисунок 1.8. б

Мы будем использовать бинарный куб позднее в нашем курсе в теории булевых функций.

1.3. Отношения

Определение. Подмножество R декартового произведения $A \times B$ называется *отношением* между элементами множеств A и B.

Вместо $(a; b) \in R$ часто пишут aRb.

В случае, когда $A = B$, говорят о *бинарном отношении* на множестве A.

Примеры:

1) Бинарное отношение R на множестве действительных чисел $\mathbb{R}$ определено условием: $(x, y) \in R \Leftrightarrow x^2 + y^2 \leq 25$ (рис. 1.9).

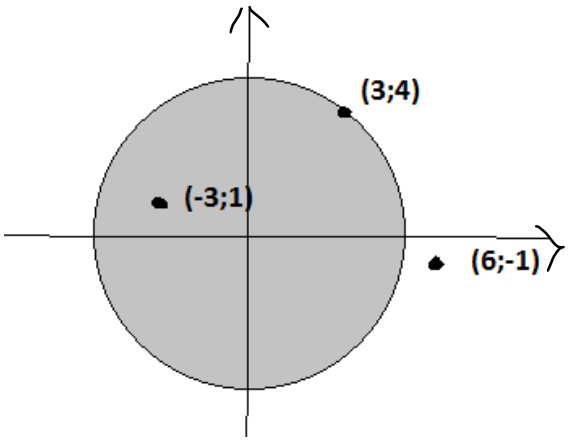


Рисунок 1.9

Для этого отношения $3R4$ и $(-3)R1$, но $6\boxed{R}(-1)$, или в другой записи: $(3;4) \in R$ и $(-3;1) \in R$, но $(6;-1) \notin R$.

2) Бинарное отношение " $\leq$ " на множестве натуральных чисел $\mathbb{N} = \{1,2.3,\dots\}$.

3) Бинарное отношение " $\equiv$ "$(mod\,3)$ на множестве $\mathbb{Z}$ всех целых чисел. Например: $16 \equiv 7(mod\,3)$, но $16 \boxed{\equiv} 17(mod\,3)$.

Два целых числа находятся в этом отношении, если они дают одинаковые остатки при делении на 3 (это будет тогда, когда их разность делится на 3).

Свойства бинарных отношений

Рефлексивность:

$\forall x \in A \quad (x,x) \in R;$

Иррефлексивность:

$\forall x \in A \quad (x,x) \notin R;$

Симметричность:

$(x,y) \in R \Rightarrow (y,x) \in R;$

Асимметричность:

$(x,y) \in R \Rightarrow (y,x) \notin R;$

Антисимметричность:

$$\left.\begin{matrix}(x,y) \in R\\(y,x) \in R\end{matrix}\right\} \Rightarrow x = y;$$

Транзитивность:

$$\left.\begin{matrix}(x,y) \in R\\(y,z) \in R\end{matrix}\right\} \Rightarrow (x,z) \in R.$$

Отношение " $\leq$ " на множестве действительных чисел является рефлексивным.

Отношение $(x,y) \in R <=> x^2 + y^2 \leq 25$ (пример 1) на множестве действительных чисел не является рефлексивным.

Отношение " $<$ " на множестве действительных чисел является иррефлексивным.

Отношение $(x,y) \in R \Leftrightarrow x^2 + y^2 \leq 25$ (пример 1) на множестве действительных чисел является симметричным.

Отношение " $\equiv$ "$(mod\,3)$ на множестве $\mathbb{Z}$ всех целых чисел (пример 2) является симметричным.

Отношение $(x,y) \in R \Leftrightarrow x > y - 3$ на множестве целых чисел не является симметричным.

Отношение " $<$ " на множестве действительных чисел является асимметричным.

Отношение " $\leq$ " на множестве действительных чисел не является асимметричным.

Отношение " $\leq$ " на множестве действительных чисел является антисимметричным.

Отношение равенства на множестве обыкновенных дробей является транзитивным.

Отношение $(x, y) \in R \Leftrightarrow x > y - 3$ на множестве целых чисел не является транзитивным ($1 > 3 - 3;\ 3 > 5 - 3$, но $1 \boxed{>} 5 - 3$).

Отношение эквивалентности

Определение. Рефлексивное, симметричное и транзитивное отношение называется *отношением эквивалентности*.

Для отношения эквивалентности часто используется значок " $\sim$ ".

Теорема. Отношение эквивалентности, заданное на множестве A, разбивает это множество на непересекающиеся подмножества (классы эквивалентности). Любые два элемента, принадлежащие одному классу, будут эквивалентны между собой, два элемента из разных классов не будут эквивалентны.

Доказательство. Для каждого элемента a множества A, обозначим $K(a) = \{b: b \in A, b \sim a\}$.

Отметим сначала, что ввиду рефлексивности отношения эквивалентности, $\forall a \in A \quad a \in K(a)$ (рис. 1.10). Поэтому объединение всех классов эквивалнтности совпадает с множеством A.

Далее докажем, что $\forall c, d \in K(a) \quad c \sim d$. Это вытекает из симметричности и транзитивности отношения эквивалентности: $c \sim a, d \sim a$, поэтому $a \sim d$ (симметричность), далее тогда $c \sim d$ (транзитивность).

Теперь докажем, что если $K(a) \cap K(b) \neq \emptyset$, то $K(a) = K(b)$. Действительно, пусть элемент c принадлежит этому пересечению классов $K(a) \cap K(b)$. Тогда $c \sim a$ и $c \sim b$ и, следовательно, $a \sim b$, откуда вытекает, что $K(a) = K(b)$.

Итак, классы эквивалентности не пересекаются и накрывают все множество A. Элементы из разных классов, очевидно, не будут эквивалентны.

Теорема доказана.

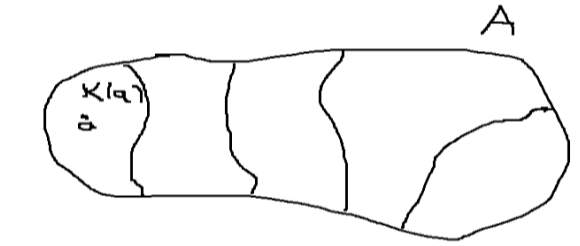


Рисунок 1.10

Множество классов эквивалентности называется *факторомножеством* множества A по отношению к данному отношению эквивалентности.

Примеры:

1) Отношение равенства дробей на множестве всех обыкновенных дробей является отношением эквивалентности. Факторомножество здесь – это множество всех *рациональных чисел.*

2) Отношение равенства закрепленных векторов на плоскости (вводимое, например, по правилу: $\overrightarrow{A_1B_1} = \overrightarrow{A_2B_2}$, если *середина* A_1B_2 = *середина* A_2B_1) является отношением эквивалентности. Факторомножество – множество всех свободных векторов на плоскости.

3) Отношение " $\sim$ " на множестве всех дифференцируемых на заданном интервале функций, определяемое так: $f_1(x) \sim f_2(x)$, если $f_1'(x) = f_2'(x)$ является отношением эквивалентности. Каждый класс эквивалентности – множество первообразных одной и той же функции (неопределенный интеграл этой функции).

3) Отношение " $\equiv$ "$(mod\ 3)$ на множестве $\mathbb{Z}$ всех целых чисел является отношением эквивалентности. Факторомножество – множество *классов вычетов по модулю 3*.

Отношение порядка

Определение. Рефлексивное, антисимметричное и транзитивное отношение называется *отношением порядка*.

Для отношения порядка часто используется значок " $\leq$ ".

Примеры:

1) Стандартное отношение " $\leq$ " на числовой прямой.

2) Отношение включения " $\subseteq$ " на множестве всех подмножеств данного множества является отношением порядка. Например, для $A = \{a, b, c\}$ так называемая диаграмма Хассе (рис. 1.11):

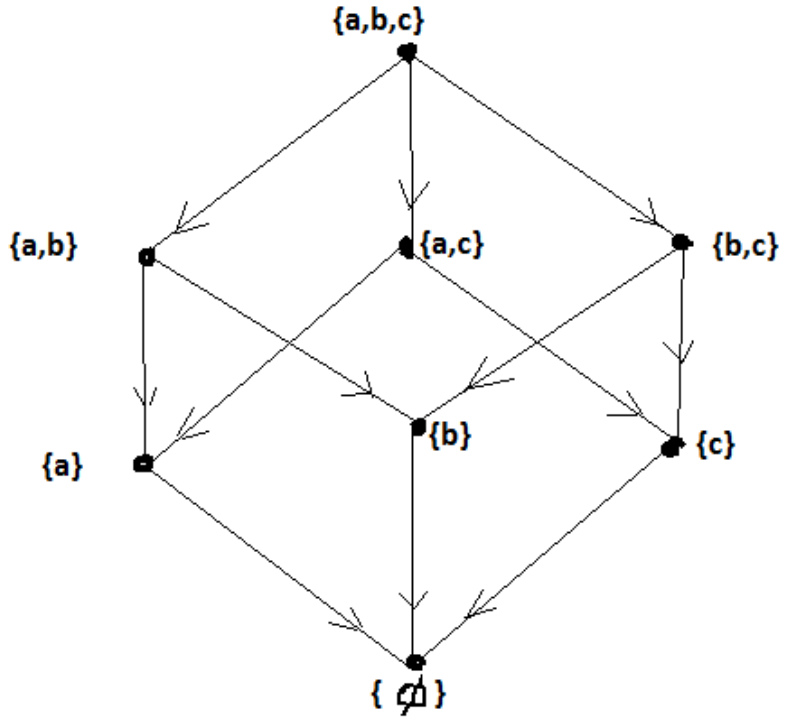


Рисунок 1.11

Отношение строгого порядка

Определение. Иррефлексивное, асимметричное и транзитивное отношение называется *отношением строгого порядка*.

Примеры:

1) Стандартное отношение " $<$ " на числовой прямой.

2) Отношение строгого включения " $\subset$ " на множестве всех подмножеств данного множества является отношением строго порядка.

Тернарные отношения. Отношение циклического порядка

Определение. *Тернарное отношение* на множестве A - это подмножество $A \times A \times A$ декартового куба множества A, то есть некоторое множество упорядоченных троек элементов этого множества.

Будем записывать то, что данная тройка находится в данном тернарном отношении так: $[a, b, c]$.

Определение. *Циклический порядок* – это тернарное отношение, удовлетворяющее свойствам:

цикличность: $[a, b, c] \Rightarrow [b, c, a]$,

асимметрия: $[a, b, c] \Rightarrow$ не $[c, b, a]$,

транзитивность: $[a, b, c]$ и $[a, c, d] \Rightarrow [a, b, d]$,

тотальность: $\forall$ различных $a, b, c \in A$ выполнено $[a, b, c]$ либо $[c, b, a]$.

Примеры:

1) Цифры на циферблате.

2) Дни недели.

3) Порядок перечисления осей в правых и левых системах координат в пространстве. Порядок перечисления векторов в правой и левой тройке векторов (рис. 1.12).

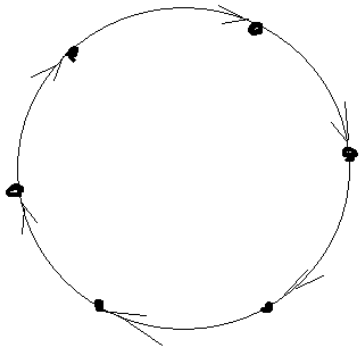


Рисунок 1.12

1.4. Отображения (функции). Биекции

Отображения (функции)

Определения. Рассмотрим отношение R между элементами множеств A и B, то есть подмножество декартового произведения $A \times B$.

Это отношение определяет *многозначное отображение (функцию)* f_R по следующему правилу:

1) *Областью определения* D этой функции f_R называется множество всех таких элементов $x \in A$, для каждого из которых найдется $y \in B$, такое, что $(x; y) \in R$. Область определения D является подмножеством множества A.

2) Для каждого $x \in A$ (многозначным) *значением (образом)* функции $f_R(x)$ на этом элементе называется множество всех таких $y \in B$, для которых $(x; y) \in R$.

Множество E всех таких $y \in B$, для каждого из которых найдется $x \in A$, такое, что $(x; y) \in R$, называется *множеством (областью) значений* функции f_R.

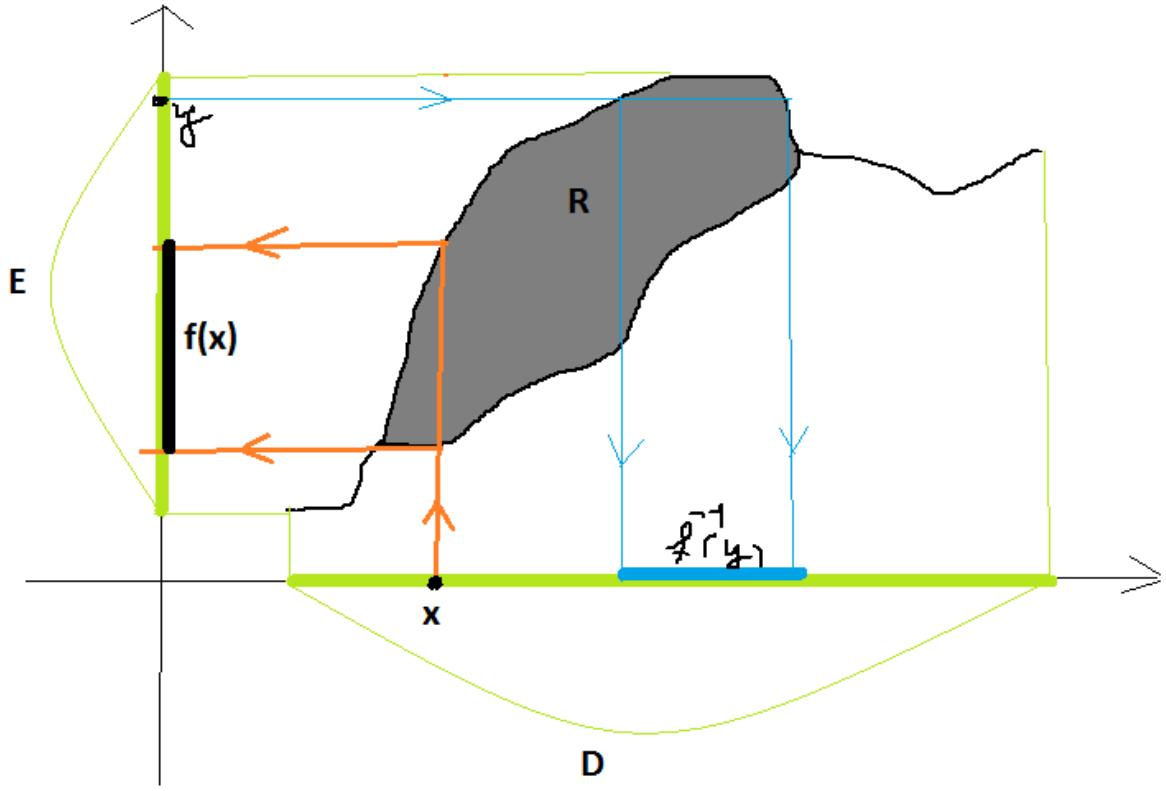


Рисунок 1.13

На рисунке $A = B = \mathbb{R}$ (рис. 1.13).

Если для каждого $x \in D$ образ $f_R(x)$ состоит из одного элемента, то f_R называют однозначным отображением (функцией). *По умолчанию отображение (функция) считается однозначным (однозначной).*

Прообразом $f_R^{-1}(y)$ элемента $y \in E$ называется множество всех $x \in A$, для которых $(x, y) \in R$.

Таким образом, каждое отношение R между элементами множеств A и B определяет (многозначную) функцию f_R.

И, наоборот, для (многозначной) функции f с областью определения $D \subseteq A$ и множеством значений $E \subseteq B$ определяется отношение R между элементами множеств A и B, для которого $f_R = f$.

Обозначение. Запись $f: A \to B$ означает, что рассматривается (однозначная) функция f с областью определения $D = A$ и множеством значений $E \subseteq B$.

Замечание. Термин *функция* обычно (но не обязательно) принято применять в случаях, когда B – это числовое множество.

Определения. Отображение $f: A \to B$ называется ***инъекцией***, если прообраз $f_R^{-1}(y)$ каждого элемента $y \in E$является одноэлементным множеством (взаимно однозначное вложение A в B).

Отображение $f: A \to B$ называется ***сюръекцией***, если $E = B$ (отображение A на всё B).

Отображение $f: A \to B$ называется ***биекцией***, если оно является инъективным и сюръективным (взаимно однозначное отображение A на всё B).

Определения. Рассмотрим отношение R между элементами множеств A и B, то есть подмножество декартового произведения $A \times B$.

Обратным отношением R^{-1} между элементами множеств B и A называется отношение, определяемое по правилу: $(b; a) \in R^{-1} \Leftrightarrow (a; b) \in R$.

Обратное отношение R^{-1} является подмножеством декартового произведения $B \times A$.

Для функции $f = f_R$ *обратной функцией* называется функция $f^{-1} = f_{R^{-1}}$.

Утверждение. Обратная функция для функции $f = f_R$ будет однозначной функцией только тогда, когда $f: D \to B$ будет инъекцией.

Доказательство. Образ $f^{-1}(y)$ каждого элемента $y \in E \subseteq B$ при отображении f^{-1} будет одноэлементным множеством только тогда, когда прообраз $f_R^{-1}(y)$ каждого элемента $y \in E$ будет одноэлементным множеством, то есть, когда $f: D \to B$ будет инъекцией.

Обратная функция к функции $f: A \to B$ будет иметь областью определения всё множество B только тогда, когда $E = B$, то есть, когда f - сюръекция. Поэтому имеет место следующее утверждение.

Утверждение. Обратная функция $f^{-1}: E \to A$ к функции $f: A \to B$ будет однозначной функцией $f^{-1}: B \to A$ только тогда, когда f - это биекция.

Определения

Рассмотрим 2 отношения:

1) отношение R_1 между элементами множеств A и B ,

2) отношение R_2 между элементами множеств B и C.

Композицией $R = R_1 \circ R_2$ этих *отношений* называется отношение между элементами множеств A и C, определяемое условием:

$(a; c) \in R \Leftrightarrow \exists b \in B: (a; b) \in R_1 \& (b; c) \in R_2$.

Рассмотрим 2 (однозначных) отображения:

1) $f_1: A \to B$,

2) $f_2: B \to C$.

Композицией $f = f_1 \circ f_2$ этих *отображений* называется отображение, соответствующее композиции отношений, соответствующих отображениям f_1 и f_2. Очевидно, что при этом $f: A \to C$, и $f(a) = f_2(f_1(a)) \ \forall a \in A$.

Отметим, что операция композиции отображений, очевидно, *обладает* свойством *ассоциативности*: $(f_1 \circ f_2) \circ f_3 = f_1 \circ (f_2 \circ f_3)$ и *не обладает* свойством коммутативности (даже для случая $A = B = C$), например, можно заметить, что $sin^2 x$ и $sin\, x^2$ - это различные функции.

Матрицы бинарных отношений на конечных множествах

Рассмотрим конечное множество $X = \{x_1, \dots, x_n\}$ и бинарное отношение R на элементах этого множества.

Определим матрицу этого отношения как квадратную матрицу $M_R = (m_{ij})$ размера $n \times n$, состоящую из нулей и единиц, по следующему правилу: $m_{ij} = 1$, если $(x_i, x_j) \in R$ и $m_{ij} = 0$, если $(x_i, x_j) \notin R$.

Определим операцию умножения* матриц отношений. Эта операция выполняется так же, как обычная операция умножения матриц, только вместо сложения применяется дизъюнкция. то есть: 0+0=0, 0+1=1, но 1+1=1.

Имеют место следующие, легко доказываемые, утверждения, которые бывают полезны при решении вопросов, связанных с отношениями на конечных множествах.

Утверждение. Матрица обратного отношения получается из матрицы исходного отношения применением операции транспонирования: $M_{R^{-1}} = M_R^T$.

Утверждение. Матрица композиции двух отношений получается из матриц этих отношений применением операции умножения «*»: $M_{R_1 \circ R_2} = M_{R_1} * M_{R_2}$.

Пример:

Пусть $X = \{x_1, x_2, x_3\}$,

$R = \{(x_1, x_2), (x_1, x_3), (x_2, x_1), (x_2, x_3), (x_3, x_2), (x_3, x_3)\}$.

$$M_R = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, M_{R^{-1}} = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix},$$

$$M_{R \circ R^{-1}} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} * \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}.$$

1.5. Подстановки, перестановки

Подстановки

Определение. Обозначим $\mathbb{N}_n = \{1; 2; \ldots; n\}$- множество натуральных чисел от 1 до n.

Рассмотрим биекцию $s: \mathbb{N}_n \to \mathbb{N}_n$. Эту биекцию можно задать таблицей с двумя строками: в первой строке в возрастающем порядке перечислены все элементы множества $\mathbb{N}_n = \{1; 2; \ldots; n\}$, во второй строке соответствующие значения $s(i)$. Эта таблица, описывающая биекцию s, называется *подстановкой* длины n:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ s(1) & s(2) & s(3) & \ldots & s(n) \end{pmatrix}.$$

Заметим, что во второй строке подстановки располагаются также все элементы множества $\mathbb{N}_n = \{1; 2; \ldots; n\}$, но, возможно, в другом порядке.

Примеры подстановок:

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix}$;

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$;

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix}$;

4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$;

5) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix}$.

Определение. Введем операцию *умножения* на множестве подстановок одинаковой длины. Операция *умножения подстановок* соответствует операции композиции функций. Подстановка $\sigma = \sigma_1 \cdot \sigma_2$ соответствует функции $s = s_1 \circ s_2$.

Пример:

$$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 3 & 2 & 5 & 1 & 4\end{pmatrix}\cdot\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 2 & 4 & 5 & 1 & 3\end{pmatrix}=\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 4 & 3 & 2 & 1\end{pmatrix}.$$

Замечание. Умножение подстановок – операция, не обладающая свойством коммутативности при n>2. (Приведите пример подстановок, для которых $\sigma_1 \cdot \sigma_2 \neq \sigma_2 \cdot \sigma_1$).

Определение. *Тождественной подстановкой* называется подстановка $\iota = \begin{pmatrix}1 & 2 & 3 & \dots & n\\ 1 & 2 & 3 & \dots & n\end{pmatrix}$, эта подстановка соответствует тождественному отображению $i: \mathbb{N}_n \to \mathbb{N}_n,\ i(k) = k\ \forall k = 1,2\dots n.$

Определение. *Обратной* подстановкой σ^{-1} к подстановке σ называется такая подстановка, для которой $\sigma \cdot \sigma^{-1} = \iota$.

Пример:

Для $\sigma = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 4 & 2 & 3 & 1\end{pmatrix}$ обратная подстановка имеет вид $\sigma^{-1} = \begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 5 & 3 & 4 & 2 & 1\end{pmatrix}$.

Для получения обратной подстановки достаточно поменять местами 1-ю и 2-ю строки подстановки, а затем отсортировать столбцы по возрастанию чисел в первой строке.

Определение. Подстановка называется *циклом* длины k, если существует подмножество $C = \{c_1; c_2; \dots; c_k\} \subseteq \mathbb{N}_n$ такое, что $s(c_m) = c_{m+1}$ для $m = 1, \dots, k-1$, $s(c_k) = c_1$ и $s(c_m) = c_m$ для $m \notin C$.

Здесь k>1.

Пример:

$\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 5 & 3 & 2 & 4\end{pmatrix}$ - это цикл длины 3. Эта биекция переставляет по кругу элементы 2, 5 и 4; остальные элементы 1 и 3 остаются на месте под действием этого отображения (рис. 1.14).

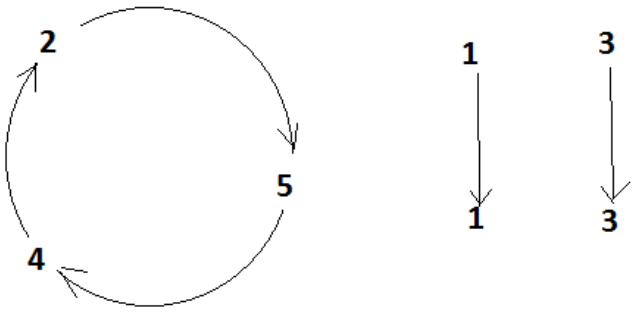


Рисунок 1.14

Обозначение. Цикл, переставляющий по кругу элементы $m_1, m_2, \ldots, m_k$, принято коротко обозначать так: $(m_1 m_2 \ldots m_k)$.

Например, цикл из предыдущего примера может быть записан так: (2 5 4), или так: (5 4 2), или так (4 2 5).

Имеет место следующая легко доказываемая теорема.

Теорема. Каждая (нетождественная) подстановка однозначно (с точностью до порядка сомножителей) раскладывается в произведение независимых (состоящих из разных наборов чисел) циклов.

Примеры:

1) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} = (1 \quad 3 \quad 5 \quad 4)$ -цикл;

2) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4 \quad 5)$ -цикл;

3) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 3 & 1 \end{pmatrix} = (1 \quad 5)(2 \quad 4 \quad 3)$;

4) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix}$ - тождественная подстановка;

5) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 2 & 4 \end{pmatrix} = (2 \quad 5 \quad 4)$ -цикл.

Утверждение. Если σ - это цикл длины k, то $\sigma^k = \iota$

Степень, как обычно, обозначает произведение k экземпляров подстановки σ.

Доказательство очевидно.

Перестановки

Определение. Отношение порядка " $\leq$ " на множестве M называется *отношением линейного порядка*, если любые два элемента множества сравнимы, то есть $\forall x, y \in M$ выполнено $x \leq y$ или $y \leq x$.

Определение. Отношение линейного порядка, введенное на множестве $\mathbb{N}_n = \{1; 2; \ldots; n\}$, называется *перестановкой* из чисел $1; 2; \ldots; n$.

Перестановку можно описать, записав элементы множества $\mathbb{N}_n = \{1; 2; \dots; n\}$ в строчку, считая, что порядок следования символов записи слева направо соответствует записи элементов в возрастающем слева направо линейном порядке данной перестановки.

Примеры:

1) 3 2 5 1 4;
2) 1 2 3 4 5;
3) 5 4 3 2 1.

Нетрудно видеть, что с каждой подстановкой взаимно однозначно связана перестановка, наблюдаемая в нижней строке подстановки.

Пример:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 1 & 4 \end{pmatrix} \leftrightarrow 3 \quad 2 \quad 5 \quad 1 \quad 4.$$

Поэтому зачастую в современных руководствах отождествляют понятия перестановки и подстановки.

Утверждение. Существует ровно $n!$ различных перестановок (подстановок) на множестве $\mathbb{N}_n = \{1; 2; \dots; n\}$.

Доказательство. При формировании перестановки у нас есть n позиций для записи в строчку чисел множества $\mathbb{N}_n = \{1; 2; \dots; n\}$.

Первую позицию можно заполнить n способами: можно поставить любое из чисел $1; 2; \dots; n$. При каждом заполнении первой позиции вторую позицию можно заполнить $(n-1)$ способом. Всего получается $n(n-1)$ способ заполнения первых двух позиций. При каждом заполнении первых двух позиций третью позицию можно заполнить $(n-2)$ способами. Всего получается $n(n-1)(n-2)$ способ заполнения первых трёх позиций и т. д.

Всего получается $n \cdot (n-1) \cdot (n-2) \dots 2 \cdot 1 = n!$ способов заполнения всех позиций, то есть $n!$ различных перестановок (и подстановок) на множестве $\mathbb{N}_n = \{1; 2; \dots; n\}$.

Четность (знак) перестановки (подстановки)

Определение. *Инверсией* в подстановке σ называется пара чисел $i < j$, для которой $s(i) > s(j)$. Обозначим число инверсий в данной подстановке $n(\sigma)$.

Определение. Подстановка σ (перестановка) называется *четной*, если $n(\sigma)$-четное число, перестановка *нечетная*, если $n(\sigma)$ - нечетное число.

Знак подстановки $sgn(\sigma)$ – это число $(-1)^{n(\sigma)}$. Очевидно, что знак будет равен 1 или (-1) для, соответственно, четной и нечетной подстановки.

Определение. *Транспозицией* для данной перестановки, рассматриваемой как упорядоченная последовательность чисел, называют перемену местами двух чисел в перестановке.

Утверждение. Выполнение любой транспозиции всегда меняет четность перестановки.

Доказательство. Пусть мы меняем местами элементы $s(i)$ и $s(j)$ для $i < j$.

Тогда:

1) не появится новых инверсий с участием $s(k)$ при $k < i$ и $k > j$,

2) для каждого из $s(k)$ при $i < k < j$ количество инверсий с его участием изменится на 2,

3) и, наконец появится или исчезнет, то есть изменится на 1, инверсия для $s(i)$ и $s(j)$.

Итак, четность общего числа инверсий изменится.

Теорема. Перестановка будет четной тогда и только тогда, когда для приведения её к возрастающему виду (1 2 3 … n) потребуется четное число транспозиций.

Доказательство. Перестановка (1 2 3 … n) не имеет инверсий, поэтому она четная. Если мы использовали четное число транспозиций для приведения перестановки к возрастающему виду, значит, четное число раз менялась четность перестановки, и, значит, исходная перестановка была четной. Если же было использовано нечетное число транспозиций, то исходная перестановка была нечетной.

Пример:

$4\ \ 3\ \ 1\ \ 2 \rightarrow 1\ \ 3\ \ 4\ \ 2 \rightarrow 1\ \ 2\ \ 4\ \ 3 \rightarrow 1\ \ 2\ \ 3\ \ 4.$

Исходная перестановка нечетная.

Утверждение. Подстановка, являющаяся циклом четной длины, будет нечетной. Подстановка, являющаяся циклом нечетной длины, будет четной.

Доказательство. В перестановке, соответствующей циклу $(a_1\ \ a_2\ \ \dots\ \ a_k)$ выполним транспозицию элементов $s(a_1)$ и $s(a_k)$. Получим цикл $(a_2\ \ \dots\ \ a_k)$. Четность изменится, длина цикла уменьшится на 1. Будем продолжать эти действия, пока не получим возрастающий вид перестановки, для этого нам потребуется $(k-1)$ транспозиция.

Утверждение. Четность подстановки совпадают с четностью числа, равного суммарной длине циклов минус число циклов (*декремент*).

Доказательство. Для приведения перестановки к возрастающему виду нужно (как в доказательстве предыдущего утверждения) сделать транспозиции в количестве, равном декременту.

Теорема. $sgn(\sigma_1\sigma_2) = sgn(\sigma_1) \cdot sgn(\sigma_2)$

Доказательство. Пару чисел назовем *инверсионной* для подстановки σ, если этой паре соответствует инверсия этой подстановки.

Четность подстановки совпадает с четностью числа инверсионных пар.

Рассмотрим теперь произвольную пару чисел $i \neq j$, а также пару $s_1(i), s_1(j)$.

1) Если первая пара инверсионна для σ_1, а вторая инверсионна для σ_2, то первая пара не инверсионна для $\sigma_1\sigma_2$.

2) Если первая пара инверсионна для σ_1, а вторая не инверсионна для σ_2, то первая пара инверсионна для $\sigma_1\sigma_2$.

3) Если первая пара не инверсионна для σ_1, а вторая инверсионна для σ_2, то первая пара инверсионна для $\sigma_1\sigma_2$.

4) Если первая пара не инверсионна для σ_1, а вторая не инверсионна для σ_2, то первая пара не инверсионна для $\sigma_1\sigma_2$.

Если перебрать всевозможные пары $i \neq j$, то можно увидеть, что четность числа инверсионных пар для $\sigma_1\sigma_2$ равна сумме четностей чисел инверсионных пар для σ_1 и для σ_2 .

Теорема доказана.

Замечание. Напомним определение определителя квадратной матрицы:

$$\begin{vmatrix} a_{11} & \dots & a_{1n} \\ \vdots & \vdots & \vdots \\ a_{n1} & \dots & a_{nn} \end{vmatrix} = \sum_{i_1 \dots i_n} sgn(i_1 \dots i_n) \cdot a_{1i_1} \cdot a_{2i_2} \cdot \dots \cdot a_{ni_n}.$$

Суммирование проводится по всевозможным перестановкам элементов $\mathbb{N}_n$.

Определение. *Матрицей перестановки* σ называется квадратная матрица $M_\sigma = (m_{ij})$, в которой $m_{is(i)} = 1$, а остальные элементы равны 0.

Пример:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad M_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Утверждение. $sgn(\sigma) = det(M_\sigma)$

Доказательство очевидным образом вытекает из определения определителя.

Легко проверяется следующее утверждение.

Утверждение. $M_{\sigma_1\sigma_2} = M_{\sigma_1} \cdot M_{\sigma_2}$

Теперь, приведенная выше, теорема о знаке подстановки вытекает из этих двух утверждений и теоремы об определителе произведения двух квадратных матриц.

1.6. Алгебраические структуры

Группы

Определение. Рассмотрим множество G, на элементах которого рассматривается бинарная операция " $\cdot$ ", которую (пока) мы будем называть умножением. Пусть выполнены следующие требования (аксиомы):

1) $\forall a, b, c \in G \quad (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (ассоциативность умножения);

2) $\exists e \in G$, такой что $\forall a \in G \;\; e \cdot a = a \cdot e = a$ (наличие единичного (нейтрального) элемента);

3) $\forall a \in G \;\; \exists a^{-1} \in G$, такой что $a^{-1} \cdot a = a \cdot a^{-1} = e$ (наличие обратного элемента у любого элемента).

Множество G с рассматриваемой операцией называется (мультипликативной) ***группой***.

Группа G называется *коммутативной* (или *абелевой*, в честь норвежского математика 19 века Нильса Абеля), если, кроме того, выполнено требование:

4) $\forall a, b \in G \quad a \cdot b = b \cdot a.$

Если групповая операция называется сложением, то говорят об *аддитивной* группе и вместо " $\cdot$ " используют символ «+», вместо единичного элемента рассматривают нулевой элемент (обычно обозначаемый **0),** вместо обратного a^{-1} используют противоположный элемент, который обозначают $-a$.

Примеры групп:

1) Множество действительных чисел $\mathbb{R}$ с обычной операцией сложения образует аддитивную абелеву группу.

2) Множество действительных чисел без нуля $\mathbb{R} \setminus \{0\}$ с обычной операцией умножения образует мультипликативную абелеву группу.

3) Множество комплексных чисел $\mathbb{C}$ с обычной операцией сложения

образует аддитивную абелеву группу.

4) Множество комплексных чисел без нуля $\mathbb{C}\setminus\{0\}$ с обычной операцией умножения образует мультипликативную абелеву группу.

5) Множество рациональных чисел $\mathbb{Q}$ с обычной операцией сложения образует аддитивную абелеву группу.

6) Множество рациональных чисел без нуля $\mathbb{Q}\setminus\{0\}$ с обычной операцией умножения образует мультипликативную абелеву группу.

7) Множество целых чисел $\mathbb{Z}$ с обычной операцией сложения образует аддитивную абелеву группу.

Заметим, что множество целых чисел без нуля $\mathbb{Z}\setminus\{0\}$ с обычной операцией умножения НЕ образует группу.

Заметим также, что множество натуральных чисел $\mathbb{N}$ с обычной операцией сложения НЕ образует группу.

8) Множество всех комплексных корней уравнения $z^n = 1$, с операцией умножения комплексных чисел образует мультипликативную абелеву группу.

Порядок этой группы (количество элементов в ней) равен n.

Определение. Две группы G_1 и G_2 *изоморфны*, если существует взаимно однозначное отображение группы G_1 на группу G_2, то есть *биекция* $f: G_1 \to G_2$, такая, что, если $b_1 = f(a_1)$ и $b_2 = f(a_2)$, то $b_1 \bullet b_2 = f(a_1 \cdot a_2)$ (здесь $\cdot$ - это групповая операция в группе G_1, а $\bullet$ - это групповая операция в группе G_2).

9) Множество всех поворотов правильного n -угольника вокруг его центра, при каждом из которых повернутый многоугольник совмещается с исходным, с операцией композиции поворотов образует мультипликативную абелеву группу. Порядок этой группы равен n. Эта группа *изоморфна* группе, рассмотренной в предыдущем примере.

10) Рассмотрим множество $\mathbb{Z}_n = \{0,1,\dots n-1\}$ с операцией сложения, определяемой следующим образом: для двух элементов $a, b \in \mathbb{Z}_n$ их сумма равна остатку при делении на n числа $(a+b)$. Это множество с так определенной операцией сложения образует абелеву группу. Эта группа изоморфна группам, рассмотренным в предыдущих примерах.

Множество $\mathbb{Z}_n = \{0,1,\dots n-1\}$ естественным образом биективно соответствует фактормножеству множества $\mathbb{Z}$ по отношению сравнения по модулю n (это отношение является отношением эквивалентности).

11) Рассмотрим множество $\widehat{\mathbb{Z}}_n = \{1,2,\ldots,n-1\}$ с операцией умножения, определяемой следующим образом: для двух элементов $a, b \in \widehat{\mathbb{Z}}_n$ их произведение равно остатку при делении на n числа $a \cdot b$. Это множество с так определенной операцией умножения образует (абелеву) группу лишь в случае, когда $n = p$ - простое число.

(Проверьте, что, например, $\widehat{\mathbb{Z}}_7$ образует мультипликативную группу, а $\widehat{\mathbb{Z}}_6$ нет!)

12) Рассмотрим множество всех поворотов окружности вокруг ее центра с операцией композиции. Это множество образует абелеву группу (которая обозначается $SO(2)$).

13) Рассмотрим множество всех поворотов сферы вокруг всевозможных осей, проходящих через центр сферы, с операцией композиции. То, что композиция двух поворотов снова будет поворотом, вытекает из теоремы Эйлера.

Теорема вращения Эйлера. *«Всякое, имеющее неподвижную точку, движение твердого тела, в результате которого тело совмещается с самим собой, является поворотом вокруг некоторой оси, проходящей через эту неподвижную точку».*

Рассматриваемое множество образует некоммутативную группу, которая обозначается $SO(3)$.

Докажем некоммутативность.

Рассмотрим прямоугольную систему координат с началом в центре сферы. Рассмотрим поворот A вокруг оси y, совмещающий ось x с осью z по кратчайшему углу и поворот B вокруг оси z, совмещающий ось x с осью y по кратчайшему углу. Тогда произведение AB переводит точку P пересечения оси x и сферы в точку Q пересечения оси z и сферы, тогда как произведение BA переводит точку P в точку R пересечения оси y и сферы (рис. 1.15).

Следовательно, AB ≠ BA.

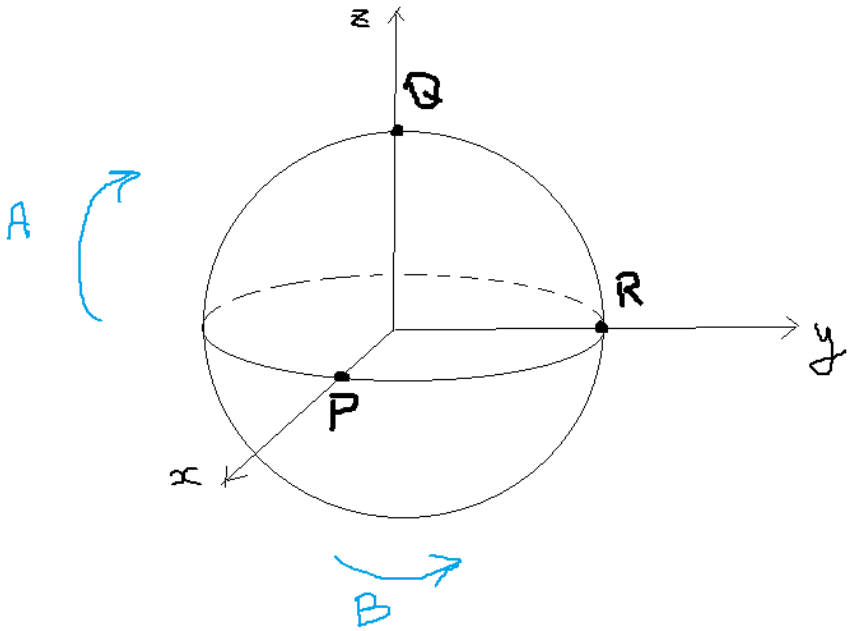


Рисунок 1.15

14) Множество всех матриц одинакового размера $k \times n$ с обычной операцией сложения образует аддитивную абелеву группу.

15) Множество всех невырожденных квадратных матриц одинакового размера $n \times n$ с операцией умножения матриц образует некоммутативную мультипликативную группу.

16) Множество всех матриц вида: $\begin{pmatrix} cos\,\phi & -sin\,\phi \\ sin\,\phi & cos\,\phi \end{pmatrix}$ с операцией умножения матриц образует коммутативную мультипликативную группу. Эта группа изоморфна *специальной ортогональной* группе $SO(2)$, рассмотренной в примере 12.

17) Множество всех *ортогональных* матриц размера 2×2, то есть всех таких матриц C, для которых $C^{-1} = C^T$, с операцией умножения матриц образует некоммутативную мультипликативную группу.

18) Рассмотрим множество всех поворотов окружности вокруг ее центра. Добавим к этому множеству процедур процедуры симметричного отражения точек окружности относительно некоторой прямой проходящей через центр окружности. Полученное множество с операцией композиции образует некоммутативную группу. Ее обозначают $O(2)$ (*ортогональная группа*). Эта группа изоморфна группе, рассмотренной в предыдущем примере.

19) Множество всех векторов на плоскости с операцией сложения векторов образует абелеву группу.

Эта группа изоморфна аддитивной группе всех матриц размера 2×1 (столбцов). Также эта группа изоморфна аддитивной группе всех комплексных

чисел $\mathbb{C}$.

20) Рассмотрим множество всех строк, состоящих из символов a, a^{-1}, b, b^{-1}, причем в этих строках a и a^{-1}не могут стоять рядом, также b и b^{-1} не могут стоять рядом. Например: $aab^{-1}abbba^{-1}a^{-1}b$.

Рассмотрим следующую операцию на этом множестве. Для двух таких строк S_1 и S_2 результат $S_1 \cdot S_2$ - это строка, полученная приписыванием справа к строке S_1 строки S_2 с последующим уничтожением a и a^{-1} и b и b^{-1}, оказавшихся рядом друг с другом. Например, если $S_1 = baabba^{-1}$, $S_2 = ab^{-1}b^{-1}a^{-1}b$, то $S_1 \cdot S_2 = bab$.

Это множество с этой операцией является некоммутативной группой (*свободная группа с двумя образующими*). В роли единичного элемента выступает пустая строка.

Заметим, что свободная группа с одной образующей изоморфна аддитивной группе всех целых чисел $\mathbb{Z}$.

21) Множество всех подстановок длины n с операцией умножения подстановок и единичным элементом ι образуют некоммутативную (при n>2) группу. Эта группа называется *симметрической группой* и обозначается S_n. Порядок этой группы (число различных перестановок длины n) равен $n!$.

Множество всех матриц перестановок со стандартной операцией умножения матриц и единичной матрицей I в роли единичного элемента образует группу, очевидно, изоморфную симметрической группе S_n.

Поскольку всякая матрица перестановок является ортогональной, то эта группа является *подгруппой* группы $O(n)$ всех ортогональных матриц размера $n \times n$.

В дискретной математике предметом нашего особого внимания станут *конечные* группы, то есть группы, содержащие конечное число элементов. Рассмотрим простейший, но важный пример конечной группы.

Определение. *Циклической группой* порядка n назовем группу $C_n = \{a, a^2, \ldots, a^n = e\}$. В этой группе n элементов, все элементы этой группы – это степени элемента a, причем a^n равен единичному элементу этой группы.

Примеры:

1) Группа всех поворотов правильного n -угольника вокруг его центра, при каждом из которых повернутый многоугольник совмещается с исходным, с

операцией композиции поворотов.

2) Группа всех комплексных корней уравнения $z^n = 1$, с операцией умножения комплексных чисел (рис. 1.16).

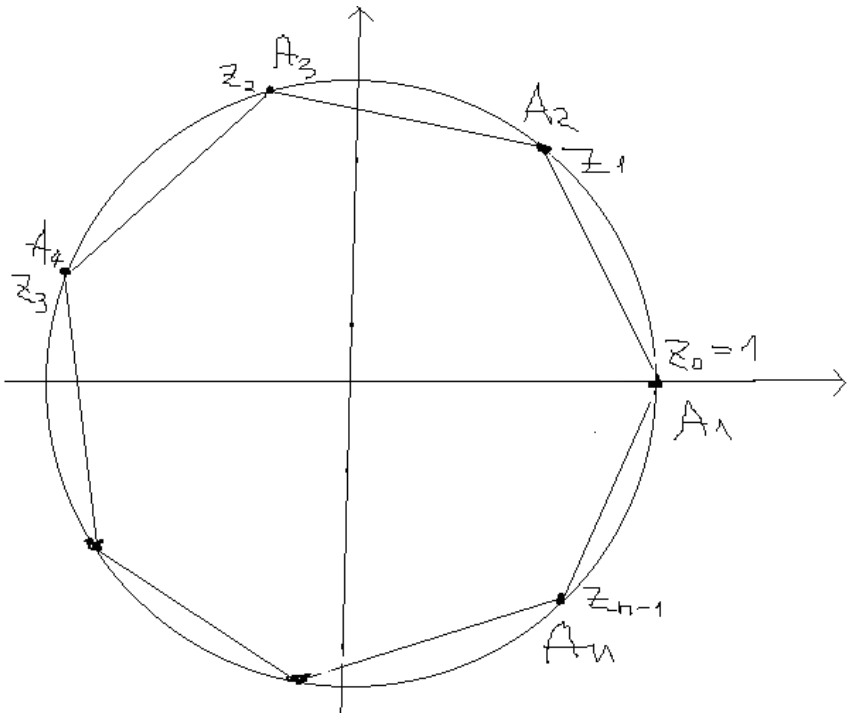


Рисунок 1.16

3) Группа $\mathbb{Z}_n = \{0,1,\dots n-1\}$ с операцией сложения, определяемой следующим образом: для двух элементов $a, b \in \mathbb{Z}_n$ их сумма равна остатку при делении на n числа $(a+b)$.

4) Группа (порядка $n-1$), элементами которой являются элементы множества $\widehat{\mathbb{Z}}_n = \{1,2,\dots,n-1\}$, с операцией умножения, определяемой следующим образом: для двух элементов $a, b \in \widehat{\mathbb{Z}}_n$ их произведение равно остатку при делении на n числа $a \cdot b$. Это множество с так определенной операцией умножения образует (абелеву) группу лишь в случае, когда $n = p$ - простое число.

5) Группа всех степеней циклической подстановки
$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix} = (1 \quad 2 \quad 3 \quad 4 \quad 5)$ с операцией умножения подстановок является циклической группой порядка 5.

Определение. Рассмотрим группу G. Пусть G_1 - подмножество множества G, само являющееся группой (с той же групповой операцией, что и в G). В этом случае G_1 называется *подгруппой* группы G.

Утверждение. Рассмотрим конечную группу G. Рассмотрим ее любой элемент a. Найдется натуральное число n, такое, что $a^n = e$.

Доказательство. Будем рассматривать последовательно натуральные степени элемента a. Так как группа конечна, найдутся такие k и m, что $a^k = a^m$. Тогда $a^{k-m} = a^k \cdot (a^{-1})^m = a^k \cdot (a^m)^{-1} = e$.

Определение. Минимальное значение n, при котором $a^n = e$, называется *порядком* элемента a в конечной группе G.

Легко проверяется следующее утверждение.

Утверждение. Рассмотрим конечную группу G. Рассмотрим ее любой элемент a. Пусть n - порядок этого элемента. Множество $\{a, a^2, \ldots, a^n\}$ является циклической подгруппой порядка n в группе G.

Теорема Лагранжа. В конечной группе порядок любой подгруппы является делителем порядка группы.

Доказательство. Рассмотрим конечную группу G и ее подгруппу H.

Введем отношение эквивалентности на множестве G по следующему правилу: $b \sim a$, если найдется $h \in H$, такое, что $b = ah$.

Проверим, что это действительно отношение эквивалентности.

Рефлексивность есть: $b = be$ и $e \in H$.

Симметричность: $b \sim a \Rightarrow b = ah \Rightarrow a = bh^{-1} \Rightarrow a \sim b$ (здесь $h \in H \Rightarrow h^{-1} \in H$, так как H - группа).

Транзитивность:

$a \sim b, b \sim c \Rightarrow a = bh_1, b = ch_2 \Rightarrow a = ch_2h_1 \Rightarrow a \sim c$

($h_2h_1 \in H$, так как H - группа).

Заметим далее, что в каждом классе эквивалентности столько же элементов, сколько в подгруппе H. Действительно, каждый класс $K(a)$ состоит из элементов вида $b = ah$, причем если $h_1 \neq h_2$, то $ah_1 \neq ah_2$.

Отсюда получаем, что $|G| = m|H|$, где m - число классов эквивалентности.

Теорема доказана.

Следствие. В конечной группе порядок любого элемента является делителем порядка группы.

Нормальный делитель. Факторгруппа

Определение. Подгруппа H в группе G называется *нормальным делителем* этой группы, если $\forall g \in G$ выполнено $gH = Hg$. Это равносильно тому, что $\forall g \in G, \forall h \in H \ \ g^{-1}hg \in H$.

Определение. Рассмотрим группу G и нормальный делитель H в этой группе. Факторгруппой *G/H* называется фактормножество по отношению эквивалентности, рассмотренному в доказательстве теоремы Лагранжа, с групповой операцией: $K_1K_2 = \{c: c = ab, a \in K_1, b \in K_2\}$.

В роли единичного элемента здесь будет H. (Проверьте, что определение корректно.)

Пример:

Рассмотрим аддитивную группу $\mathbb{Z} = \{\dots -2, -1, 0, 1, 2, \dots\}$. Рассмотрим подгруппу $n\mathbb{Z} = \{\dots -2n, -n, 0, n, 2n, \dots\}$ всех целых чисел делящихся на n.

Поскольку аддитивная группа $\mathbb{Z}$ - коммутативна, то в ней любая подгруппа будет нормальным делителем.

Можно тогда рассмотреть факторгруппу $\mathbb{Z}/n\mathbb{Z}$. Два числа будут попадать в один класс эквивалентности, если их разность будет делиться на n.

Легко показать, что эта факторгруппа изоморфна группе $\mathbb{Z}_n = \{0, 1, \dots n-1\}$, рассмотренной в примере выше.

Симметрическая группа

Ранее мы заметили, что множество всех подстановок длины n с операцией умножения подстановок и единичным элементом ι образуют некоммутативную (при n>2) группу. Эта группа называется *симметрической группой* и обозначается S_n. Порядок этой группы (число различных перестановок длины n) равен n!.

Рассмотрим теперь произвольное (не обязательно конечное) множество X. Рассмотрим множество всех биекций $X \to X$, обозначим его $S(X)$.

Это множество $S(X)$ будет снабжено алгебраической структурой группы, если рассмотреть в качество группового умножения операцию композиции. Назовем эту группу *симметрической группой множества* X.

Теорема Кэли. Каждая группа изоморфна некоторой подгруппе некоторой симметрической группы $S(X)$.

Доказательство. Рассмотрим группу G. Возьмем множество $X = G$ и

рассмотрим симметрическую группу $S(G)$.

Поставим теперь в соответствии каждому $g \in G$ биекцию $\sigma_g: G \to G$ по следующему правилу: $\sigma_g(a) = ag \ \ \forall a \in G$. Тогда соответствие между элементами группы Gи биекциями вида σ_g будет изоморфизмом групп, поскольку $\sigma_{g_1 g_2}(a) = a(g_1 g_2) = (ag_1)g_2 = \sigma_{g_2}(\sigma_{g_1}(a)) \ \forall a \in G$, то есть произведению элементов соответствует композиция биекций.

Действие группы. Орбиты

Определение. Рассмотрим две группы G_1 и G_2. Отображение $f: G_1 \to G_2$, такое, что, если $b_1 = f(a_1)$ и $b_2 = f(a_2)$, то $b_1 \bullet b_2 = f(a_1 \cdot a_2)$ называется *гомоморфизмом* групп.

(Здесь $\cdot$ - это групповая операция в группе G_1, а $\bullet$ - это групповая операция в группе G_2).

Изоморфизм является частным случаем гомоморфизма. Но, в отличие от изоморфизма, гомоморфизм не обязан быть биекцией.

Определение. Группа G *действует* на множестве M, если задан гомоморфизм $\Phi: G \to S(M)$.

Применяется обозначение: $(\Phi(g))(m) = gm$. Группу G называют *группой преобразований*, а ее элементы *преобразованиями*.

Определение. Элемент $m \in M$ называется *стационарной точкой* для элемента $g \in G$, если $gm = m$.

Обозначим M_g- множество стационарных для g точек.

Определение. Рассмотрим две группы G_1 и G_2.

Отображение $f: G_1 \to G_2$, называется *гомоморфизмом* групп, если $\forall a_2, a_2 \in G_1 \quad f(a_1 \cdot a_2) = f(a_1) \bullet f(a_2)$.

(Здесь «$\cdot$» - это групповая операция в группе G_1, а «$\bullet$»- это групповая операция в группе G_2).

Определение. Группа G *действует* на множестве X, если задан гомоморфизм $\Phi: G \to S(X)$.

Применяется обозначение: $(\Phi(g))(x) = gx$. Группу G называют *группой преобразований*, а ее элементы *преобразованиями*.

Определение. Подмножество $Gx = \{gx: g \in G\} \subseteq X$ называется *орбитой* элемента $x \in X$.

Определение. Элемент $x \in X$ называется *стационарной точкой* для элемента $g \in G$, если $gx = x$.

Обозначим X_g- множество стационарных для g точек.

Лемма Бернсайда (лемма Коши – Фробениуса).

Число орбит k при действии конечной группы G на конечном множестве точек X равно средней по группе мощности множества X_g

$$k = \frac{\sum_{g \in G} |X_g|}{|G|}.$$

Доказательство. Пусть количество элементов в группе G равно n.

Рассмотрим отношение R между элементами группы G и множества X:

$R = \{(x, g): gx = x, g \in G, x \in X\}$.

Пусть $O_1, \ldots, O_k$ - орбиты, возникшие в X под действием группы G. Очевидно, что множество X будет дизъюнктным объединением этих орбит.

Докажем, что для каждой орбиты O_i в декартовом произведении $O_i \times G$ будет ровно n элементов, то есть: $|(O_i \times G) \cap R| = n$.

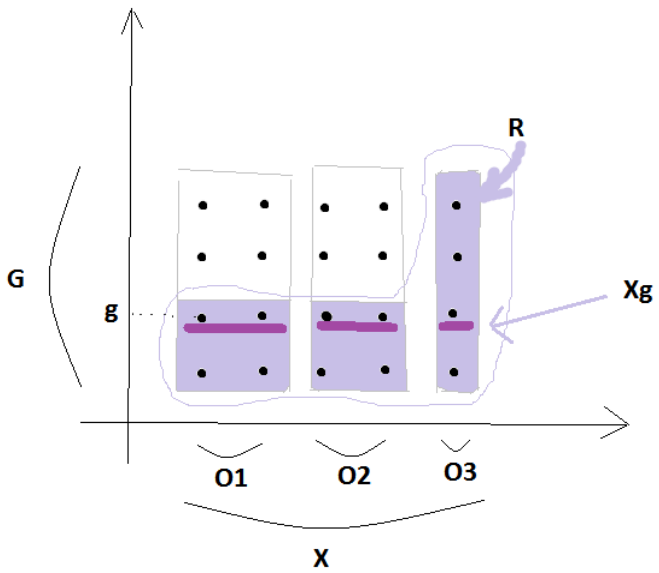


Рисунок 1.17

Рассмотрим любой элемент первой орбиты $x_1 \in O_1$. Пусть в первой орбите будет m элементов: $O_1 = \{x_1, \ldots x_m\}$ (рис. 1.17). Рассмотрим $x_1 \in O_1$.Обозначим $S = S_{x_1} = \{g \in G: gx_1 = x_1\}$ - стабилизатор элемента x_1. Обозначим

$|S| = l$ Нетрудно проверить, что S будет подгруппой группы G.

Рассмотрим другой элемент первой орбиты $x_2 \in O_1$. Пусть $g_2 x_1 = x_2$.

Обозначим: $C_2 = \{\hat{g}_2 \in G: \hat{g}_2 x_1 = x_2\}$ - множество всех элементов группы, которые своим действием переводит x_1 в x_2. Докажем, что $C_2 = g_2 S$.

Во-первых, всякий элемент из $g_2 S$ будет принадлежать C_2, поскольку для любого $g \in S$ будет $g_2 g x_1 = g_2 x_1 = x_2$, а значит $g_2 g \in C_2$.

Во-вторых, всякий элемент из C_2 будет принадлежать $g_2 S$, поскольку, если $\hat{g}_2 x_1 = x_2$, то $\hat{g}_2 x_1 = g_2 x_1$, откуда получается $g_2^{-1} \hat{g}_2 x_1 = x_1$. Это значит, что $g_2^{-1} \hat{g}_2 = g \in S$, следовательно $\hat{g}_2 = g_2 g \in g_2 S$.

Из доказанного вытекает, что в C_2 будет столько же элементов, сколько их в S, $|C_2| = |S| = l$

Аналогично определяются множества C_i для каждого $i = 1, \ldots, m$, и далее так же доказывается, что $|C_i| = |S| = l$.

Каждый элемент группы G принадлежит какому-нибудь C_i (это вытекает из определения орбиты), поэтому $G = C_1 \cup \ldots \cup C_m$.

Отсюда получим: $|G| = |C_1| + \ldots + |C_m|$, то есть $n = m \cdot l$.

Мы доказали, что $l = \frac{n}{m}$, то есть мощность стабилизатора S_{x_1} равна $\frac{n}{m}$.

Аналогично получим, что мощности стабилизаторов всех элементов этой орбиты равны $\frac{n}{m}$.

Суммарная мощность всех стабилизаторов элементов этой орбиты будет равна $\left|S_{x_1}\right| + \ldots + \left|S_{x_m}\right| = \frac{n}{m} + \ldots + \frac{n}{m} = m \cdot \frac{n}{m} = n$.

Мы получаем, что $|(O_1 \times G) \cap R| = \left|S_{x_1}\right| + \ldots + \left|S_{x_m}\right| = n$.

Аналогично, для всех остальных орбит $|(O_i \times G) \cap R| = n$.

Поэтому мощность всего отношения $|R| = k \cdot n$.

С другой стороны, очевидно, что

$$|R| = \sum_{g \in G} X_g.$$

Отсюда

$$k \cdot n = \sum_{g \in G} X_g \quad \text{и} \quad k = \frac{\sum_{g \in G} X_g}{n} = \frac{\sum_{g \in G} X_g}{|G|}.$$

Лемма Бернсайда доказана.

Эта лемма потребуется нам при изучении теории Пойа в перечислительной комбинаторике.

Рассмотрим далее кратко другие алгебраические структуры.

Кольца

Определение. Рассмотрим множество R, на элементах которого рассматриваются две бинарных операции: «сложение» $+$и «умножение» " $\cdot$ ".

Пусть выполнены следующие требования:

1) Множество R с операцией сложения образует абелеву группу.

2) Имеет место дистрибутивность умножения относительно сложения:

$\forall a, b, c \in R \quad (a + b) \cdot c = a \cdot c + b \cdot c$ и

$\forall a, b, c \in R \quad a \cdot (b + c) = a \cdot b + a \cdot c.$

(В этих записях мы считаем, что операция умножения имеет более высокий приоритет чем сложение, поэтому не ставим скобки в правой части).

3) Операция умножения обладает свойством ассоциативности.

4) В R есть единичный элемент для операции умножения.

Кольцо называют *коммутативным*, если умножение в нем является коммутативной операцией.

Примеры колец:

1) Множество целых чисел $\mathbb{Z}$ с обычными операциями сложения и умножения образует коммутативное кольцо.

2) Рассмотрим множество $\mathbb{Z}_n = \{0,1,\dots n-1\}$ с операцией сложения, определяемой следующим образом: для двух элементов $a, b \in \mathbb{Z}_n$ их сумма равна остатку при делении на n числа $(a + b)$ и операцией умножения, определяемой аналогично: для двух элементов $a, b \in \mathbb{Z}_n$ их произведение равно остатку при делении на n числа $a \cdot b$. Это множество с этими операциями сложения и умножения является коммутативным кольцом.

3) Множество всех многочленов всевозможных степеней от одной переменной с действительными коэффициентами с обычными операциями сложения и умножения является коммутативным кольцом.

4) Множество всех многочленов всевозможных степеней от одной переменной с комплексными коэффициентами с обычными операциями сложения и умножения является коммутативным кольцом.

Для кольца целых чисел имеет место *основная теорема арифметики* о разложении целого числа в произведение простых сомножителей.

Для кольца многочленов с комплексными коэффициентами имеет место *основная теорема алгебры* о разложении многочлена в произведение многочленов 1-й степени.

Для кольца многочленов с действительными коэффициентами имеет место *теорема* о разложении многочлена в произведение многочленов 1-й и 2-й степени.

5) Множества рациональных чисел $\mathbb{Q}$, действительных чисел $\mathbb{R}$, комплексных чисел $\mathbb{C}$ с обычными операциями сложения и умножения являются коммутативными кольцами.

6) Множество всех квадратных матриц размера $n \times n$ с операциями сложения и умножения матриц образует некоммутативное кольцо.

Рассмотрим множество всех подмножеств некоторого множества U.

В роли операции сложения на элементах этого множества будет выступать операции *симметрической разности*: положим A+B=(A\B) U (B\A).

В роли операции умножения выступает *пересечение* множеств: $A \cdot$ B=A $\cap$ B (рис. 1.18).

Это множество с этими операциями сложения и умножения будет коммутативным кольцом. В роли нуля будет выступать пустое множество. В роли единицы – все множество U.

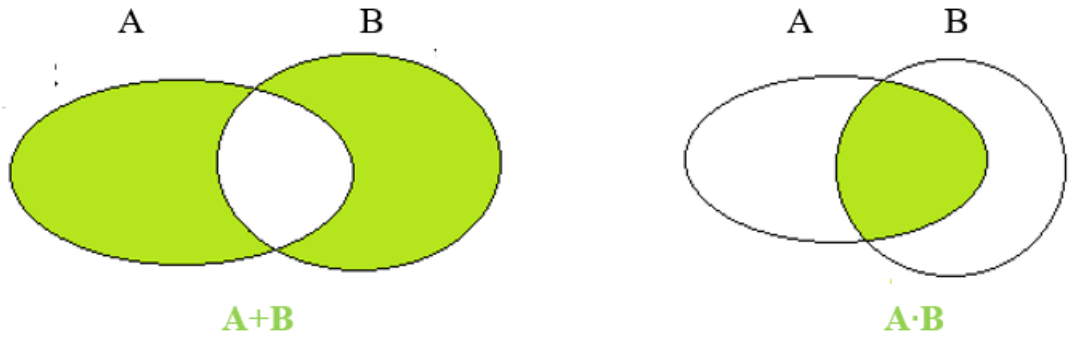


Рисунок 1.18

Познакомимся с развитой в 19 веке алгебраической теорией «двойных чисел», играющих важную роль в гиперболической (неэвклидовой) геометрии, а тем самым и в специальной теории относительности.

Двойные числа (Split complex numbers)

Определение. Двойное число – это алгебраическое выражение вида $x + yj$, где $x, y \in \mathbb{R}$, j - символ.

Арифметические операции над комплексными числами осуществляются по правилам оперирования с алгебраическими выражениями, с учетом равенства $j^2 = 1$.

Сложение, вычитание и умножение оказывается осуществимым для любых двойных чисел.

Множество двойных чисел является коммутативным кольцом. Разделить можно лишь на число, не являющееся делителем нуля, то есть не равное $a + aj$ или $a - aj$, то есть должно быть не выполнено $x^2 = y^2$.

Определение. *Сопряженным* двойному числу $z = x + yj$ называется двойное число $z^* = x - yj$.

Единичной окружности $z \cdot z^* = 1, x^2 + y^2 = 1$ на комплексной плоскости, соответствует *единичная гипербола* $z \cdot z^* = 1, x^2 - y^2 = 1$ на плоскости двойных чисел (пространство Минковского размерности (1+1)).

Аналог формулы Эйлера:

$$e^{j\phi} = ch\phi + j \cdot sh\phi,$$

где $ch\phi = \frac{e^{\phi}+e^{-\phi}}{2}, sh\phi = \frac{e^{\phi}-e^{-\phi}}{2}$ - гиперболические косинус и синус.

Тейлоровские разложения гиперболических функций:

$$shx = x + \frac{x^3}{3!} + \frac{x^5}{5!} + \frac{x^7}{7!} + \ldots..$$

$$chx = 1 + \frac{x^2}{2!} + \frac{x^4}{4!} + \frac{x^6}{6!} + \ldots..$$

Матричное представление двойных чисел. При этом представлении мы отождествляем двойное число $z = x + yj$ с квадратной матрицей $Z = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$. Определитель матрицы $Z = \begin{pmatrix} x & y \\ y & x \end{pmatrix}$, соответствующей числу $z = x + yj$, будет равен: $det(Z) = x^2 - y^2 = (x + yj)(x - yj) = z \cdot z^*$.

Определение. Кольцо, в котором каждый ненулевой элемент имеет обратный (по отношению к операции умножения) называется ***телом*** (англ. термин: *division ring*).

Кватернионы

Тело кватернионов можно определить как множество выражений вида $a + bi + cj + dk$, где $a, b, c, d \in \mathbb{R}$, i, j, k -символы («мнимые единицы»).

Сложение кватернионов осуществляется обычным образом как сложение

алгебраических выражений.

Умножение не коммутативно, нужно учитывать правила умножения мнимых единиц: $ij = k, jk = i, ki = j$, но $ji = -k, kj = -i, ik = -j$.

Кроме того, $i^2 = -1, j^2 = -1, k^2 = -1$.

Кватернионы открыл в 1843 году Вильям Гамильтон. Это было грандиозное открытие. На этом пути были введены скалярное и векторное произведения, да и сами термины «скаляр» и «вектор». Кватернионы используются в чистой математике, но также имеют практическое применение в физике и в прикладной математике, особенно для вычислений, включающих трехмерное вращение, например, в трехмерной компьютерной графике.

Матричное представление кватернионов: $\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & b \\ d & -c & b & a \end{pmatrix}$

Поля

Определение. *Полем* F называется коммутативное кольцо, в котором каждый ненулевой элемент имеет обратный (по отношению к операции умножения).

То есть поле F образует абелеву группу по сложению, $F\backslash\{0\}$ образует абелеву группу по умножению, и выполнено требование дистрибутивности умножения по отношению к сложению: $\forall a, b, c \in F \quad (a + b) \cdot c = a \cdot c + b \cdot c$.

Можно еще сказать, что *поле* – это коммутативное *тело.*

Примеры полей:

1) Множество рациональных чисел $\mathbb{Q}$ с обычными операциями сложения и умножения образует поле.

2) Множество действительных чисел $\mathbb{R}$ с обычными операциями сложения и умножения образует поле.

3) Множество комплексных чисел $\mathbb{C}$ с обычными операциями сложения и умножения образует поле.

4) Действительное число называется *алгебаическим*, если оно является корнем многочлена с рациональными коэффициентами. Можно доказать, что множество всех алгебраических чисел является полем.

Пример алгебраического числа - отношение золотого сечения $\phi = \frac{\sqrt{5}+1}{2}$, поскольку это корень многочлена $x^2 - x - 1$.

Существуют неалгебраические числа, например, константы π и e (можно также неконструктивно доказать существование неалгебраических чисел, если

заметить, что множество алгебраических чисел счетно, а множество всех действительных чисел несчетно).

5) Действительное число называется *конструируемым*, если оно может быть получено из целых чисел применением арифметических операций (сложение, вычитание, умножение и деление), а также операции извлечения квадратного корня.

Если на плоскости задан отрезок, имеющий длинну единица, то для любого конструируемого числа с помощью циркуля и линейки можно построить отрезок, имеющий длину, равную этому числу.

Примеры конструируемых чисел:

отношение золотого сечения;

$cos\frac{2\pi}{17}$ (Этот результат получил Гаусс в 18-летнем возрасте при исследовании множества комплексных корней уравнения $z^{17}=1$. Отсюда вытекает возможность построения правильного 17-угольника с помощью циркуля и линейки).

Множество всех конструируемых чисел, очевидно, является полем. Каждое конструируемое число является алгебраическим. Обратное неверно.

Примеры неконструируемых чисел:

$\sqrt[3]{2}$ - данное число является алгебраическим (неконструируемость этого числа доказывает неразрешимость античной задачи удвоения куба);

$\sqrt{\pi}$ – данное число неалгебраическое (неконструируемость этого числа доказывает неразрешимость античной задачи квадратуры круга);

$cos\frac{2\pi}{7}$ - данное число является алгебраическим (неконструируемость этого числа доказывает неразрешимость задачи построения правильного 7-угольника с помощью циркуля и линейки).

6) Множество всех рациональных функций с операциями сложения и умножения является полем.

7) Кольцо $\mathbb{Z}_n=\{0,1,\dots n-1\}$ при $n=p$ - простое число будет (конечным) полем.

Конечные поля называют *полями Галуа*. Можно доказать, что количество элементов в поле Галуа может быть равным лишь p^m, где p - простое число.

Поле, называется *алгебраически замкнутым*, если всякий многочлен с коэффициентами из этого поля имеет корень из данного поля.

Из рассмотренных полей алгебраически замкнутыми являются только поле комплексных чисел $\mathbb{C}$ (основная теорема алгебры) и поле алгебраических чисел.

Линейные (векторные) пространства

Определение. Рассмотрим множество V, на элементах которого (мы будем их называть *векторами*) определены операции сложение элементов и умножение элементов V на элементы поля F (*скаляры*).

Пусть выполнены следующие требования:

1. $\forall \bar{a}, \bar{b} \in V \quad \bar{a} + \bar{b} = \bar{b} + \bar{a}$ (коммутативность сложения);

2. $\forall \bar{a}, \bar{b}, \bar{c} \in G \quad (\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$ (ассоциативность сложения);

3. $\exists \bar{0} \in V$, такой что $\forall \bar{a} \in F \ \bar{0} + \bar{a} = \bar{a}$ (наличие нулевого вектора);

4.$\forall \bar{a} \in V \ \exists(-\bar{a}) \in V$, такой что $(-\bar{a}) + a = \bar{0}$ (наличие противоположного вектора у любого вектора);

Таким образом, множество V с операцией сложения является абелевой группой.

5. $\forall \lambda, \mu \in F \ \ \forall \bar{a} \in V \ (\lambda \cdot \mu) \cdot \bar{a} = \lambda \cdot (\mu \cdot \bar{a})$ (сочетаемость умножения чисел и умножения вектора на число);

6. $\forall \bar{a} \in V \ 1 \cdot \bar{a} = \bar{a}$, где $1 \in F$ - единица поля F;

7. $\forall \lambda \in F \ \ \forall \bar{a}, \bar{b} \in V \ \lambda \cdot (\bar{a} + \bar{b}) = \lambda \cdot \bar{a} + \lambda \cdot \bar{b}$; (дистрибутивность умножения вектора на число относительно сложения векторов);

8. $\forall \lambda, \mu \in F \ \ \forall \bar{a} \in V \ (\lambda + \mu) \cdot \bar{a} = \lambda \cdot \bar{a} + \mu \cdot \bar{a}$; (дистрибутивность умножения вектора на число относительно сложения элементов поля).

Множество V с рассмотренными операциями называется ***линейным пространством над полем F.***

Примеры линейных пространств:

1) Множество всех геометрических векторов на прямой с операциями сложения векторов и умножения вектора на число является линейным пространством над полем действительных чисел.

2) Множество всех геометрических векторов на плоскости является линейным пространством над полем действительных чисел.

3) Множество всех геометрических векторов в пространстве является линейным пространством над полем действительных чисел.

4) Множество всех столбцов чисел одинаковой длины с операцией сложения столбцов и операцией умножения столбца на число является линейным пространством над полем действительных чисел.

5) Множество всех матриц одинакового размера $k \times n$ с операцией сложения матриц и умножения матрицы на число является линейным пространством

над полем действительных чисел.

6) Множество всех функций, определенных на отрезке $[a; b]$, с операцией сложения функций и умножения функции на число является линейным пространством над полем действительных чисел.

7) Множество всех непрерывных функций, определенных на отрезке $[a; b]$, с операцией сложения функций и умножения функции на число является линейным пространством над полем действительных чисел.

8) Само поле F с операцией сложения и умножения может рассматриваться как линейное пространство над полем F.

9) Обозначим $F^n = \{(x_1, x_2, \ldots, x_n): x_i \in F\}$- множество упорядоченных наборов (строк) из n элементов F. Можно это множество рассматривать как декартово произведение n экземпляров этого поля: $F^n = F \times F \times \ldots \times F$. На этом множестве рассмотрим операцию поэлементного сложения и умножение строки на число. Тогда F^n будет линейным пространством над полем F.

10) Множество $\mathbf{B} = \{0; 1\}$ с операциями сложения по модулю 2 и обычного умножения является полем.

Следовательно, $\mathbf{B^n} = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n): x_i \in \mathbf{B}\}$ - множество упорядоченных наборов длины n, состоящих из нулей и единиц с операциями поэлементного сложения по модулю 2 и обычного умножения строки на число (0 или 1) будет линейным пространством над полем $\mathbf{B}$.

Это линейное пространство содержит лишь конечное число элементов.

Задачи к главе 1

1. Проверить, является ли выполнение включения $A \subseteq B \setminus C$ необходимым и достаточным условием выполнения равенства $A \cup C = (C \setminus A) \cup \big((A \cap B) \setminus C\big)$. Здесь A, B, C - произвольные множества.

2. Пусть для множеств A, B, C, X выполнена система условий. Выразить множество X через A, B, C, используя теоретико-множественные операции, либо доказать, что X — пустое множество. Или установить, что условия системы не совместимы.

a) $\begin{cases} C \setminus X = A \cup (C \setminus B), \\ A \cup X = B, \\ A \subseteq B \subseteq C; \end{cases}$ b) $\begin{cases} C \setminus X = C \setminus (A \cup B), \\ A \setminus B = X, \\ A \cup B \subseteq C; \end{cases}$ c) $\begin{cases} A \setminus X = C \cap B, \\ C \setminus X = B \setminus A, \\ X \setminus B = A \cup C. \end{cases}$

3. Для отношения P найти: P^{-1}, $P \circ P$, $P^{-1} \circ P$, если:

a) P = {(2,2), (4,4), (1,2), (3,1), (3,4)};

b) P = {(a, b), (a, c), (d, b), (c, c), (b, c)}.

Указание: использовать матрицы отношений.

4. Для данных P и T из соотношения $P \circ X = T$ найти отношение X наибольшей возможной мощности. Найти все решения поставленной задачи.

Указание: использовать матрицы отношений.

a) P = {(c, a), (c, b), (a, a), (b, a)},
T = {(c, c), (c, b), (c, a), (a, c), (a, b), (b, c), (b, b)};

b) P = {(a, c), (a, b), (c, b)},
T = {(a, a), (a, b), (a, c), (c, a), (c, c)}.

5. На множестве действительных чисел задано бинарное отношения $x \rho y \Leftrightarrow x > y + 1$. Установить, какими из свойств: рефлексивность, иррефлексивность, симметричность, асимметричность, антисимметричность, транзитивность это отношение обладает. Является ли оно отношением эквивалентности? Является ли оно отношением порядка? Является ли оно отношением строгого порядка?

ГЛАВА 2. КОМБИНАТОРИКА

Перечислительная комбинаторика отвечает на вопрос: «сколько?» и занимается пересчетом числа объектов, построенных на конечных множествах.

2.1. Предварительные определения. Метод математической индукции

Определение. Пусть $n, k \in \mathbb{N}$ - натуральные числа, $n \geq k$.

Нисходящей факториальной степенью $n^{\underline{k}}$ называется число равное:
$n^{\underline{k}} = n \cdot (n-1) \cdot \ldots (n-k+1)$ (всего k сомножителей).

Пример: $n! = n^{\underline{n}} = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$

Определение. Пусть $n, k \in \mathbb{N}$ - натуральные числа.

Восходящей факториальной степенью $n^{\overline{k}}$ называется число равное:
$n^{\overline{k}} = n \cdot (n+1) \cdot \ldots (n+k-1)$ (всего k сомножителей).

Пример: $n! = 1^{\overline{n}} = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$

Замечание. В русскоязычной учебной литературе иногда употребляются термины: *возрастающий* и *убывающий факториалы.* Англоязычные термины: *falling and rising factorials* лучше отражают суть.

Определение (А.Н. Выборнов). Пусть $m, n \in \mathbb{Z}$ - целые числа, $n > m$.
Мультисегментом $\langle m, n \rangle$ назовем число равное:
$\langle m, n \rangle = m \cdot (m+1) \cdot \ldots \cdot n$ (всего $(n-m+1)$ сомножителей).

Пример: $\langle 3{,}5 \rangle = 3 \cdot 4 \cdot 5 = 60.$

Пример: $\langle 1, n \rangle = n! = 1 \cdot 2 \cdot \ldots \cdot (n-1) \cdot n$

Пример: $n^{\underline{k}} = \langle n-k+1, n \rangle.$

Пример: $n^{\overline{k}} = \langle n, n+k-1 \rangle.$

Метод математической индукции

Метод доказательства утверждения, состоящего в том, что некоторое свойство (формула) выполнено для всех натуральных значений n.

Метод состоит из двух шагов:

1) Основание индукции.

Здесь проверяется, что утверждение выполнено для $n = 1$.

2) Шаг индукции.

Здесь доказывается, что из того, что утверждение выполнено для $n = k$ (так

называемое, *предположение индукции*) следует, что оно выполнено для $n = k + 1$.

Пример:

Докажем формулу $1^3 + 2^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$.

1) Основание индукции. При $n = 1$: $1^3 = \left(\frac{1(1+1)}{2}\right)^2$ – утверждение выполнено.

2) Шаг индукции. Пусть $1^3 + 2^3 + \ldots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$ (предположение индукции).

Рассмотрим $1^3 + 2^3 + \ldots + k^3 + (k+1)^3 = \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 =$

$= (k+1)^2 \cdot \left(\frac{k^2}{4} + k + 1\right) = (k+1)^2 \cdot \left(\frac{k^2+4k+4}{4}\right) = \left(\frac{(k+1)(k+2)}{2}\right)^2$.

Итак, из того, что формула верна для $n = k$ следует, что она верна для $n = k + 1$.

Доказательство формулы методом математической индукции проведено.

2.2. Комбинаторные числа

Перестановки

Определение. Перестановкой из элементов конечного множества, называется отношение линейного порядка, действующее на элементах этого множества (отношение тотально: любые два элемента сравнимы).

Обозначим число различных перестановок на множестве, состоящем из n элементов символами: P_n.

Выше мы доказали утверждение:

Утверждение. $P_n = n!$

Докажем его еще раз методом математической индукции.

1) Основание индукции. При $n = 1$ утверждение очевидно выполнено.

2) Шаг индукции. Пусть число различных перестановок из k элементов равно: $P_k = k!$ (предположение индукции).

Рассмотрим множество, состоящее из $(k+1)$-го элемента.

Рассмотрим все перестановки на этом множестве. Для каждого элемента, перестановок, начинающихся с этого элемента, будет $k!$ штук по

предположению индукции (этот элемент стоит на первом месте, остальные элементы в количестве k могут располагаться в $P_k = k!$ вариантах порядка). Всего элементов $(k+1)$. Поэтому $P_{k+1} = (k+1) \cdot P_k = (k+1) \cdot k! = (k+1)!$

Итак, из того, что утверждение верно для $n = k$ следует, что оно верно для $n = k+1$. Доказательство утверждения методом математической индукции проведено.

Замечание. Заметим, что само определение факториала, по сути, индуктивно: $(n+1)! = (n+1) \cdot n!$

Замечание. Формулу $P_{n+1} = (n+1) \cdot P_n$ назовем ***рекуррентной*** *формулой*. (Другой вариант записи этой же зависимости данного значения от предыдущего: $P_n = n \cdot P_{n-1}$).

Размещения

Определение. Рассмотрим множество, состоящее из n элементов. Выберем из этого множества k элементов и упорядочим эту выборку (разместим по k позициям). Получим *размещение.*

Число таких различных размещений обозначим: A_n^k.

Утверждение. $A_n^k = n^{\underline{k}} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) =$

$= \langle (n-k+1), n \rangle = \frac{\langle 1,(n-k)\rangle \cdot \langle (n-k+1),n\rangle}{\langle 1,(n-k)\rangle} = \frac{\langle 1,n\rangle}{\langle 1,(n-k)\rangle} = \frac{n!}{(n-k)!}$.

Доказательство. Будем заполнять позиции элементами нашего множества, состоящего из n элементов.

У нас n способов заполнить 1-ю позицию.

При каждом варианте заполнения 1-й позиции имеется $(n-1)$ способ заполнения 2-й позиции. Всего имеется $n \cdot (n-1)$ способ заполнения 2-х позиций.

При каждом варианте заполнения 2-х позиций имеется $(n-2)$ способов заполнения 3-й позиции. Всего имеется $n \cdot (n-1) \cdot (n-2)$ способов заполнения 3-х позиций.

И так далее, пока не будут заполнены все k позиций.

Получим: $A_n^k = n \cdot (n-1) \cdot \ldots \cdot (n-k+1)$, что и требовалось доказать.

Пример: $A_6^3 = 6 \cdot 5 \cdot 4 = 120$

Определение. Положим по определению $A_n^0 = 1$ для всех $n = 0,1,2,\ldots$

Утверждение. $A_n^k = n \cdot A_{n-1}^{k-1}$.

Доказательство. При каждом из n вариантов заполнения первой позиции имеется A_{n-1}^{k-1} вариантов заполнения остальных позиций.

Используя это рекуррентное соотношение, мы можем заполнять таблицу значений A_n^k (табл. 1).

Таблица 1

n \ k	0	1	2	3	4	…
0	1					
1	1	1				
2	1	2	$2 \cdot 1$			
3	1	3	$3 \cdot 2$	$3 \cdot 2 \cdot 1$		
4	1	4	$4 \cdot 3$	$4 \cdot 3 \cdot 2$	$4 \cdot 3 \cdot 2 \cdot 1$	
5	1	5	$5 \cdot 4$	$5 \cdot 4 \cdot 3$	…	…
6	1	6	$6 \cdot 5$	$6 \cdot 5 \cdot 4$	…	…
7	1	7	$7 \cdot 6$	$7 \cdot 6 \cdot 5$	…	…
…	…	…	…	…	…	…

Приведем еще одно рекуррентное соотношение для чисел размещений.

Утверждение. $A_n^k = k \cdot A_{n-1}^{k-1} + A_{n-1}^k$

Доказательство. Отложим в сторону один любой элемент из множества мощности n. Нам нужно сформировать k -элементное размещение.

Можно поместить отложенный элемент на одну из kпозиций (kвариантов), после чего можно взять $(k-1)$ элемент из оставшихся $(n-1)$ элементов и разместить их на оставшиеся позиции (A_{n-1}^{k-1} вариантов). Всего, таким образом, получается kA_{n-1}^{k-1} вариантов формирования размещения.

Или можно взять все k элементов из оставшихся $(n-1)$ элементов и образовать из них упорядоченный набор, получится A_{n-1}^k вариантов.

Всего получается $k \cdot A_{n-1}^{k-1} + A_{n-1}^k$ способов сформировать нужное размещение.

Здесь значение в клетке таблицы выражено через значения в двух верхних клетках (рис. 2.1).

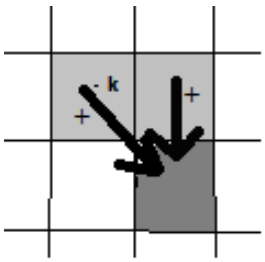


Рисунок 2.1

Упорядоченные наборы символов

Рассмотренные нами размещения могут пониматься как упорядоченные наборы символов длины k, в которых все символы разных типов и всего возможных типов n.

Рассмотрим теперь случай, когда ***типы символов могут повторяться и на каждом месте может располагаться символ, любого из n типов.***

Обозначим число таких наборов D_n^k.

Утверждение. $D_n^k = n^k$.

Доказательство. Будем заполнять позиции символами (у нас n типов символов). Существует n способов заполнить 1-ю позицию.

При каждом варианте заполнения 1-й позиции имеется n способов заполнения 2-й позиции. Всего имеется $n \cdot n = n^2$ способ заполнения 2-х позиций.

При каждом варианте заполнения 2-х позиций имеется n способов заполнения 3-й позиции. Всего имеется $n \cdot n \cdot n = n^3$ способов заполнения 3-х позиций.

И так далее, пока не будут заполнены все k позиций.

Получим: $D_n^k = n \cdot n \cdot \ldots \cdot n = n^k$, что и требовалось доказать.

Отметим очевидное рекуррентное равенство

Утверждение. $D_n^k = n \cdot D_n^{k-1}$.

Рассмотрим теперь ***упорядоченные наборы длины k, в которых встречаются символы n типов, причем для каждого типа известна кратность k_i, с которой присутствует символ этого типа в наборе*** ($k_i \geq 0$, i=1,…,n), $k_1 + \ldots + k_n = k$.

Обозначим число таких различных упорядоченных наборов $A(k_1, \ldots, k_n)$.

Утверждение. $A(k_1,\ldots,k_n)=\frac{k!}{k_1!\cdot\ldots\cdot k_n!}$.

Доказательство. Расположим в ряд k_1 символов 1-го типа, затем k_2 символов 2-го типа и так далее. Рассмотрим всевозможные перестановки этого упорядоченного набора. Их будет $k!$ штук. Все нужные нам упорядоченные наборы будут присутствовать в этом множестве перестановок, даже несколько раз.

Поскольку k_1 символов 1-го типа можно переставлять друг с другом $k_1!$ способами, k_2 символов 2-го типа можно независимо переставлять $k_2!$ способами и т. д., то упорядоченный набор одного и того же облика будет присутствовать в этом множестве перестановок $k_1!\cdot\ldots\cdot k_n!$ раз.

Поэтому, чтобы получить число различных упорядоченных наборов нужно разделить $k!$ на $k_1!\cdot\ldots\cdot k_n!$

Сочетания

Определение. ***Подмножество*** *мощности k в конечном множестве мощности n называется k -элементным* ***сочетанием,*** *взятым из множества мощности n.*

Обозначение. Число различных сочетаний будем обозначать C_n^k.

Замечание. В научной и учебной литературе часто используется также другое обозначение для числа сочетаний: $\binom{n}{k}$.

Утверждение. $C_n^k=\frac{n^{\underline{k}}}{k!}$.

Доказательство. Каждое сочетание можно упорядочить $k!$ способами, поэтому сочетаний в $k!$ раз меньше, чем размещений.

Пример: $C_6^3=\frac{6\cdot5\cdot4}{1\cdot2\cdot3}=20$.

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

Утверждение. $C_n^k=C_n^{n-k}$.

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

Также очевидные комбинаторные соображения доказывают это утверждение, поскольку в n - элементном множестве k - элементных подмножеств столько же, сколько и $(n-k)$ - элементных.

Используя это утверждение, можно всегда добиться того, чтобы верхний

параметр в числе сочетаний составлял не более половины нижнего.

Пример: $C_8^6 = C_8^2 = \frac{8 \cdot 7}{1 \cdot 2} = 28.$

Утверждение. Имеет место следующая рекуррентная формула:

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

Доказательство. Используем комбинаторное рассуждение, подобное проведенному для чисел размещений.

Отложим в сторону один любой элемент из множества мощности n.

Нам нужно сформировать k - элементное подмножество.

Можно взять $(k-1)$ элемент из оставшихся $(n-1)$ элементов и добавить к ним отложенный элемент, это можно сделать C_{n-1}^{k-1} способами.

Или можно набрать все k элементов из оставшихся $(n-1)$ элементов, это можно сделать C_{n-1}^k способами.

Всего получается $C_{n-1}^{k-1} + C_{n-1}^k$ способов сформировать k - элементное подмножество из множества мощности n.

Замечание. Естественно считать, что $C_n^0 = 1$ и при $k \geq 1$ $C_0^k = 0$.

Треугольник Паскаля (Биномиальный треугольник)

Доказанное рекуррентное соотн0ошение позволяет сформировать таблицу значений C_n^k (табл. 2).

Таблица 2

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	0	0	0	
1	1	1	0	0	0	0	0	0	
2	1	2	1	0	0	0	0	0	
3	1	3	3	1	0	0	0	0	
4	1	4	6	4	1	0	0	0	
5	1	5	10	10	5	1	0	0	…
6	1	6	15	20	15	6	1	0	…
7	1	7	21	35	35	21	7	1	…
…	…	…	…	…	…	…	…	…	…

Формула степени бинома (бином Ньютона):

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

$$= a^n + n a^{n-1} b^1 + \ldots + b^n.$$

Доказательство. $(a+b)^n = (a+b)(a+b)\ldots(a+b)$.

После открытия скобок образуются произведения вида $a^{n-k}b^k$, здесь число k – это число множителей $(a+b)$ из которых в этом произведении участвует буква b, а число $(n-k)$ – это число оставшихся множителей $(a+b)$, из них в рассматриваемом произведении участвует буква a.

Всего существует C_n^k способов выбрать из n сомножителей k множителей, поэтому произведений вида $a^{n-k}b^k$ получится C_n^k штук.

Тем самым доказано, что $(a+b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$.

Утверждение. $\sum_{k=0}^{n} C_n^k = C_n^0 + C_n^1 + \ldots + C_n^n = 2^n$.

Доказательство. Подставить в формулу степени бинома $a = b = 1$.

Следствие. Конечное множество, состоящее из n элементов, содержит ровно 2^n различных подмножеств.

Замечание. Комбинаторные числа сочетаний выступают в качестве коэффициентов в формуле степени бинома, поэтому часто их называют *биномиальными коэффициентами*.

Сочетания с повторениями (мультимножества)

Пусть имеется n типов элементов и требуется набрать k элементов из этих имеющихся элементов, при этом могут быть повторяющиеся элементы. Это и есть сочетание с повторениями.

Число различных сочетаний с повторениями будем обозначать $\overline{C}_n^k$ (используется также обозначение $\left(\binom{n}{k}\right)$).

Утверждение. Имеет место следующая рекуррентная формула:

$$\overline{C}_n^k = \overline{C}_{n-1}^k + \overline{C}_n^{k-1}.$$

Доказательство. Проведем рассуждение, подобное уже нами проводившимся для чисел размещений и чисел сочетаний.

Рассмотрим один элемент типа n. Нам нужно набрать k - элементов.

Если элементы этого типа n не входят в наше сочетание, то все k элементов будут из первых $(n-1)$ типов, их можно набрать $\overline{C}_{n-1}^{k}$ способами.

Если же в формируемое сочетание с повторениями входит элемент типа n, то можно взять оставшийся $(k-1)$ элемент из всех n типов элементов и добавить туда отложенный элемент, это можно сделать C_n^{k-1} способами.

Таким образом, получается, что общее число сформировать k - элементное сочетание с повторениями равно $\overline{C}_{n-1}^{k} + \overline{C}_{n}^{k-1}$.

Доказанное рекуррентное соотношение позволяет сформировать таблицу значений $\overline{C}_{n}^{k}$ (табл. 3).

Таблица 3

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	…	…	…	…
1	1	1	1	1	1	…			
2	1	2	3	4	…				
3	1	3	6	10	…				
4	1	4	10	20					
5	1	…	…	…					
6	1								
7	1								
…	…								

Теорема. $\overline{C}_{n}^{k} = \frac{n^{\overline{k}}}{k!}$.

Доказательство. В доказательстве мы будем использовать так называемую *двумерную индукцию.*

Заметим, во-первых, что $\overline{C}_{n}^{0} = 1$ для всех n, а также $\overline{C}_{0}^{k} = 0$ для всех положительных k.

Пусть формула верна для $\overline{C}_{n-1}^{k}$ и для $\overline{C}_{n}^{k-1}$.

$$\overline{C}_{n}^{k} = \overline{C}_{n-1}^{k} + \overline{C}_{n}^{k-1} = \frac{(n-1)^{\overline{k}}}{k!} + \frac{n^{\overline{k-1}}}{(k-1)!} = \frac{\langle n-1, n+k-2\rangle}{k!} + \frac{\langle n, n+k-2\rangle}{(k-1)!} =$$

$$= \frac{\langle n, n+k-2\rangle}{(k-1)!} \cdot \left(\frac{n-1}{k} + 1\right) = \frac{\langle n, n+k-2\rangle}{(k-1)!} \cdot \frac{n+k-1}{k} = \frac{\langle n, n+k-1\rangle}{k!} = \frac{n^{\overline{k}}}{k!}.$$

Пример: $\overline{C}_2^3 = \frac{2^{\overline{3}}}{3!} = \frac{2 \cdot 3 \cdot 4}{1 \cdot 2 \cdot 3} = 4.$

Итак, мы получили схожие формулы для чисел сочетаний и чисел сочетаний с повторениями: $C_n^k = \frac{n^{\underline{k}}}{k!}$ и $\overline{C}_n^k = \frac{n^{\overline{k}}}{k!}$.

Эти формулы можно доказать единообразными комбинаторными рассуждениями (А.Н. Выборнов).

Начнем наше рассмотрение с **чисел сочетаний** $C_n^k = \binom{n}{k}$.

Докажем формулу $C_n^k = \frac{n^{\underline{k}}}{k!} = \frac{n(n-1)\ldots(n-k+1)}{1 \cdot 2 \cdot \ldots \cdot k}$.

Фиксируем n. Будем использовать индукцию по k. Равенство выполнено для $k = 1$. Докажем, что $C_n^k = C_n^{k-1} \cdot \frac{(n-k+1)}{k}$.

Рассмотрим n -элементное множество A. Пусть имеется набор M_{k-1} всех $(k-1)$ - элементных подмножеств множества A.

Образуем набор, включающий в себя все k - элементные подмножества множества A, каждое по несколько раз. Для этого для каждого сочетания из M_{k-1} добавим к нему еще один из элементов A, не присутствующий в этом сочетании. Из каждого сочетания мощности $(k-1)$ мы получим $(n-k+1)$ сочетаний мощности k.

Докажем, что в новом наборе каждое сочетание мощности k будет представлено в k экземплярах. Рассмотрим сочетание $\{a_1, a_2, \ldots, a_k\}$. Это сочетание образовалось из сочетаний мощности $(k-1)$ путем добавления одного элемента. Каждый из k элементов множества$\{a_1, a_2, \ldots, a_k\}$мог быть добавлен. Поэтому рассматриваемое сочетание получалось k раз.

Следовательно, в новом наборе, состоящий из $C_n^{k-1} \cdot (n-k+1)$ штук k -элементных сочетаний будет $k \cdot C_n^k$ сочетаний.

То есть $k \cdot C_n^k = C_n^{k-1} \cdot (n-k+1)$, откуда получаем $C_n^k = C_n^{k-1} \cdot \frac{(n-k+1)}{k}$.

Теперь рассмотрим **числа сочетаний с повторениями** $\bar{C}_n^k = \left(\binom{n}{k}\right)$.

Докажем формулу $\bar{C}_n^k = \frac{n^{\bar{k}}}{k!} = \frac{n(n+1)\ldots(n+k-1)}{1 \cdot 2 \cdot \ldots \cdot k}$.

Фиксируем n. Равенство выполнено для $k = 1$.

Докажем, что $\bar{C}_n^k = \bar{C}_n^{k-1} \cdot \frac{(n+k-1)}{k}$.

Пусть есть n типов элементов. Пусть имеется набор N_{k-1} всех сочетаний с повторениями мощности $(k-1)$, состоящих из элементов n возможных типов.

Образуем новый набор, состоящий из сочетаний с повторениями мощности k из элементов n типов. Для каждого сочетания с повторениями из N_{k-1} образуем $(n+k-1)$ сочетаний с повторениями мощности k следующим образом. Пусть $\{a_1, a_2, \ldots, a_{k-1}\}$- сочетание с повторениями, добавим к нему элемент, совпадающий по типу с a_i ($(k-1)$ способ), или элемент любого из n типов (n способов). Всего из каждого сочетания с повторениями мощности $(k-1)$ получится $(k-1+n)$ сочетаний с повторениями мощности k.

Очевидно, что в этом новом наборе присутствуют все сочетания с повторениями мощности k. Докажем, что каждое сочетание с повторениями мощности k представлено в этом новом наборе ровно k раз.

Рассмотрим сочетание $\{a_1, a_2, \ldots, a_k\}$. Пусть элемент a_i является элементом типа j, и это сочетание содержит m элементов типа j. Тогда, если мы уберем из этого сочетания элемент типа j, то получим сочетание с повторениями мощности $(k-1)$, которое находится в N_{k-1}. В нем присутствует $(m-1)$ элемент типа j. Если рассматриваемое сочетание получилось из этого сочетания добавлением элемента типа j, то всего таких сочетаний получилось m штук (дублировался $(m-1)$ элемент и добавлялся элемент типа j). Итак, сочетание, состоящее из $m_1 + m_2 + \ldots + m_l = k$ элементов l типов (элемент типа j повторен m_j раз), представлено в новом наборе $m_1 + m_2 + \ldots + m_l = k$ экземплярами.

Поэтому $k \cdot \bar{C}_n^k = \bar{C}_n^{k-1} \cdot (n+k-1)$, и $\bar{C}_n^k = \bar{C}_n^{k-1} \cdot \frac{(n+k-1)}{k}$.

Рассмотрим еще одно утверждение, в котором число сочетаний с повторениями выражено через обычное число сочетаний.

Утверждение. Имеет место следующая формула: $\overline{C}_n^k = C_{n+k-1}^k$.

Доказательство

$$\overline{C}_n^k = \frac{n^{\overline{k}}}{k!} = \frac{n \cdot (n+1) \cdot \ldots \cdot (n+k-1)}{k!} = \frac{\langle n, (n+k-1) \rangle}{k!} = \frac{(n+k-1)^{\underline{k}}}{k!} = C_{n+k-1}^k.$$

Замечание. Формулу доказанного утверждения некоторые авторы

используют как основную формулу для вычисления чисел сочетаний с повторениями и доказывают ее искусственным приемом «звездочек и перегородок». Изложенный нами путь глубже и гармоничнее.

2.3. Разбиения

Числа Стирлинга 2-го рода

Определение. *Числом Стирлинга 2-го рода* S_n^k называется *число различных разбиений* n -элементного множества на k непустых подмножеств.

Естественно считать, что:

$S_0^k = 0$ при $k \geq 1$,

$S_n^0 = 0$ при $n \geq 1$,

$S_0^0 = 1$.

Замечание. Используется также другое обозначение для чисел Стирлинга 2-го рода: $\begin{Bmatrix} n \\ k \end{Bmatrix}$.

Имеет место простое двумерное рекуррентное соотношение для чисел Стирлинга 2-го рода, подобное соотношениям для чисел размещений, чисел сочетаний и чисел сочетаний с повторениями.

Утверждение. $S_n^k = S_{n-1}^{k-1} + k \cdot S_{n-1}^k$.

Доказательство. Пометим один из элементов разбиваемого n - элементного множества.

Нам нужно получить разбиение n - элементного множества на k непустых частей.

Можно образовать из помеченного элемента отдельную часть, и далее разбить множество, состоящее из оставшихся $(n-1)$ элементов на $(k-1)$ часть (S_{n-1}^{k-1} способ). Или можно разбить множество, состоящее из оставшихся $(n-1)$ элементов на k частей, и присоединить к одной из частей помеченный элемент, ($k \cdot S_{n-1}^k$ способ).

Итого: $k \cdot S_{n-1}^k + S_{n-1}^{k-1}$ способ.

Утверждение доказано.

Доказанное рекуррентное соотношение позволяет сформировать таблицу значений S_n^k (табл. 4).

Таблица 4

n \ k	0	1	2	3	4	5	6	7	8	…
0	1	0	0	0	0	0	0	0	0	
1	0	1	0	0	0	0	0	0	0	…
2	0	1	1	0	0	0	0	0	0	…
3	0	1	3	1	0	0	0	0	0	…
4	0	1	7	6	1	0	0	0	0	…
5	0	1	15	25	10	1	0	0	0	…
6	0	1	31	90	65	15	1	0	0	…
7	0	1	63	301	350	140	21	1	0	…
8	0	1	127	966	1701	1050	266	28	1	…
…		…	…	…	…	…	…	…	…	…

Замечание. Имеет место громоздкая формула для прямого вычисления чисел Стирлинга 2-го рода:

$$S_n^k = \sum_{\substack{j_1,\dots,j_n\geq 0 \\ 1\cdot j_1+\dots+n\cdot j_n=n \\ j_1+\dots+j_n=k}} \frac{n!}{\prod_{i=1}^{n}((i!)^{j_i}j_i!)}.$$

Для ее доказательства достаточно заметить, что число различных разбиений n - элементного множества на k непустых частей, среди которых j_1 одноэлементных, j_2 двухэлементных, …, j_n n -элементных частей будет равно

$$\frac{n!}{\prod_{i=1}^{n}((i!)^{j_i}j_i!)},$$

поскольку можно рассмотреть перестановку из элементов разбиваемого множества, образовать нужное разбиение, образовав, набирая элементы слева направо, j_1 часть из одного элемента, j_2 частей из двух элементов и т.д.

Разбиение остается тем же, если переставлять элементы внутри частей или переставлять местами части одинаковой мощности, поэтому для нахождения числа разбиений нужно число перестановок разделить на $\prod_{i=1}^{n}((i!)^{j_i}j_i!)$.

Следующую теорему мы докажем позже.

Теорема (формула Стирлинга)

$$S_n^k = \frac{1}{k!}\sum_{i=0}^{k-1}(-1)^i C_k^i (k-i)^n =$$

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

Числа Белла

Определение. *Числом Белла* B_n называется *полное число различных разбиений* n - элементного множества на непустые части.

Очевидно, что число Белла равно сумме чисел Стирлинга 2-го рода:

$$B_n = \sum_{k=0}^{n} S_n^k.$$

По определению положим: $B_0 = 1$.

Имеет место рекуррентное соотношение для чисел Белла:

Утверждение

$$B_{n+1} = \sum_{k=0}^{n} C_n^k B_k\,.$$

Доказательство. Фиксируем один элемент в $(n+1)$ - элементном множестве. Для каждого $k = 0, \ldots, n$ формируем разбиения этого множества, выбирая $(k+1)$ - элементную часть, содержащую фиксированный элемент (C_n^k способов), и разбивая его дополнение B_{n-k} способами на части.

Получим

$$B_{n+1} = \sum_{k=0}^{n} C_n^k B_{n-k} = \sum_{k=0}^{n} C_n^{n-k} B_{n-k} = \sum_{n-k=0}^{n} C_n^{n-k} B_{n-k} = \sum_{k=0}^{n} C_n^k B_k\,.$$

Замечание. В доказательстве использовано, приведенное нами ранее, свойство биномиальных коэффициентов:

$C_n^k = C_n^{n-k}$, которое вытекает из формулы $C_n^k = \frac{n!}{(n-k)!\cdot k!}$.

Числа Стирлинга 1-го рода

Определение. *Числом Стирлинга 1-го рода* s_n^k называется *число различных разбиений* n - элементного множества на k *циклически упорядоченных* подмножеств.

Это число совпадает с числом подстановок длины n, раскладывающихся в произведение k независимых циклов (при этом элементы, не участвующие в циклах длины ≥ 2, считаются циклами длины 1).

Естественно считать, что: $s_0^k = 0$ при $k \geq 1$, $s_n^0 = 0$ при $n \geq 1$, и $s_0^0 = 1$.

Замечание. Используется также другое обозначение для чисел Стирлинга 1-го рода: $\begin{bmatrix} n \\ k \end{bmatrix}$.

Имеет место простое двумерное рекуррентное соотношение для чисел Стирлинга 1-го рода, подобное соотношениям для чисел размещений, чисел сочетаний, чисел сочетаний с повторениями и чисел Стирлинга 2-го рода.

Утверждение. $s_n^k = s_{n-1}^{k-1} + (n-1) \cdot s_{n-1}^k$.

Доказательство. Пометим один из элементов. Нам нужно получить подстановку длины n, являющиеся произведением k циклов.

Можно образовать из помеченного элемента отдельный цикл, и добавить его к $(k-1)$ циклам, действующим на оставшихся $(n-1)$элементах, (s_{n-1}^{k-1} способ).

Или можно взять подстановку длины $(n-1)$, действующую на оставшихся элементах и имеющую k циклов и присоединить к одному из циклов помеченный элемент. Это можно сделать $(n-1) \cdot s_{n-1}^k$ способами, поскольку есть l способов присоединить один элемент к циклу длины l, а суммарная длина циклов равна $(n-1)$.

Итого: $(n-1) \cdot s_{n-1}^k + s_{n-1}^{k-1}$ способ.

Утверждение доказано.

Замечание. Имеет место громоздкая формула для прямого вычисления чисел Стирлинга 1-го рода

$$s_n^k = \sum_{\substack{j_1,\dots,j_n \geq 0 \\ 1 \cdot j_1 + \dots + n \cdot j_n = n \\ j_1 + \dots + j_n = k}} \frac{n!}{\prod_{i=1}^n (i^{j_i} j_i!)}.$$

Для ее доказательства достаточно заметить, что число подстановок длины n, являющихся произведением k независимых циклов, среди которых j_1 циклов длины 1, j_2 циклов длины 2, …, j_n циклов длины n, будет равно

$$\frac{n!}{\prod_{i=1}^{n}(i^{j_i}j_i!)},$$

поскольку можно рассмотреть перестановку из элементов разбиваемого множества, образовать нужную подстановку, набирая элементы для циклов слева направо, j_1 цикл из одного элемента, j_2 циклов из двух элементов и т.д. Подстановка остается той же, если циклически переставлять элементы внутри циклов или переставлять местами циклы одинаковой длины, поэтому для нахождения числа подстановок нужно число перестановок разделить на $\prod_{i=1}^{n}(i^{j_i}j_i!)$.

Доказанное рекуррентное соотношение $s_n^k = s_{n-1}^{k-1} + (n-1)\cdot s_{n-1}^k$ позволяет сформировать таблицу значений s_n^k (табл. 5).

Таблица 5

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	0	0	0	…
1	0	1	0	0	0	0	0	0	…
2	0	1	1	0	0	0	0	0	…
3	0	2	3	1	0	0	0	0	…
4	0	6	11	6	1	0	0	0	…
5	0	24	50	35	10	1	0	0	…
6	0	120	274	225	85	15	1	0	…
7	0	720	1764	1624	735	175	21	1	…
…	…	…	…	…	…	…	…	…	…

Числа Лаха

Определение. *Числом Лаха* L_n^k называется *число различных разбиений* n -элементного множества на k *линейно упорядоченных* классов.

Утверждение. $L_n^k = L_{n-1}^{k-1} + (n+k-1)\cdot L_{n-1}^k$.

Доказательство. Пометим один из элементов разбиваемого n -элементного множества. Нам нужно получить разбиение n - элементного множества на k линейно упорядоченных непустых частей.

Можно образовать из помеченного элемента отдельную часть, и далее разбить множество, состоящее из оставшихся $(n-1)$ элементов на $(k-1)$ часть (L_{n-1}^{k-1} способ).

Или можно разбить множество, состоящее из оставшихся $(n-1)$

элементов на k линейно упорядоченных частей, и присоединить к одной из частей помеченный элемент, ($(n+k-1)\cdot L_{n-1}^{k}$ способ).

Поясним: пусть у нас в разбиении получились части мощности $l_1,\ldots,l_k$, в каждую часть помеченный элемент можно внедрить l_i+1 способами, поэтому всего способов для каждого разбиения:

$(l_1+1)+\ldots+(l_k+1)=(l_1+\ldots+l_k)+(1+\ldots+1)=n-1+k$;

Всего получаем $(n+k-1)\cdot L_{n-1}^{k}+L_{n-1}^{k-1}$ способов.

Утверждение доказано.

Доказанное рекуррентное соотношение позволяет сформировать таблицу значений L_n^k (табл. 6).

Таблица 6

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	0	0	0	
1	0	1	0	0	0	0	0	0	…
2	0	2	1	0	0	0	0	0	…
3	0	6	6	1	0	0	0	0	…
4	0	24	36	12	1	0	0	0	…
5	0	120	240	120	20	1	0	0	…
6	0	720	1800	1200	300	30	1	0	…
7	0	5040	15120	12600	4200	630	42	1	…
8									…

Мы считаем, что $L_n^0=0$.

Для чисел Лаха есть простая формула.

Утверждение. $L_n^k=C_{n-1}^{k-1}\cdot\frac{n!}{k!}$

Доказательство. Достаточно проверить выполнение рекуррентного соотношения $L_n^k=(n+k-1)\cdot L_{n-1}^{k}+L_{n-1}^{k-1}$, то есть нужно проверить тождество:

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

Оставляем это читателям в качестве упражнения.

Можно также доказать это утверждение следующим прямым комбинаторным рассуждением.

Выстроим все элементы разбиваемого множества в линеечку ($n!$ способов).

У нас есть $(n-1)$ промежуток между элементами, в которые мы поставим

$(k-1)$ перегородку (C_{n-1}^{k-1}способ), определив тем самым разбиение нашего множества на линейно упорядоченные части. Получившиеся k частей можно переставлять $k!$ способами, разбиение останется тем же. Получили $L_n^k = \frac{n!\cdot C_{n-1}^{k-1}}{k!}$.

Числа Стирлинга и Лаха и факториальные степени

Шотландский математик 18 века Джеймс Стирлинг обнаружил числа, которые мы называем числами Стирлинга, открыв скобки в выражении для факториальной степени. Числа Стирлинга 1-го рода возникают как коэффициенты при степенях переменной x в многочлене $P_n(x) = x\cdot(x+1)\cdot\ldots\cdot(x+n-1)$.

Напомним, что $x^{\overline{n}} = x\cdot(x+1)\cdot\ldots\cdot(x+n-1)$.

Имеет место следующая теорема.

Теорема

$$1)\ x^{\overline{n}} = s_n^0x^0 + s_n^1x^1 + s_n^2x^2 + \cdots + s_n^nx^n = \sum_{k=0}^{n} s_n^kx^k;$$

$$2)\ x^{\underline{n}} = (-1)^{n-0}s_n^0x^0 + (-1)^{n-1}s_n^1x^1 + (-1)^{n-2}s_n^2x^2 + \cdots + (-1)^{n-n}s_n^nx^n = \sum_{k=0}^{n}(-1)^{n-k}s_n^kx^k;$$

$$3)\ x^n = \sum_{k=0}^{n} S_n^kx^{\underline{k}};$$

$$4)\ x^n = \sum_{k=0}^{n}(-1)^{n-k}S_n^kx^{\overline{k}};$$

$$5)\ x^{\overline{n}} = \sum_{k=0}^{n} L_n^kx^{\underline{k}};$$

$$6)\ x^{\underline{n}} = \sum_{k=0}^{n}(-1)^{n-k}L_n^kx^{\overline{k}}.$$

Доказательство. Для доказательства нужно использовать рекуррентные соотношения для чисел Стирлинга и Лаха.

Докажем первый пункт теоремы. Остальные пункты доказываются аналогично. Имеем:

$x^{\overline{n}} = x\cdot(x+1)\cdot\ldots\cdot(x+n-1)$;

$x^{\overline{n+1}} = x \cdot (x+1) \cdot \ldots \cdot (x+n-1) \cdot (x+n).$

Поэтому $x^{\overline{n+1}} = x^{\overline{n}} \cdot (x+n).$

Далее, используем индуктивное рассуждение. Формула верна для $n = 1$.

Пусть формула верна для n, докажем, что она выполнена для $(n+1)$.

Итак, $x^{\overline{n}} = s_n^0 x^0 + s_n^1 x^1 + s_n^2 x^2 + \ldots + s_n^n x^n$. Тогда

$x^{\overline{n+1}} = x^{\overline{n}}(x+n) = x^{\overline{n}} \cdot x + x^{\overline{n}} \cdot n =$

$=(s_n^0 x^0 + s_n^1 x^1 + s_n^2 x^2 + \cdots + s_n^n x^n) \cdot x + (s_n^0 x^0 + s_n^1 x^1 + s_n^2 x^2 + \cdots + s_n^n x^n) \cdot n = (s_n^0 x^1 + s_n^1 x^2 + s_n^2 x^3 + \cdots + s_n^n x^{n+1}) + +(n \cdot s_n^0 x^0 + n \cdot s_n^1 x^1 + n \cdot s_n^2 x^2 + \cdots + n \cdot s_n^n x^n) = n \cdot s_n^0 x^0 + (s_n^0 + n \cdot s_n^1) x^1 + (s_n^1 + n \cdot s_n^2) x^2 + \ldots = s_{n+1}^0 x^0 + s_{n+1}^1 x^1 + s_{n+1}^2 x^2 + \ldots + s_{n+1}^{n+1} x^{n+1}.$

Рекомендуем читателям провести подробные доказательства всех остальных пунктов теоремы.

Эта теорема имеет следующую трактовку в терминах линейной алгебры.

Рассмотрим линейное пространство всех многочленов (с действительными коэффициентами) степени не выше n.

В этом линейном пространстве можно рассмотреть три базиса:

$E = (1, x, x^2, \ldots, x^n),$

$\overline{E} = (1, x, x^{\overline{2}}, \ldots, x^{\overline{n}}),$

$\underline{E} = (1, x, x^{\underline{2}}, \ldots, x^{\underline{n}}).$

Первый базис состоит из степеней x, а второй и третий из факториальных степеней.

Из теоремы можно увидеть, что каждый из этих базисов линейно выражается через другой, в качестве коэффициентов выступают числа Стирлинга или числа Лаха (где-то со знаком минус).

Таким образом, соответствующие матрицы перехода от одного базиса к другому будут заполнены числами Лаха или числами Стирлинга 1-го или 2-го рода (может быть с добавленными минусами как во 2-м, 4-м и 6-м случаях).

Задача. Рассмотрите случай $n = 3$ и запишите все матрицы перехода (6 случаев).

Замечание. Рассмотрим еще один базис в пространстве многочленов:
$\hat{E} = (1, (x+1), (x+1)^2, \ldots, (x+1)^n)$.

Ввиду формулы степени бинома (бинома Ньютона)

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

то есть матрица перехода от E к $\hat{E}$ будет состоять из биномиальных коэффициентов.

Разбиения чисел

Если элементы разбиваемого множества неразличимы, то каждое разбиение полностью характеризуется мощностями подмножеств разбиения. Это эквивалентно представлению натурального числа, выражающего мощность разбиваемого множества в виде суммы натуральных чисел – мощностей подмножеств разбиения (порядок слагаемых не имеет значения).

Обозначим через P_n^k число способов представления натурального числа n в виде суммы k натуральных слагаемых.

Следующее утверждение содержит рекуррентную формулу для чисел P_n^k.

Утверждение. $P_n^k = P_{n-1}^{k-1} + P_{n-k}^k$

Доказательство. Каждое разбиение числа n на k натуральных слагаемых либо содержит среди слагаемых число 1 (таких разбиений P_{n-1}^{k-1} штук), либо не содержит среди слагаемых число 1 (таких разбиений столько же сколько разбиений числа $(n-k)$ на k натуральных слагаемых, то есть P_{n-k}^k штук, поскольку из каждого слагаемого такого разбиения можно убрать по единице).

Всего получается $P_{n-1}^{k-1} + P_{n-k}^k$ разбиений.

Доказанное рекуррентное соотношение позволяет сформировать таблицу значений P_n^k (табл. 7).

Таблица 7

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0	0	0	0	…
1	0	1	0	0	0	0	0	0	…
2	0	1	1	0	0	0	0	0	…
3	0	1	1	1	0	0	0	0	…
4	0	1	2	1	1	0	0	0	…
5	0	1	2	2	1	1	0	0	…
6	0	1	3	3	2	15	1	0	…
7	0	1	3	4	3	175	1	1	…
…	…	…	…	…	…	…	…	…	…

Для чисел разбиений натурального числа в сумму натуральных слагаемых нет простой формулы для их прямого вычисления, поэтому использование рекуррентных соотношений для вычисления этих комбинаторных чисел (по сути, заполнение приведенной выше таблицы) является единственным путем получения их значений.

Для чисел Стирлинга, для которых также нет простых прямых формул, использование рекуррентных соотношений является наилучшим выбором.

Комбинаторные отображения (двенадцать сценариев, twelvefold way)

Многие задачи комбинаторики сводятся к изучению отображений из одного конечного множества в другое.

Рассмотрим два множества A и B. Пусть $|A| = n$ и $|B| = k$.

Рассмотрим функции $f: A \to B$. Мы будем вводить различные отношения эквивалентности на множестве таких функций и вычислять число получившихся классов эквивалентности. Будем различать случаи, когда элементы множеств A или B различимы или неразличимы (4 случая), а также когда функция f будет произвольной функцией, будет инъекцией, или будет сюръекцией (3 случая). Всего получится $4 \cdot 3 = 12$ случаев.

В случае неразличимости элементов множества A две функции $f_1: A \to B$ и $f_2: A \to B$ мы считаем эквивалентными, если некоторой перестановкой элементов множества A одна функция может быть переведена в другую. Точнее говоря, существует такая биекция $\sigma: A \to A$, что $f_2 = \sigma \circ f_1$, то есть $\forall a \in A$ выполнено $f_2(a) = f_1(\sigma(a))$.

Аналогично определяется отношение эквивалентности в случае неразличимости элементов множества B. Две функции будут эквивалентными, если существует перестановка $\pi: B \to B$ элементов множества B, такая что $f_2 = f_1 \circ \pi$, то есть $\forall a \in A$ выполнено $f_2(a) = \pi(f_1(a))$ (рис. 2.2).

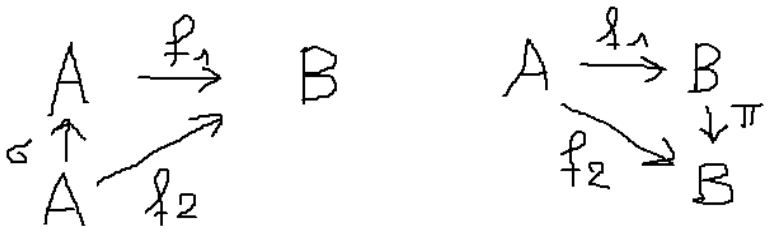


Рисунок 2.2

Нетрудно проверить, что мы действительно определили отношения эквивалентности.

Рассматриваемые задачи можно интерпретировать как размещения различимых или неразличимых шариков (множество A) по различимым или неразличимым коробкам (множество B). Тогда, если f - инъекция, в каждой коробке не более одного шарика, а если f - сюръекция, то нет пустых коробок.

Представим формулы, задающие соответствующие числа классов эквивалентности, для каждого из 12 случаев в таблице 8.

Таблица 8

Элементы множества A	Элементы множества B	f – произвольная функция	f - инъекция, $n \le m$	f - сюръекция, $n \ge m$
Различимы	различимы	k^n	A_k^n	$k!\,S_n^k$
Неразличимы	различимы	$\overline{C}_k^n$	C_k^n	$\overline{C}_k^{n-k}$
Различимы	неразличимы	$\sum_{i=1}^{k} S_n^i$	1	S_n^k
Неразличимы	неразличимы	$\sum_{i=1}^{k} P_n^i$	1	P_n^k

Проведем доказательство правильности наполнения клеток таблицы.

Первая строчка: шарики различимы, коробки различимы

1) каждый из n шариков может оказаться в любой из k коробок, для него

k вариантов расположения, всего вариантов $k \cdot k \cdot \ldots \cdot k = k^n$,
2) коробок не меньше, чем шариков, в каждой коробке не более одного шарика, число вариантов равно числу размещений из множества k коробок на n позиций (шариков): A_k^n,
3) шариков не меньше, чем коробок, нет пустых коробок, число вариантов равно числу разбиений множества шариков на k частей, с учетом порядка перечисления частей: $k!\, S_n^k$.

Вторая строчка: шарики неразличимы, коробки различимы
1) есть k типов шариков (тип шарика определяется коробкой, в которой он размещен), нужно набрать всего n шариков, здесь число вариантов равно числу сочетаний с повторений для выбора n элементов из элементов k типов (тип шарика определяется коробкой, в которой он размещен): $\overline{C}_k^n$,
2) коробок не меньше, чем шариков, в каждой коробке не более одного шарика, число вариантов равно числу способов выбрать n коробок из множества k коробок, в которых будет по одному шарику: C_k^n,
3) шариков не меньше чем коробок, нет пустых коробок, при подсчете числа вариантов учтем, что в каждой коробке не меньше одного шарика, поэтому разместим вначале в каждой коробке по шарику, остается разместить $(n-k)$ шариков, поэтому число вариантов равно числу сочетаний с повторений для выбора $(n-k)$ элементов из элементов k типов: $\overline{C}_k^{n-k}$.

Третья строчка: шарики различимы, коробки неразличимы
1) здесь число вариантов равно числу способов разбить множество из n различимых шариков на не более чем k частей: $\sum_{i=1}^{k} S_n^i$,
2) коробок не меньше, чем шариков, в каждой коробке не более одного шарика, поскольку коробки неразличимы, здесь лишь один вариант размещения,
3) шариков не меньше, чем коробок, нет пустых коробок, число вариантов равно числу разбиений множества из n различимых шариков на k частей: S_n^k.

Четвертая строчка: шарики неразличимы, коробки неразличимы
1) здесь число вариантов равно числу способов разбить множество из n неразличимых шариков на не более чем k кучек, то есть числу способов разбить натуральное число n в сумму не более чем k слагаемых: $\sum_{i=1}^{k} P_n^i$,
2) коробок не меньше, чем шариков, в каждой коробке не более одного шарика, поскольку коробки не различимы, здесь лишь один вариант размещения,

3) шариков не меньше, чем коробок, нет пустых коробок, здесь число вариантов равно числу способов разбить множество из n неразличимых шариков на k кучек, то есть числу способов разбить натуральное число n в сумму k слагаемых: P_n^k.

Числа Каталана

Числа Каталана были открыты Леонардом Эйлером в 1740 году. Он рассматривал число способов разбиения диагоналями выпуклого многоугольника на треугольники (рис. 2.3). Он получил формулу для этого числа, об этом он сообщил в письме Христиану Гольдбаху.

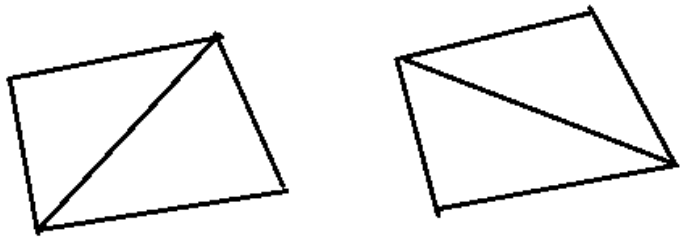


Рисунок 2.3

Числа названы в честь французского математика 19 века Эжена Каталана. (Имя Каталана прославила также **гипотеза Каталана**, которую он сформулировал в 1844 году – это утверждение, согласно которому уравнение:
$x^a - y^b = 1$, $(a, b > 1)$ имеет только одно решение в натуральных числах
$x = 3, a = 2, y = 2, b = 3$.

Гипотеза доказана немецким математиком Михэйлеску лишь в 2002 году.)

Обозначим n -е число Каталана K_n (общепринятое обозначение C_n, но нам так сейчас удобнее). Существует много комбинаторных задач, решением которых являются числа Каталана, например:

1) K_n - число разбиений выпуклого $(n + 2)$-угольника на треугольники.

2) K_n - число полных *бинарных деревьев* с n внутренними узлами (будем говорить о них позже).

3) K_n - число *слов фон Дика* длины $2n$. Слово фон Дика – это строка, состоящая из n символов “X” и n символов “Y”, такая, что в любом ее начальном отрезке символов “X” не меньше, чем символов “Y”. Например: XXYXYY или XYXYXY.

4) K_n - число способов, которыми в произведении, состоящем из $(n + 1)$-го

сомножителя, может быть расставлены скобки, устанавливающие порядок выполнения умножений, например: $a\big((bc)d\big)$ или $(ab)(cd)$.

5) K_n - число перестановок длины n, не содержащих трех элементов, следующих в возрастающем порядке, например: 1432 или 2143 или 3412.

6) K_n - число перестановок длины n, элементы которых можно отсортировать, располагая только одним *стеком*. Это доказано Д. Кнутом в 1968 году.

Приведем первые значения K_n: для $n = 0,1,2,3,4,5$ $K_n = 1,1,2,5,14,42$.

Возьмем за определение чисел Каталана числа, указанные в 3-м примере.

Рассмотрим следующее обобщение чисел Каталана.

Определение. Числом K_n^m назовем число строк, состоящих из n символов “X” и m символов “Y”, таких, что в любом начальном отрезке строки символов “X” не меньше, чем символов “Y”.

Легко проверить утверждение.

Утверждение

1) $K_n^0 = 1$ для $n \geq 0$,

2) $K_n^1 = n$ для $n \geq 1$,

3) $K_{n+1}^{n+1} = K_{n+1}^n$ для $n \geq 1$.

Имеет место также утверждение, содержащее рекуррентную формулу для чисел K_n^m.

Утверждение. $K_n^m = K_n^{m-1} + K_{n-1}^m$ для $1 < m < n$

Доказательство. Рассмотрим всех множество строк, состоящих из n символов “X” и m символов “Y”, таких, что в любом начальном отрезке строки символов “X” не меньше, чем символов “Y”. Разобьем его на две группы.

К первой группе отнесем строки, оканчивающиеся на “X”, в этой группе будет всего K_{n-1}^m строк.

Ко второй группе отнесем строки, оканчивающиеся на “Y”, в этой группе будет всего K_n^{m-1} строк. Утверждение доказано.

Приведенные утверждения позволяют заполнять таблицу значений K_n^m (табл. 9).

Таблица 9

n \ k	0	1	2	3	4	5	6	7	…
0	1								
1	1	1							
2	1	2	2						
3	1	3	5	5					
4	1	4	9	14	14				
5	1	5	14	28	42	42			
6	1	6	20	48	90	132	132		
7	1	7	27	75	165	297	429	429	
…	…	…	…	…	…	…	…	…	…

Теперь, используя два последних утверждения, мы можем доказать теорему.

Теорема. $K_n^m = C_{n+m}^m - C_{n+m}^{m-1}$

Доказательство. Используем двумерную индукцию.

1) Нужно проверить формулу, подставив $K_n^m = C_{n+m}^m - C_{n+m}^{m-1}$ во всех трех пунктах первого из предыдущих утверждений (основание индукции).

2) Нужно подставить $K_n^m = C_{n+m}^m - C_{n+m}^{m-1}$ в выражение второго утверждения (шаг индукции).

Выкладку оставляем читателям в качестве полезного упражнения.

Теорема доказана.

Следствие. $K_n^m = \frac{n-m+1}{n+1} C_{n+m}^m$.

Следствие легко доказывается прямой выкладкой.

Вернемся к числам Каталана. Очевидно, что $K_n = K_n^n$. Поэтому немедленно получаем прямые формулы для вычисления чисел Каталана.

Теорема. $K_n = C_{2n}^n - C_{2n}^{n-1} = \frac{1}{n+1} C_{2n}^n$.

Можно предложить также прямое комбинаторное этой формулы, выражающей числа Каталана через биномиальные коэффициенты.

Доказательство теоремы (А.Н. Выборнов).

Докажем формулу $K_n = C_{2n}^n - C_{2n}^{n-1}$.

Во-первых, заметим, что $C_{2n}^{n-1} = C_{2n}^{n+1}$, поэтому мы можем доказывать формулу $K_n = C_{2n}^n - C_{2n}^{n+1}$.

Будем рассматривать число Каталана как число различных наборов, состоящих из n символов «+1» и n символов «-1», таких для любого начального

отрезка этой записи, трактуемой как арифметическое выражение, получаемое число будет неотрицательно. Например: +1-1+1+1-1-1.

Общее число упорядоченных наборов из n символов «+1» и n символов «-1» равно C_{2n}^{n}.

Докажем, что «некаталановых» наборов среди них будет ровно C_{2n}^{n+1} штук.

Рассмотрим любой набор из $(n-1)$ символов «+1» и $(n+1)$ символов «-1» (таковых $C_{2n}^{n-1} = C_{2n}^{n+1}$ штук). Сумма всех элементов такого набора равна (-2), поэтому найдется «массив» из последовательно расположенных, по меньшей мере 2-х символов «-1».

Изменим конечный символ в самом правом из таких массивов на символ «+1». Полученный набор будет некаталановым.

Итак, всякому набору из $(n-1)$ символов «+1» и $(n+1)$ символов «-1» соответствует некаталанов набор из n символов «+1» и n символов «-1». Это соответствие будет взаимно однозначным. Действительно, рассмотрим любой некаталанов набор из n символов «+1» и n символов «-1». Найдем в этом наборе самый правый символ «+1», которому предшествует символ «-1» и за которым не следует символ «-1». Заменим его на символ «-1». Получим набор из $(n-1)$ символов «+1» и $(n+1)$ символов «-1». Замененный символ будет в полученном наборе конечным символом в самом правом массиве из символов «-1».

Тем самым доказательство завершено.

2.4. Производящие функции

Понятие производящей функции ввел в начале 18-го века Авраам де Муавр (великий математик, открывший важнейшее в теории вероятности и математической статистике **нормальное распределение**).

Определение. Рассмотрим (бесконечную) последовательность действительных чисел: $a_0, a_1, a_2, \ldots$

Производящей функцией (обыкновенной производящей функцией) этой последовательности называется формальный *степенной ряд*:

$$a_0 + a_1 x^1 + a_2 x^2 \ldots = \sum_{n=0}^{\infty} a_n x^n.$$

Пример:

Рассмотрим последовательность $1,1,1,\ldots$

Производящая функция этой последовательности – это ряд

$$1 + 1 \cdot x^1 + 1 \cdot x^2 \ldots = \sum_{k=0}^{\infty} x^n.$$

В школьном курсе математики (9 класс) содержится формула для суммы бесконечной геометрической прогрессии со знаменателем q ($|q| < 1$) и первым членом b_1: $S = \frac{b_1}{1-q}$.

Итак, получаем, что ряд

$$1 + x^1 + x^2 \ldots = \sum_{k=0}^{\infty} x^n$$

можно «свернуть», то есть (хотя бы при $|x| < 1$) верно равенство:

$$1 + x + x^2 \ldots = \sum_{k=0}^{\infty} x^n = \frac{1}{1-x}.$$

Поэтому говорят, что производящей функцией последовательности $1,1,1,\ldots$ является функция $\frac{1}{1-x}$.

Примеры:

Вспомним **формулу Тейлора**, которая обычно рассматривается в 1-м семестре курса математического анализа.

Если функция $f(x)$ имеет непрерывные производные до $(n+1)$-го порядка включительно в окрестности точки 0, то в этой окрестности имеет место равенство:

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \frac{f'''(0)}{3!}x^3 + \ldots + \frac{f^{(n)}(0)}{n!}x^n + R_n(x),$$

где $R_n(x)$ - остаточный член.

В частности, имеем следующие тейлоровские разложения:

$e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots + \frac{1}{n!}x^n + R_n(x)$;

$cos\, x = 1 - \frac{1}{2!}x^2 + \frac{1}{4!}x^3 + \ldots + R_n(x)$;

$sin\, x = x - \frac{1}{3!}x^3 + \ldots + R_n(x)$.

Причем во всех этих случаях $\forall x \;\; R_n(x) \to 0$ при $n \to \infty$. Поэтому можно считать, например, что

$$e^x = 1 + x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \ldots + \frac{1}{n!}x^n + \ldots = \sum_{k=0}^{\infty} \frac{1}{k!}x^k.$$

То есть e^x является производящей функцией последовательности

$$1, \frac{1}{2!}, \frac{1}{3!}, \ldots, \frac{1}{n!}, \ldots$$

Нас в комбинаторике больше интересуют целочисленные последовательности.

Определение. Рассмотрим (бесконечную) числовую последовательность $a_0, a_1, a_2, \ldots$ *Экспоненциальной производящей функцией* этой последовательности называется формальный *степенной ряд*:

$$\frac{a_0}{0!}x^0 + \frac{a_1}{1!}x^1 + \frac{a_2}{2!}x^2 \ldots = \sum_{n=0}^{\infty} \frac{a_n}{n!}x^n.$$

Теперь можно считать, что e^x является экспоненциальной производящей функцией последовательности $1,1,1,\ldots,1,\ldots$

Итак, с данной последовательностью можно связать формальный степенной ряд, который (часто) может быть «свернут» в функцию, которую и называют производящей функцией этой последовательности.

Поставим обратный вопрос. Пусть нам известна производящая функция некой последовательности. Как нам по этой функции построить саму последовательность? Во-первых, заметим, что, подставив значение $x = 0$ в ряд

$$f(x) = a_0 + a_1x^1 + a_2x^2 \ldots = \sum_{k=0}^{\infty} a_nx^n$$

получим $a_0 = f(0)$.

Во-вторых, если ряд почленно формально продифференцировать и затем подставить $x = 0$, получим

$$f'(x) = a_1 + 2a_2x \ldots = \sum_{n=1}^{\infty} na_nx^{n-1}$$

и $f'(0) = a_1$, $a_1 = f'(0)$.

Далее, если полученное равенство продифференцировать еще раз и подставить $x = 0$, получим

$$f''(x) = 2a_2 + 3 \cdot 2a_3x \ldots = \sum_{n=2}^{\infty} n(n-1)a_nx^{n-2}$$

и $f''(0) = 2a_2$, $a_2 = \frac{f''(0)}{2!}$ и так далее.

Таким образом, имеет место формула: $a_n = \frac{f^{(n)}(0)}{n!}$ для $n = 0,1,2,\ldots$

Последовательность Фибоначчи

Рассмотрим последовательность, в которой нулевой элемент равен 0, первый равен 1, и для которой выполнено рекуррентное соотношение:

$a_n = a_{n-1} + a_{n-2}$ для всех $n \geq 2$.

Запишем несколько ее элементов: $0,1,1,2,3,5,8,\ldots$

Предположим, что $F(x)$ - производящая функция этой последовательности, то есть $F(x) = \sum_{n=0}^{\infty} a_n x^n$.

Умножим обе части рекуррентного соотношения на x^n:

$a_n x^n = a_{n-1}x^n + a_{n-2}x^n$,

а затем просуммируем по всем значениям n от 2 до ∞. Получим

$$\sum_{n=2}^{\infty} a_n x^n = \sum_{n=2}^{\infty} a_{n-1}x^n + \sum_{n=2}^{\infty} a_{n-2}x^n.$$

$$\sum_{n=2}^{\infty} a_n x^n = x\sum_{n-1=1}^{\infty} a_{n-1}x^{n-1} + x^2\sum_{n-2=0}^{\infty} a_{n-2}x^{n-2}$$

$$F(x) - x = xF(x) + x^2F(x)$$

$$(x^2 + x - 1)F(x) = -x$$

$$F(x) = \frac{-x}{x^2+x-1}.$$

Обозначим корни многочлена $x^2 + x - 1 = 0$ через $x_1 = \frac{-1-\sqrt{5}}{2}$ и $x_2 = \frac{-1+\sqrt{5}}{2}$.

Представим

$$\frac{-x}{x^2+x-1} = \frac{A}{x-x_1} - \frac{B}{x-x_2}.$$

Умножив обе части равенства на знаменатель левой части и подставляя $x = x_1$ и $x = x_2$, найдем $A = \frac{x_1}{x_2-x_1}, B = \frac{-x_2}{x_2-x_1}$.

В итоге получим

$$F(x) = \frac{-x}{x^2+x-1} = \frac{1}{x_2-x_1}\left(\frac{x_1}{x-x_1} - \frac{x_2}{x-x_2}\right) =$$

$$= \frac{1}{\sqrt{5}}\left(\frac{1}{\frac{x}{x_1}-1} - \frac{1}{\frac{x}{x_2}-1}\right) = \frac{1}{\sqrt{5}}\left(\frac{1}{-xx_2-1} - \frac{1}{-xx_1-1}\right) = \frac{1}{\sqrt{5}}\left(\frac{1}{1+xx_1} - \frac{1}{1+xx_2}\right) =$$

$$= \frac{1}{\sqrt{5}}\left(\sum_{n=0}^{\infty}\big((-x_1)x\big)^n - \sum_{n=0}^{\infty}\big((-x_2)x\big)^n\right) =$$

$$= \frac{1}{\sqrt{5}}\sum_{n=0}^{\infty}((-x_1)^n - (-x_2)^n)x^n.$$

(Мы использовали то, что $x_1x_2 = -1$ и $x_2 - x_1 = \sqrt{5}$).

Мы вывели так называемую формулу Бине для n -го члена последовательности Фибоначчи:

$$a_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Эту формулу впервые получил де Муавр в 1730 году, используя изобретенный им же метод производящих функций, которым сейчас воспользовались и мы. Бине переоткрыл эту формулу на 100 лет позже. Леонардо Фибоначчи – ученый 12 века.

В написанном выражении можно видеть отношение золотого сечения, которое мы упоминали здесь ранее.

При больших n отношение соседних элементов последовательности Фибоначчи близко к отношению золотого сечения, поэтому эти отношения 5:3, 8:5 и т. д. использовали архитекторы в своих проектах как пропорции отвечающие требованию гармонии (мы это обнаружили в книге «Далекое близкое» великого художника И.Е. Репина).

Получим теперь формулу Бине для чисел Фибоначчи другим способом, но также используя производящую функцию последовательности Фибоначчи. Предварительно докажем важную теорему о вычислении производной высшего порядка для произведения нескольких функций.

Теорема (общее правило Лейбница). Пусть функция $F(x)$ является произведением n раз дифференцируемых в точке x функций:
$F(x) = u_1(x) \cdot u_2(x) \cdot \ldots \cdot u_k(x)$.

Тогда производная n -го порядка функции $F(x)$ равна:

$$F^{(n)}(x) = \sum_{\substack{n_1,\ldots,n_k \geq 0 \\ n_1+\ldots+n_k=n}} \frac{n!}{n_1! \cdot n_2! \cdot \ldots \cdot n_k!} u_1^{(n_1)}(x) \cdot u_2^{(n_2)}(x) \cdot \ldots \cdot u_k^{(n_k)}(x).$$

Доказательство. Заметим, сначала, что из правила для дифференцирования произведения двух функций легко вытекает правило дифференцирования произведения любого большего числа функций:

$$\left(v_1(x)\cdot v_2(x)\cdot \ldots \cdot v_k(x)\right)' = v_1'(x)\cdot v_2(x)\cdot \ldots \cdot v_k(x) + v_1(x)\cdot v_2'(x)\cdot \ldots \cdot v_k(x) + \ldots + v_1(x)\cdot v_2(x)\cdot \ldots \cdot v_k'(x).$$

(Это правило присутствует уже на первых страницах знаменитой книги маркиза де Лопиталя, вышедшей в свет в конце 17 века и являющейся исторически первым изложением только что созданных основ теории дифференциального исчисления. Именно с опорой на это правило де Лопиталь (да и мы так делаем обычно) доказывает, что $(x^n)' = n\cdot x^{n-1}$).

Таким образом, при каждом дифференцировании произведения, состоящего из k сомножителей, появляется сумма из k штук произведений, в которых ровно над одним из сомножителей появляется штрих.

После n дифференцирований исходной функции появится сумма из k^n произведений вида $u_1^{(n_1)}(x)\cdot u_2^{(n_2)}(x)\cdot \ldots \cdot u_k^{(n_k)}(x)$, где $n_1+\ldots+n_k = n$.

Здесь как обычно $u^{(m)}(x)$ обозначает производную m -го порядка, то есть штрих стоит m раз.

При этом в сумме будут присутствовать одинаковые выражения. Чтобы понять с какой кратностью они будут присутствовать, рассмотрим строку символов длины n, а символами будут служить $u_1(x),\ldots,u_k(x)$ (всего k типов символов), причем каждый символ $u_i(x)$ будет присутствовать в этой строке n_i раз, и $n_1+\ldots+n_k = n$.

Всего таких строк символов мы будем иметь $A(n_1,\ldots,n_k) = \frac{n!}{n_1!\cdot\ldots\cdot n_k!}$. Каждая такая строка будет описывать историю появления каждого произведения $u_1^{(n_1)}(x)\cdot u_2^{(n_2)}(x)\cdot \ldots \cdot u_k^{(n_k)}(x)$, присутствующего в рассматриваемой сумме.

Например, при $n = 4$ и $k = 3$, строка $(u_1(x), u_3(x), u_1(x), u_1(x))$ будет описывать появление произведения $u_1^{(3)}(x)\cdot u_2(x)\cdot u_3^{(1)}(x)$ и означает, что первый раз дифференцировали первый сомножитель, второй раз – третий, третий и четвертый раз опять первый сомножитель, второй сомножитель не дифференцировали ни разу, всего провели 4 дифференцирования.

Отсюда можно увидеть, что произведений вида $u_1^{(n_1)}(x)\cdot u_2^{(n_2)}(x)\cdot \ldots \cdot u_k^{(n_k)}(x)$ будет столько же, сколько различных строк с известными кратностями

символов, то есть $A(n_1,\ldots,n_k)=\frac{n!}{n_1!\cdot\ldots\cdot n_k!}$ штук.

Теорема доказана.

Следствие. Пусть функция $F(x)$ является произведением двух n раз дифференцируемых в точке x функций: $F(x)=u(x)\cdot v(x)$.

Тогда производная n -го порядка функции $F(x)$ равна:

$$F^{(n)}(x)=\sum_{m=0}^{n}\left(C_n^m\cdot u^{(m)}(x)\cdot v^{(n-m)}(x)\right).$$

Доказательство. Следствие, очевидно, является частным случаем рассмотренного общего правила Лейбница для $k=2$. Здесь учтено, что $C_n^m=\frac{n!}{m!\cdot(n-m)!}$.

По схеме рассмотренного доказательства общего правила Лейбница доказывается *мультиномиальная теорема*, являющаяся обобщением *биномиальной теоремы* (бинома Ньютона).

Теорема (мультиномиальная теорема)

$$(a_1+a_2+\ldots+a_k)^n=\sum_{\substack{n_1,\ldots,n_k\geq 0\\ n_1+\ldots+n_k=n}}\frac{n!}{n_1!\cdot n_2!\cdot\ldots\cdot n_k!}a_1^{n_1}\cdot a_2^{n_2}\cdot\ldots\cdot a_k^{n_k}.$$

Коэффициенты $A(n_1,\ldots,n_k)=\frac{n!}{n_1!\cdot\ldots\cdot n_k!}$, присутствующие в этой формуле, называют *мультиномиальными коэффициентами* (числа $C_n^m=\frac{n!}{m!\cdot(n-m)!}$, присутствующие в формуле степени бинома, как мы уже говорили, называют *биномиальными коэффициентами*).

Вернемся к числам Фибоначчи. Докажем теперь уже доказанную нами ранее формулу Бине (на самом деле формулу де Муавра) для чисел Фибоначчи другим способом, используя общее правило Лейбница.

Ранее мы доказали, что, если $F(x)$ - производящая функция последовательности $a_1, a_2, \ldots$, то ее n -й член будет равен $a_n=\frac{F^{(n)}(0)}{n!}$.

Для последовательности Фибоначчи $F(x)=\frac{-x}{x^2+x-1}$.

Учитывая, корни многочлена x^2+x-1 равные $x_1=\frac{-1-\sqrt{5}}{2}$ и $x_2=\frac{-1+\sqrt{5}}{2}$, производящую функцию можно записать в виде:

$F(x)=-x\cdot(x-x_1)^{-1}\cdot(x-x_2)^{-1}$.

Тогда, используя общее правило Лейбница, будем получать:

$$a_n = \frac{F^{(n)}(x)}{n!}\Big|_{x=0} =$$
$$= -\left(\frac{1}{n!}\sum_{i+j+k=n}\frac{n!}{i!\cdot j!\cdot k!}x^{(i)}((x-x_1)^{-1})^{(j)}((x-x_2)^{-1})^{(k)}\right)\Big|_{x=0} =$$
$$= -\left(\sum_{j+k=n-1}\frac{1}{j!\cdot k!}((x-x_1)^{-1})^{(j)}((x-x_2)^{-1})^{(k)}\right)\Big|_{x=0} =$$
$$= \sum_{j+k=n-1}\frac{1}{j!\cdot k!}(-1)^j j!\,(-x_1)^{-j-1}(-1)^k k!\,(-x_2)^{-k-1} =$$
$$= (-1)^n\sum_{j=0}^{n-1}x_2^{j+1}x_1^{n-j} =$$
$$= (-1)^n\sum_{j=0}^{n-1}(-1)^{j+1}(-x_2)^{j+1}(-1)^{n-j}(-x_1)^{n-j} =$$
$$= (-1)^{2n+1}\sum_{j=0}^{n-1}(-x_2)^{j+1}(-x_1)^{n-j} =$$
$$= (-1)(-x_2)(-x_1)\sum_{j=0}^{n-1}(-x_2)^j(-x_1)^{n-1-j} = \frac{(-x_1)^n-(-x_2)^n}{(-x_1)-(-x_2)} =$$
$$= \frac{1}{\frac{1+\sqrt{5}}{2}-\frac{1-\sqrt{5}}{2}}\cdot\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right) = \frac{1}{\sqrt{5}}\cdot\left(\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n\right).$$

Формула Бине доказана.

В процессе нашей выкладки мы отбросили слагаемые, соответствующие значениям $i \neq 1$, поскольку они зануляются. Кроме того, использована формула: $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \ldots + ab^{n-2} + b^{n-1})$.

Также постоянно использовалось равенство $x_1x_2 = -1$.

Последовательности, заданные линейными рекуррентным соотношениями с постоянными коэффициентами

Мы будем рассматривать числовые последовательности $a_0, a_1, \ldots$, для которых заданы первые d их членов, а также для всех $n \geq d$ выполнено рекуррентное соотношение: $a_n = c_1a_{n-1} + c_2a_{n-2} + \ldots + c_da_{n-d}$.

Такие последовательности будем называть *линейными рекуррентными последовательностями*.

Примером, нами уже рассмотренным, такой последовательности может служить последовательность Фибоначчи.

Проведя выкладку, подобную проведенной нами для последовательности Фибоначчи, можно легко получить производящую функцию и убедиться в том, что имеет место следующая теорема.

Теорема. Производящая функция линейной рекуррентной последовательности будет рациональной функцией: $F(x) = \frac{p(x)}{q(x)}$,

здесь $p(x)$ и $q(x)$ - многочлены.

Далее получить формулу для общего члена такой последовательности можно, разлагая рациональную дробь в сумму простейших (мы так сделали при первом выводе формулы Бине для последовательности Фибоначчи).

Существует общий подход к получению формулы общего члена рекуррентной линейной последовательности, основанный на получении корней так называемого характеристического уравнения:

$x^d - c_1 x^{d-1} - c_2 x^{d-2} - \ldots - c_d = 0.$

Мы не будем подробно сейчас рассматривать этот подход. Возникающая здесь теория параллельна теории линейных дифференциальных уравнений с постоянными коэффициентами.

Рассмотрим некоторые примеры линейных рекуррентных последовательностей.

Пример 1: *Геометрическая прогрессия* $a_0, a_0 q, a_0 q^2, \ldots$

Заданы a_0 и q. Рекуррентное соотношение: $a_n = q \cdot a_{n-1}$ для $n \geq 1$.

Производящая функция: $F(x) = \frac{a_0}{1-qx}$.

Формула n -го члена: $a_n = a_0 \cdot q^n$.

Пример 2: *Арифметическая прогрессия* $a_0, a_0 + r, a_0 + 2r, \ldots$

Заданы a_0 и r.

Рекуррентное соотношение: $a_n = a_{n-1} + r$ для $n \geq 1$ не является однородным, так как содержит в правой части постоянное число r.

Но, если из соотношения $a_n = a_{n-1} + r$ вычесть соотношение $a_{n-1} = a_{n-2} + r$, то получим $a_n - a_{n-1} = a_{n-1} - a_{n-2}$, и далее

$a_n = 2a_{n-1} - a_{n-2}$ для $n \geq 2$. Мы получили рекуррентное соотношение 2-го порядка с уже однородной правой частью.

Производящая функция: $F(x) = \frac{(2a_0 - a_1)x - a_0}{(x-1)^2}$.

Формула n -го члена: $a_n = a_0 + nr = a_0 + n(a_1 - a_0)$.

Пример 3: Последовательность чисел Фибоначчи мы много обсуждали выше.

Пример 4: *Последовательность чисел Люка.*

Как и для чисел Фибоначчи для чисел Люка выполнено то же рекуррентное соотношение $a_n = a_{n-1} + a_{n-2}$, но начальные значения другие:

$a_0 = 2, a_1 = 1.$

Производящая функция: $F(x) = \frac{x-2}{x^2+x-1}$.

Формула n -го члена: $a_n = \left(\frac{1+\sqrt{5}}{2}\right)^n + \left(\frac{1-\sqrt{5}}{2}\right)^n$.

Пример 5: *Последовательность чисел Перрена.*

Здесь $a_0 = 3, a_1 = 0, a_2 = 2$, и $a_n = a_{n-2} + a_{n-3}$ для $n \geq 3$.

Производящая функция: $F(x) = \frac{x^2-3}{x^3+x^2-1}$.

Формула n -го члена: $a_n = x_1^n + x_2^n + x_3^n$.

Здесь x_1, x_2, x_3 - корни многочлена $x^3 + x^2 - 1$, причем $x_1 = p$ (*пластическое число*) - действительный корень многочлена, а два других корня – это пара комплексно-сопряженных чисел. Пластическое число $p \approx 1.325$, а модули двух других корней меньше единицы, поэтому при больших n выполнено: $a_n \approx p^n$ (так же как для чисел Фибоначчи при больших n: $a_n \approx \frac{1}{\sqrt{5}}\varphi^n$, где ϕ - отношение золотого сечения).

Примеры 6 и 7:

Рассмотрим последовательность подходящих дробей к квадратному корню из двух: $\frac{1}{1}, \frac{3}{2}, \frac{7}{5}, \frac{17}{12}, \frac{41}{29}, \ldots$. Последовательность знаменателей этих дробей называется *последовательностью чисел Пелля*, а последовательность удвоенных числителей называется *последовательностью чисел Пелля-Люка*.

Для чисел Пелля имеет место рекуррентное соотношение:

$a_0 = 0, a_1 = 1$, и $a_n = 2a_{n-1} + a_{n-2}$ для $n \geq 2$.

Формула n -го члена: $a_n = \frac{1}{2\sqrt{2}}\left(\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n\right)$.

Здесь отношение *серебряного сечения* $\delta = 1 + \sqrt{2}$ играет ту же роль, что и отношение золотого сечения в формуле Бине для последовательности Фибоначчи.

Замечание. Отношение длин сторон ватманского листа, как и листов А2, А3, А4, равно $\sqrt{2}$, что и дает возможность делить эти листы пополам с сохранением пропорции.

Для чисел Пелля-Люка имеет место рекуррентное соотношение:

$a_0 = 2, a_1 = 2$, и $a_n = 2a_{n-1} + a_{n-2}$ для $n \geq 2$.

Формула n -го члена: $a_n = \left(1 + \sqrt{2}\right)^n + \left(1 - \sqrt{2}\right)^n$.

В качестве простого упражнения рекомендуем получить производящие функции для последовательностей чисел Пелля и чисел Пелля-Люка.

Пелль – британский ученый и деятель 17 века, его брат и его сын сыграли большую роль в образовании и становлении города Нью-Йорка, его прямые потомки являются современными государственными деятелями. Последовательность Пелля названа так Эйлером.

Люка – французский математик 19 века.

Производящие функции нескольких переменных

Рассмотрим двумерный счетный набор чисел a_n^k, $n = 0,1,2,\ldots, k = 0,1,2,\ldots$.

Производящей функцией этого набора называется формальный степенной ряд

$$\sum_{n=0}^{\infty}\sum_{k=0}^{\infty} a_n^k x^k y^n.$$

Если этот ряд удается свернуть в функцию двух переменных $F(x, y)$, то эту функцию называют производящей функцией.

Получим для примера производящую функцию для чисел сочетаний с повторениями (табл. 10).

Таблица 10

n \ k	0	1	2	3	4	5	6	7	…
0	1	0	0	0	0				
1	1	1	1	1	1				
2	1	2	3	4					
3	1	3	6	10					
4	1	4	10	20					
5	1								
6	1								
7	1								
…									

Мы имеем рекуррентное соотношение: $\overline{C}_n^k = \overline{C}_{n-1}^k + \overline{C}_n^{k-1}$.

Умножим правую и левую части этого равенства на $x^k y^n$ и просуммируем, считая, что n и k меняются от 1 до ∞:

$$\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_n^k x^k y^n = \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_{n-1}^k x^k y^n + \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_n^{k-1} x^k y^n$$

$$\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_n^k x^k y^n = y\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_{n-1}^k x^k y^{n-1} + x\sum_{n=1}^{\infty}\sum_{k=1}^{\infty} \overline{C}_n^{k-1} x^{k-1} y^n$$

$$- \sum_{n=0}^{\infty} \overline{C}_n^0 x^0 y^n - \sum_{k=1}^{\infty} \overline{C}_0^k x^k y^0 + F =$$

$$= y(-\sum_{n=0}^{\infty} \overline{C}_n^0 x^0 y^n + F) + x(-1 + F)$$

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

$$-\frac{1}{1-y} + F = y(-\frac{1}{1-y} + F) + x(-1 + F)$$

$$F - yF - xF = \frac{1}{1-y} - \frac{y}{1-y} - x$$

$$F = \frac{1-x}{1-x-y}.$$

Рассуждая подобным образом, можно получить производящую функцию двух переменных для биномиальных коэффициентов C_n^k: $F(x,y) = \frac{1}{1-y-xy}$.

Аналогично доказанному ранее утверждению для одномерного случая доказывается следующее утверждение.

Утверждение. Если $F(x,y)$ - производящая функция набора a_n^k, то для любой пары чисел $n = 0,1,2,\ldots$ и $k = 0,1,2,\ldots$ имеет место равенство:

$$a_n^k = \frac{1}{n! \cdot k!} \cdot \frac{\partial^{n+k} F}{\partial x^k \partial y^n}\bigg|_{\substack{x=0 \\ y=0}}.$$

Асимптотические оценки. Формула Стирлинга

Во многих комбинаторных выражениях мы видим функцию $n!$.

Это быстро растущая функция, но сравнение ее по скорости роста с другими функциями натурального аргумента затруднительно.

Познакомимся с асимптотической формулой Стирлинга, которая очень часто используется в асимптотических оценках.

Теорема (формула Стирлинга). $n! \simeq \sqrt{2\pi} \cdot \sqrt{n} \cdot \left(\frac{n}{e}\right)^n$.

Относительная погрешность этого равенства стремится к нулю при $n \to \infty$, отношение правой части к левой стремится к 1 при $n \to \infty$.

Но и при малых значениях n формула Стирлинга дает хорошую точность оценки факториала.

Производящие функции (продолжение)

Определение. Рассмотрим две (бесконечные) числовые последовательности (a_n) и (b_n).

Сверткой этих последовательностей называется последовательность (c_n), элементы которой вычисляются по формуле:

$$c_n = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0 = \sum_{k=0}^{n} a_k b_{n-k}.$$

Определение. Под формальным произведением формальных степенных рядов $\sum_{n=0}^{\infty} a_n x^n$ и $\sum_{n=0}^{\infty} b_n x^n$ понимается степенной ряд

$$\sum_{n=0}^{\infty} c_n x^n,$$

где $c_n = \sum_{k=0}^{n} a_k b_{n-k}$.

В случае, когда в рядах $\sum_{n=0}^{\infty} a_n x^n$ и $\sum_{n=0}^{\infty} b_n x^n$ лишь конечное число слагаемых отличны от нуля, это определение согласуется с обычным умножением многочленов.

Утверждение. Если $f_1(x)$ и $f_2(x)$ это, соответственно, производящие функции последовательностей (a_n)и (b_n), то производящая функция $f(x)$ свертки (c_n)этих последовательностей ровна произведению функций $f_1(x)$ и $f_2(x)$.

Доказательство очевидно вытекает из предыдущего определения.

Рассмотрим пример применения введенных понятий.

Пример: В коробочке находится 4 желтых шарика и 5 зеленых. Шарики

одного цвета неразличимы. Сколько способов набрать из коробочки 7 шариков?

Решение. Рассмотрим последовательность (a_n), где a_n - число способов взять из коробочки n желтых шариков. Поскольку шарики одного цвета неразличимы, то $a_0 = 1, a_1 = 1, a_2 = 1, a_3 = 1, a_4 = 1$ и $a_n = 0$ при $n > 4$.

Поэтому производящая функция этой последовательности будет равна

$f_1(x) = 1 + x + x^2 + x^3 + x^4$.

Рассуждая аналогично, получим производящую функцию для числа способов взять n зеленых шариков:

$f_2(x) = 1 + x + x^2 + x^3 + x^4 + x^5$.

В таком случае производящая функция для числа способов взять n шариков из коробки будет равна:

$f(x) = (1 + x + x^2 + x^3 + x^4) \cdot (1 + x + x^2 + x^3 + x^4 + x^5)$.

Поэтому ответом на поставленный в задаче вопрос будет коэффициент при x^7 в многочлене $f(x)$ после открытия скобок и приведения подобных.

Поскольку 7= 2+5=3+4=4+3. Ответом будет число 3.

Рассмотрим еще один пример.

Пример: В коробочке находится 4 желтых шарика и 5 синих и 3 зеленых. Шарики одного цвета неразличимы. Сколько способов набрать из коробочки 7 шариков, если нужно взять нечетное число желтых, четное число синих и не меньше одного зеленого?

Решение. Ответом на поставленный в задаче вопрос будет коэффициент при x^7в многочлене $f(x) = (x + x^3)(1 + x^2 + x^4)(x + x^2 + x^3)$ после открытия скобок и приведения подобных.

Поскольку 7=1+4+2=3+2+2, то ответом будет число 2.

Производящая функция чисел Каталана

Используем понятие свертки для получения производящей функции чисел Каталана, которые мы рассматривали ранее.

Заметим, во-первых, что числа Каталана удовлетворяют следующему рекуррентному соотношению:

$$K_{n+1} = \sum_{i=0}^{n} K_i K_{n-i}.$$

Чтобы это доказать можно заметить, что каждое слово фон Дика w может

быть единственным образом записано в виде $w = Xw_1Yw_2$ с (может быть пустыми) словами фон Дика w_1 и w_2.

Далее, отметим, что $K_0 = 1$.

Умножим приведенное соотношение на x^{n+1} и просуммируем от $n = 0$ до ∞, получаем

$$\sum_{n+1=1}^{\infty} K_{n+1}x^{n+1} = x\sum_{n=0}^{\infty}\left(\sum_{i=0}^{n} K_iK_{n-i}\right)x^n.$$

Обозначим через $F(x)$ производящую функцию последовательности чисел Каталана.

Мы получили соотношение: $F(x) - K_0 = x(F(x))^2$ (здесь учтено, что в правой части у нас записана свертка двух экземпляров последовательности Каталана).

Имеем квадратное уравнение относительно производящей функции последовательности чисел Каталана:

$x(F(x))^2 - F(x) + 1 = 0.$

Решая квадратное уравнение, получим $F(x) = \frac{1-\sqrt{1-4x}}{2x}$.

(Берем радикал с минусом, чтобы выполнялось условие $\lim\limits_{x\to 0} F(x) = 1$).

Найденная производящая функция может быть использована для получения формулы $K_n = C_{2n}^n - C_{2n}^{n-1} = \frac{1}{n+1}C_{2n}^n$.

Но мы ее уже изящно получили ранее, используя обобщение чисел Каталана и двумерную индукцию, а также проведя прямое комбинаторное рассуждение.

2.5. Формула включения-исключения

Мы приступаем к рассмотрению не чисто комбинаторного вопроса, но вопроса, связанного с теорией меры и имеющего смыслы в других разделах математики, например, в алгебре, геометрии многомерного куба и пр.

С аналогом этой формулы вы встретитесь в курсе теории вероятностей, когда будете рассматривать теорему сложения.

Введем несколько предварительных определений. Здесь мы будем следовать своему пути, и будем использовать некоторые свои термины для вводимых новых понятий.

Определение (А.Н. Выборнов). *Слоеным множеством*, мы назовем

множество, каждому элементу которого приписана *кратность*. Кратность – это целое число. Для конечного множества слоеное множество – это расширение понятия *мультимножества*, но в слоеном множестве кратность может быть отрицательным числом.

Обычные множества при необходимости мы будем трактовать как слоеные множества с кратностями всех элементов равными единице.

Определение (А.Н. Выборнов). Введем операции над слоеными множествами.

1) *Сложение.*

Рассмотрим два слоеных множества A и B. Их *суммой* $A + B$ мы назовем слоеное множество, которое будет состоять из элементов объединения $A \cup B$, при этом элементы симметрической разности $A \triangle B$ сохранят свою кратность, а кратность каждого элемента, лежащего в пересечении $A \cap B$, будет равна сумме его кратности в слоеном множестве A и его кратности в слоеном множестве B (рис. 2.4).

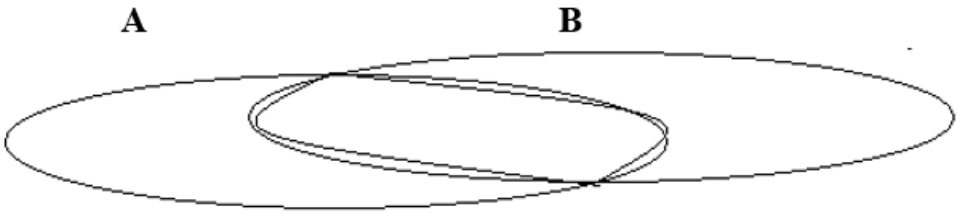


Рисунок 2.4

2) *Умножение.*

Рассмотрим два слоеных множества A и B. Их *произведением* $A \cdot B$ мы назовем слоеное множество, которое будет состоять из элементов пересечения $A \cap B$, и кратность каждого элемента, лежащего в пересечении $A \cap B$, будет равна произведению его кратности в слоеном множестве A и его кратности в слоеном множестве B.

3) *Одноместный минус.*

Рассмотрим слоеное множество A. Слоеное множество $-A$ состоит из элементов множества A, но с противоположной кратностью.

4) *Разность.*

Разность $A - B$ определяется как сумма $A - B = A + (-B)$, при этом множеством элементов этого слоеного множества мы считаем множество $A \cup B$.

Легко проверяется следующее утверждение.

Утверждение

1) $-(-A) = A$;

2) $(-A) \cdot B = -(A \cdot B)$;

3) $-(A + B) = (-A) + (-B)$;

4) $(A + B) \cdot C = AC + BC$.

Определение (А.Н. Выборнов). Рассмотрим *конечное* слоеное множество A.

Мерой $\mu(A)$ назовем сумму кратностей всех элементов множества A.

Очевидно, что если обычное конечное множество трактовать как слоеное множество с кратностью всех элементов, равной единице, то его мера будет совпадать с его мощностью, то есть с количеством элементов этого конечного множества: $\mu(A) = |A|$.

Легко проверяется следующее утверждение.

Утверждение

1) $\mu(-A) = -\mu(A)$;

2) $\mu(A + B) = \mu(A) + \mu(B)$;

3) $\mu(A - B) = \mu(A) - \mu(B)$.

Теорема (формула включения-исключения)

1) Рассмотрим конечное универсальное множество U и его любые подмножества A и B. Имеет место формула

$$|U \backslash (A \cup B)| = |U| - |A| - |B| + |A \cap B|;$$

2) Рассмотрим конечное универсальное множество U и его любые подмножества A, B и C. Имеет место формула

$$|U \backslash (A \cup B \cup C)| =$$
$$= |U| - |A| - |B| - |C| + |A \cap B| + |A \cap C| + |B \cap C| - |A \cap B \cap C|;$$

3) Рассмотрим конечное универсальное множество U и его любые подмножества A, B, Cи D. Имеет место формула

$$|U \backslash (A \cup B \cup C \cup D)| = |U| - |A| - |B| - |C| - |D| +$$
$$+|A \cap B| + |A \cap C| + |A \cap D| + |B \cap C| + |B \cap D| + |C \cap D| -$$
$$-|A \cap B \cap C| - |A \cap B \cap D| - |A \cap C \cap D| - |B \cap C \cap D| +$$
$$+|A \cap B \cap C \cap D|;$$

4) Рассмотрим конечное универсальное множество U и его любые подмножества A_i, $i = 1, \ldots, n$,. Имеет место формула

$$\left|U\backslash\bigcup_{i=1}^{n}A_i\right| = |U| - \sum_{i=1}^{n}|A_i| + \sum_{i_1<i_2}\left|A_{i_1}\cap A_{i_2}\right| - \sum_{i_1<i_2<i_3}\left|A_{i_1}\cap A_{i_2}\cap A_{i_3}\right| +$$
$$+\ldots+(-1)^n|A_1\cap A_2\cap\ldots\cap A_n|.$$

Доказательство

1) Используя тождество де Моргана, можно записать:

$$U\backslash(A\cup B) = (U\backslash A)\cap(U\backslash B).$$

Будем теперь трактовать универсальное множество U и его подмножества A и B как слоеные множества с кратностями элементов равными единице, а в конце выкладки снова как обычные множества.

Тогда

$$|(U\backslash A)\cap(U\backslash B)| = \mu\big((U-A)\cdot(U-B)\big) =$$
$$= \mu(U\cdot U - U\cdot A - U\cdot B + A\cdot B) = \mu(U - A - B + A\cdot B) =$$
$$= \mu(U) - \mu(A) - \mu(B) + \mu(A\cdot B) = |U| - |A| - |B| + |A\cap B|.$$

Пункты 2) ,3) и 4) проверяются аналогично.

Следствие (тоже формула включения-исключения)

1) Рассмотрим конечные множества A и B. Имеет место формула

$$|A\cup B| = |A| + |B| - |A\cap B|;$$

2) Рассмотрим конечные множества A, B и C. Имеет место формула

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

3) Рассмотрим конечные множества A, B, C и D. Имеет место формула

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

4) Рассмотрим любые конечные множества A_i, $i = 1,\ldots,n$,.

Имеет место формула

$$\left|\bigcup_{i=1}^{n}A_i\right| = \sum_{i=1}^{n}|A_i| - \sum_{i_1<i_2}\left|A_{i_1}\cap A_{i_2}\right| + \sum_{i_1<i_2<i_3}\left|A_{i_1}\cap A_{i_2}\cap A_{i_3}\right| -$$
$$-\ldots+(-1)^{n-1}|A_1\cap A_2\cap\ldots\cap A_n|.$$

Доказательство. Для любого подмножества M конечного универсального множества U очевидно имеет место равенство: $|U\backslash M| = |U| - |M|$.

Теперь следствие немедленно вытекает из рассмотренной теоремы.

Замечание. Формулы, аналогичные рассмотренным в теореме и следствии, имеют место и для бесконечных множеств, только вместо мощности множеств нужно рассматривать конечно-аддитивную меру, такую как площадь, объем или вероятность (вероятностная мера). Доказательство будет по существу повторять только что нами проведенное.

Пример:

Определим, сколько натуральных чисел не больших 100 не делятся ни на 6, ни на 15, ни на 10.

Пусть U - множество всех натуральных чисел не больших 100, $|U| = 100$.

Обозначим:

$M6$ - множество всех натуральных чисел не больших 100, которые делятся на 6,

$M15$ - множество всех натуральных чисел не больших 100, которые делятся на 15,

$M10$ - множество всех натуральных чисел не больших 100, которые делятся на 10.

$$|M6| = \left[\frac{100}{6}\right] = 16, \quad |M15| = \left[\frac{100}{15}\right] = 6, \quad |M10| = \left[\frac{100}{10}\right] = 10,$$

$$|M6 \cap M15| = \left[\frac{100}{30}\right] = 3, \quad |M6 \cap M10| = \left[\frac{100}{30}\right] = 3,$$

$$|M10 \cap M15| = \left[\frac{100}{30}\right] = 3, \quad |M6 \cap M15 \cap M10| = \left[\frac{100}{30}\right] = 3.$$

Используя пункт 2) рассмотренной теоремы получим:

$$|U \setminus (M6 \cup M15 \cup M10)| = |U| - |M6| - |M15| - |M10| +$$
$$+|M6 \cap M15| + |M6 \cap M10| + |M15 \cap M10| - |M6 \cap M15 \cap M10| =$$
$$= 100 - 16 - 6 - 10 + 3 + 3 + 3 - 3 = 74.$$

Задача о беспорядках

Определение. Перестановку из чисел $1,2,\ldots,n$, в которой никакое число i не стоит на i -м месте, назовем *беспорядком*.

Число различных беспорядков длины n обозначим $Б_n$.

Теорема. Имеет место формула:

$$Б_n = n!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \ldots + (-1)^n \frac{1}{n!}\right).$$

Доказательство

Обозначим U - множество всех перестановок длины n, $|U| = n!$.

Далее обозначим A_i - множество всех перестановок, в которых число i стоит на i -м месте.

$|A_i| = (n-1)!$

Заметим далее, что $\left|A_{i_1} \cap A_{i_2} \cap \ldots \cap A_{i_k}\right| = (n-k)!$, и всего таких пересечений k множеств будет $C_n^k = \frac{n!}{(n-k)!\cdot k!}$.

Поэтому число перестановок, в которых никакое число i не стоит на i -м месте будет равно

$$\left|U \setminus \bigcup_{i=1}^{n} A_i\right| = |U| - \sum_{i=1}^{n}|A_i| + \sum_{i_1<i_2}\left|A_{i_1} \cap A_{i_2}\right| - \sum_{i_1<i_2<i_3}\left|A_{i_1} \cap A_{i_2} \cap A_{i_3}\right| +$$

$$+ \cdots + (-1)^n|A_1 \cap A_2 \cap \ldots \cap A_n| = n! - \frac{n!}{(n-1)!\cdot 1!}\cdot(n-1)! +$$

$$+\frac{n!}{(n-2)!\cdot 2!}\cdot(n-2)! - \frac{n!}{(n-3)!\cdot 3!}\cdot(n-3)! + \cdots +$$

$$+(-1)^n\frac{n!}{(n-n)!\cdot n!}\cdot(n-n)! = n!\left(\frac{1}{0!} - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \frac{1}{4!} - \cdots + (-1)^n\frac{1}{n!}\right).$$

Теорема доказана.

Если мы вспомним тейлоровское разложение функции e^x:

$e^x = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 \ldots$

и подставим в него $x = -1$, то получим:

$e^{-1} = 1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \ldots = \frac{1}{2!} - \frac{1}{3!} + \ldots$

Теперь мы видим, что в скобках выражения для числа беспорядков находится начальный отрезок ряда разложения e^{-1}.

Если разделить число беспорядков на $n!$, мы найдем вероятность того, что в случайно выбранной перестановке ни одно число не будет стоять на своем месте. И вероятность эта будет приближенно равна $e^{-1} \approx 0.37$.

Уже при $n = 10$ погрешность будет меньше $\frac{1}{1000000}$.

Используя формулу включения-исключения, докажем следующую формулу для чисел Стирлинга 2-го рода.

Утверждение

$$S_n^k = \frac{1}{k!}\sum_{i=0}^{k-1}(-1)^i\, C_k^i (k-i)^n =$$

$$= \frac{1}{k!}\left(k^n - C_k^1(k-1)^n + C_k^2(k-2)^n - \ldots + C_k^{k-1}(-1)^{k-1}\right).$$

Доказательство. Число $S_n^k \cdot k!$ может трактоваться, как число способов разбить n - элементное множество на k непустых частей с учетом порядка перечисления частей.

Обозначим через U - множество всех разбиений n - элементного множество на k (может быть и пустых) частей с учетом порядка перечисления частей. Таких разбиений будет k^n штук, поскольку каждый элемент разбиваемого множества может оказаться в любой из k частей, то есть $|U| = k^n$.

Обозначим через A_l - множество всех разбиений, в которых число l-ая часть пустая, $|A_l| = (k-1)^n$.

Для мощностей пересечений, очевидно, имеют место равенства:

$\left|A_{l_1} \cap A_{l_2} \cap \ldots \cap A_{l_i}\right| = (k-i)^n$.

Наборов $\{l_1, l_2, \ldots, l_i\}$ имеется C_k^i штук.

Используя формулу включения-исключения, будем иметь:

$$\left|U \setminus \bigcup_{l=1}^{n} A_l\right| = |U| - \sum_{l=1}^{n}|A_l| + \sum_{l_1<l_2}\left|A_{l_1} \cap A_{l_2}\right| - \sum_{l_1<l_2<l_3}\left|A_{l_1} \cap A_{l_2} \cap A_{l_3}\right| +$$

$$+\ldots+(-1)^n|A_1 \cap A_2 \cap \ldots \cap A_n| =$$

$$= k^n - C_k^1 \cdot (k-1)^n + C_k^2 \cdot (k-2)^n - C_k^3 \cdot (k-3)^n +$$

$$+\ldots+(-1)^n C_k^{k-1} \cdot (k-(k-1))^n = \sum_{i=0}^{k-1}(-1)^i C_k^i \cdot (k-i)^n.$$

Поэтому

$$k! \cdot S_n^k = \sum_{i=0}^{k-1}(-1)^i C_k^i \cdot (k-i)^n$$

$$S_n^k = \frac{1}{k!}\sum_{i=0}^{k-1}(-1)^i C_k^i \cdot (k-i)^n\,.$$

Доказанная формула может быть использована для вычисления чисел

Стирлинга 2-го рода, но она не дает нам более быстрого и удобного способа по сравнению с использованием двумерных рекуррентных соотношений.

2.6. Теория Пойа

Напомним некоторые понятия, которые мы рассматривали ранее.

Определение. Рассмотрим две группы G_1 и G_2. Отображение $f: G_1 \to G_2$, называется *гомоморфизмом* групп, если $\forall a_2, a_2 \in G_1$

$$f(a_1 \cdot a_2) = f(a_1) \bullet f(a_2).$$

(Здесь $\cdot$ - это групповая операция в группе G_1, а $\bullet$ - это групповая операция в группе G_2).

Определение. Группа G *действует* на множестве X, если задан гомоморфизм $\Phi: G \to S(X)$.

Применяется обозначение: $(\Phi(g))(x) = gx$. Группу G называют *группой преобразований*, а ее элементы *преобразованиями*.

Определение. Подмножество $Gx = \{gx: g \in G\} \subseteq X$ называется *орбитой* элемента $x \in X$.

Определение. Элемент $x \in X$ называется *стационарной точкой* для элемента $g \in G$, если $gx = x$.

Обозначим X_g - множество стационарных для g точек.

Лемма Бернсайда (лемма Коши – Фробениуса). Число орбит k при действии конечной группы G на конечном множестве точек X равно среднему по группе числу стационарных точек множества X:

$$k = \frac{\sum_{g \in G} |X_g|}{|G|}.$$

Доказательство леммы Бернсайда проведено нами ранее в этом курсе.

Рассмотрим теперь следующую задачу. Пусть каждая вершина равностороннего треугольника покрашена в один из 2-х цветов: черный и белый. Нужно определить число различных раскрасок.

Если мы ставим этот вопрос для закрепленного треугольника, у которого мы различаем вершины, то ответом, очевидно, будет число $2^3 = 8$ (рис. 2.5).

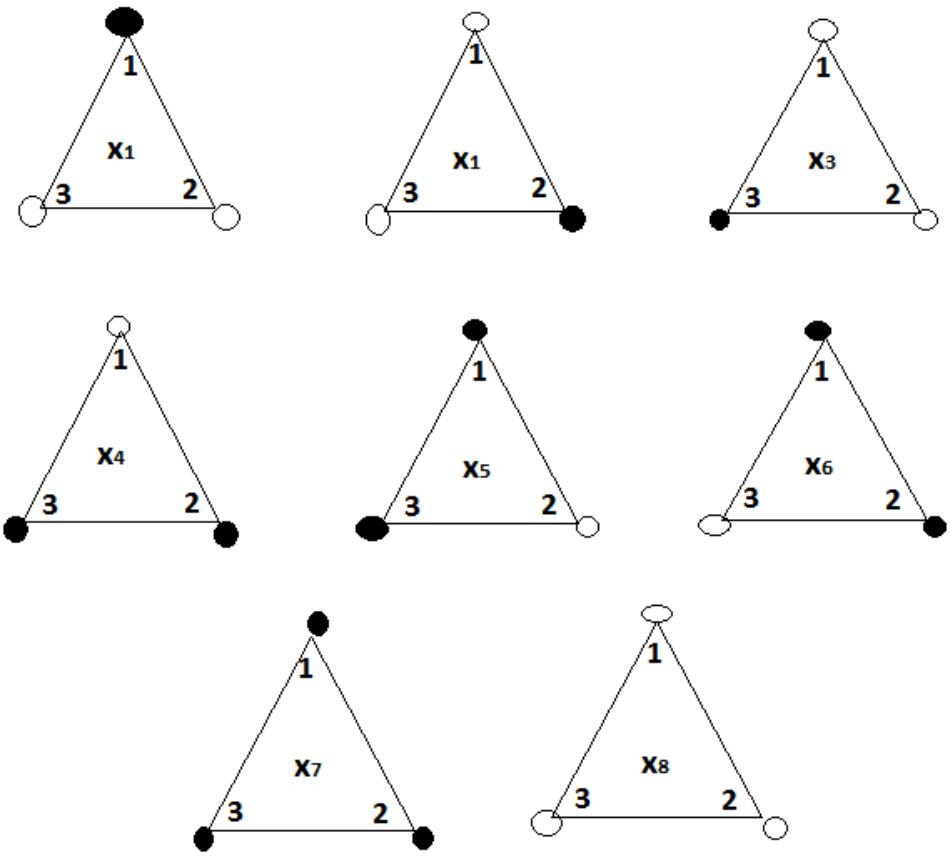


Рисунок 2.5

Но, если мы не будем различать вершины, то есть будем считать, что покрашены углы треугольной пластина, которую мы можем как угодно поворачивать и переворачивать, прежде чем положить на место, то различные раскраски могут совместиться. Совместимые раскраски мы теперь считаем одинаковыми. Множество всех закрепленных раскрашенных треугольников разбивается на классы эквивалентности: в каждом классе находятся треугольники с совместимыми окрасками. Задача теперь состоит в определении числа этих классов эквивалентности.

Для решения этой задачи рассмотрим группу движений, действующую на множестве $X = \{x_1, x_2, \ldots, x_8\}$ всех закрепленных раскрашенных треугольников. Очевидно, что орбиты при действии этой группы будут состоять из треугольников с совместимыми окрасками. То есть орбиты и будут этими классами эквивалентности. Задача свелась к определению числа орбит.

Группа движений треугольника в данном случае совпадает с симметрической группой S_3 всех перестановок длины 3. Каждому движению нашего треугольника соответствует некоторая перестановка его вершин (которые мы перенумеровали цифрами 1, 2, 3).

Перечислим все элементы этой группы, сразу представляя перестановки разложенными в произведение циклов. Циклы длины 1 здесь будем выписывать:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = (1)(2)(3)$$

$$g_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (1)(23)$$

$$g_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (2)(13)$$

$$g_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 2 \end{pmatrix} = (3)(12)$$

$$g_4 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123)$$

$$g_5 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132).$$

Далее заметим, что раскраска будет стационарной для данной подстановки только тогда, когда все вершины, соответствующие каждому циклу в разложении подстановки, покрашены одним цветом. Поэтому количество стационарных раскрасок, соответствующих данному элементу группы (данной подстановке) равно 2^m, где m - число циклов в подстановке, 2 – число цветов, используемых в раскраске.

Получаем:

$$X_e = 2^3, X_{g_1} = 2^2, X_{g_2} = 2^2, X_{g_3} = 2^2, X_{g_4} = 2, X_{g_5} = 2.$$

Далее, используя лемму Бернсайда, находим искомое число орбит, то есть число различных раскрасок:

$$k = \frac{\sum_{g \in S_3} |X_g|}{|S_3|} = \frac{2^3 + 3 \cdot 2^2 + 2 \cdot 2}{6} = 4.$$

Определение. Цикловой индекс действия группы подстановок на множестве X определяется формулой

$$Z_G(c_1, \ldots, c_n) = \frac{\sum_{g \in G} c_1^{j_1} \cdot \ldots \cdot c_n^{j_n}}{n}.$$

где в разложении подстановки g присутствует j_i циклов длины i; n - порядок группы G.

Для рассматриваемой задачи цикловой индекс будет таким:

$$Z_G(c_1, c_2, c_3) = \frac{c_1^3 + 3c_1c_2 + 2c_3}{6}.$$

Таким образом, чтобы найти число различных раскрасок нужно в цикловой индекс вместо переменных c_i подставить число различных цветов, в

рассматриваемом случае - число 2.

Цикловой индекс позволяет находить число раскрасок, в которых каждый из цветов присутствует определенное число раз (соответственно, p и q раз). Для этого нужно подставить вместо каждой переменной c_i выражение $\left(b^i + w^i\right)$. После чего привести получившийся многочлен двух переменных к сумме произведений степеней переменных. Получившийся коэффициент при $b^p w^q$ и будет нужным числом.

Например, если нас интересует число окрашенных треугольников, в которых 2 черных угла и один белый, мы составляем многочлен двух переменных:

$$\frac{(b+w)^3 + 3(b+w)(b^2+w^2) + 2(b^3+w^3)}{6} =$$

$$= \frac{6b^3 + 6b^2w + 6bw^2 + 6w^3}{6} = b^3 + b^2w + bw^2 + w^3.$$

Мы видим, что коэффициент при b^2w будет равен 1, то есть только одна раскраска нужного вида.

Замечание. Заметим, что рассмотренную задачу определения числа различных раскрасок вершин треугольника мы могли бы решить значительно быстрее, применяя формулу для числа сочетаний с повторениями. У нас есть два типа краски – нам нужно набрать три окрашенные вершины. Ответ: $\overline{C}_2^3 = \frac{2 \cdot 3 \cdot 4}{1 \cdot 2 \cdot 3} = 4$. Но рассмотренная нами в этом примере теория Д. Пойа, позволяет разобраться со случаями, в которых такой простой подход неприменим.

Рассмотрим еще один пример. Пусть каждая вершина тетраэдра раскрашена в один из четырех цветов. Нужно определить число различных раскрасок, с учетом того, что тетраэдр можно поворачивать в пространстве совмещая его с самим собой.

Для решения этого вопроса нам нужно построить цикловой индекс группы самосовмещающих поворотов (рис. 2.6).

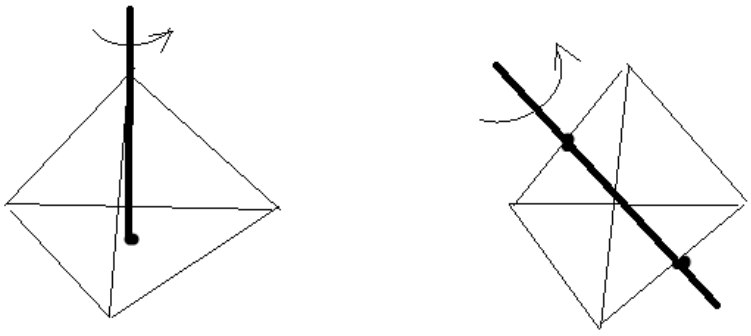


Рисунок 2.6

В группе поворотов имеется по два нетождественных поворота вокруг осей, проходящих через вершину тетраэдра и центр противоположной грани, и 4 варианта расположения осей поворота – всего 8 поворотов. Каждый такой поворот оставляет на месте одну вершину (цикл длины 1) и три остальных вершины циклически переставляются (цикл длины 3). Вклад в цикловой индекс у каждого такого поворота: $c_1 c_3$.

Кроме того, есть еще повороты вокруг осей, проходящих через середины противоположных ребер. Имеется три варианта такого расположения оси поворота. Каждый такой самосовмещающий поворот переставляет местами концы двух ребер, через которые проходит ось поворота (произведение 2-х циклов длины 2). Вклад в цикловой индекс у каждого такого поворота: c_2^2.

И, наконец, есть еще единичный элемент группы поворотов, оставляющий все вершины на месте (произведение четырех циклов длины 1). Вклад в цикловой индекс: c_1^4.

Итак, цикловой индекс действия этой группы:

$$Z_G(c_1, c_2, c_3) = \frac{c_1^4 + 8c_1c_3 + 3c_2^2}{12}$$

Отсюда получаем, что число различных раскрасок 4-мя цветами вершин тетраэдра будет равно: $\frac{4^4+8\cdot4\cdot4+3\cdot4^2}{12} = 36$.

Если бы пытались (неверно) решить рассматриваемую задачу другим способом, снабжая каждую из вершин тетраэдра цветом одного из 4-х типов, то используя число сочетаний с повторениями, мы бы получили: $\overline{C}_4^4 = \frac{4\cdot5\cdot6\cdot7}{1\cdot2\cdot3\cdot4} = 35$.

Разница в ответах вызвана тем, что существует два, несовместимых с помощью поворота варианта окраски вершин всеми 4-мя цветами (рис. 2.7).

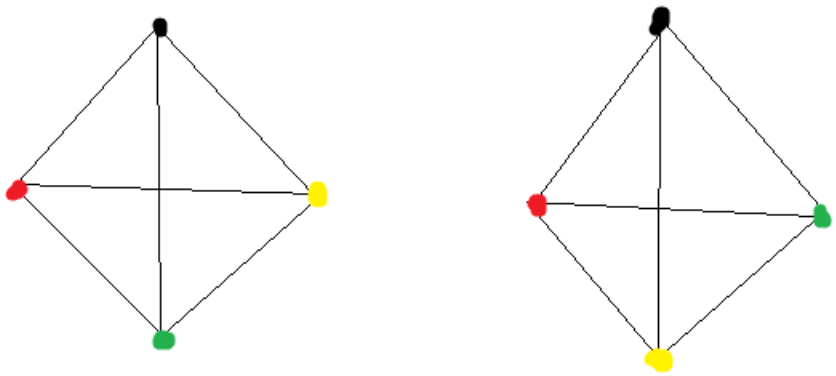


Рисунок 2.7

Получившиеся окрашенные тетраэдры имеют разную *хиральность* (комплексы вершин одинаковы по структуре, но имеют разное пространственное расположение). Понятие хиральности используется в химии при рассмотрении пространственного расположения частей, составляющих молекулу органического соединения.

Сам Д. Пойа указывал на возможность применения своей теории для перечисления химических соединений и их изомеров. С 30-х годов 20-го века и по настоящее время теория Пойа активно используется в химии.

Теория Пойа допускает следующую расширенную трактовку.

Давайте обратимся к рассмотренному нами ранее вопросу о подсчете количества классов эквивалентности комбинаторных отображений (12 сценариев, размещение шариков по коробкам).

Там мы рассматривали два множества A и B. Пусть $|A| = n$ и $|B| = k$. Далее мы рассматривали функции $f: A \to B$. Далее мы вводили различные отношения эквивалентности на множестве таких функций и вычисляли число получившихся классов эквивалентности. Мы различали случаи, когда элементы множеств A или B различимы или неразличимы (4 случая), а также когда функция f будет произвольной функцией, будет инъекцией, или будет сюръекцией (3 случая). Всего получалось $4 \cdot 3 = 12$ случаев.

Сейчас нас будут интересовать 2 из этих 12-ти случаев: когда f - произвольная функция, элементы множества B различимы, а элементы множества A различимы или неразличимы.

Рассматриваемые задачи можно интерпретировать как размещения различимых или неразличимых шариков (множество A) по различимым или неразличимым коробкам (множество B). Итак, в двух, интересующих нас сейчас, случаях мы размещаем различимые или неразличимые шарики по различимым

коробкам.

В случае неразличимости элементов множества A две функции $f_1: A \to B$ и $f_2: A \to B$ мы считаем эквивалентными, если некоторой перестановкой элементов множества A одна функция может быть переведена в другую. Точнее говоря, существует такая биекция $\sigma: A \to A$, что $f_2 = \sigma \circ f_1$, то есть $\forall a \in A$ выполнено $f_2(a) = f_1(\sigma(a))$. Рассматриваемая биекция $\sigma: A \to A$ - это, по сути, перестановка длины n.

Мы можем трактовать случай с неразличимыми шариками как то, что σ - это произвольный элемент симметрической группы S_n. В этом случае мы считаем, что на множестве шариков A действует группа всех перестановок S_n (мы не различаем шарики – любой может перейти в любой), мы красим шарики k цветами (размещаем по k коробкам). Мы определяем далее число различных раскрасок (размещений шариков по коробкам) и имеем ответ: $\overline{C}_k^n$.

В случае различимых шариков можно считать, что на множестве A действует группа, состоящая лишь из одного единичного элемента – тождественной перестановки, тогда ответом будет: k^n.

Теория Пойа позволяет рассмотреть действие на множестве A произвольной группы G. Мы можем теперь рассматривать случаи промежуточной различимости шариков, когда некоторые варианты размещений, мы считаем одинаковыми.

Задачи к главе 2

1. Методом математической индукции доказать, что сумма квадратов n первых натуральных чисел равна $\frac{n(n+1)(2n+1)}{6}$.

2. Методом математической индукции доказать, что для любого $n \in N$

а) $1 * 4 + 2 * 7 + \ldots + n(3n+1) = n(n+1)^2$;

б) $1 * 2 + 2 * 5 + \ldots + n(3n-1) = n^2(n+1)$.

3. Методом математической индукции

а) доказать, что для любого $n \in N$ $5^{n+3} + 11^{3n+1}$ делится на 17;

б) доказать, что для любого $n \in N$ $9^{n+2} - 18n - 27$ делится на 18.

4. Разложите перестановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 9 & 4 & 5 & 6 & 7 & 8 & 3 & 2 & 1 & 10 & 11 \end{pmatrix}^{21}$ в произведение независимых циклов, найдите декремент и знак подстановки.

5. Сколькими способами из колоды карт в 36 листов можно выбрать набор из 5 карт так, чтобы в этом наборе были бы 3 пиковые карты, 2 туза, 1 король?

6. Сколько различных упорядоченных наборов букв можно получить перестановкой букв слова «алгоритм» при условии, что первые три позиции заняты согласными?

7. Сколько неотрицательных целых решений имеет уравнение
x + y + z = 12?

8. Сколько натуральных решений имеет уравнение x + y + z = 14?

9. Сколько неотрицательных целых решений имеет неравенство
x + y + z ≤ 15?

10. Сколько натуральных решений имеет неравенство x + y + z <13?

11. Используя рекуррентное соотношение $s_n^k = s_{n-1}^{k-1} + (n-1) \cdot s_{n-1}^k$, и условия $s_0^0 = 1$, $s_0^k = 0$, k ≥ 1, $s_n^0 = 0$, n ≥ 1, заполнить (до нужного места) таблицу чисел Стирлинга 1-го рода, а затем найти количество способов рассадить 10 человек за 5 круглыми столами.

12. Используя рекуррентное соотношение $S_n^k = S_{n-1}^{k-1} + k \cdot S_{n-1}^k$, и условия $s_0^0 = 1$, $s_0^k = 0$, k ≥ 1, $s_n^0 = 0$, n ≥ 1, заполнить (до нужного места) таблицу чисел Стирлинга 2-го рода, а затем найти количество способов разбить 10 человек на 5 групп.

13. Используя рекуррентное соотношение
$L_n^k = L_{n-1}^{k-1} + (n+k-1) \cdot L_{n-1}^k$, и условия $L_0^0 = 1$, $L_0^k = 0$, k ≥ 1,

$L_n^0 = 0, \mathrm{n} \geq 1$, заполнить (до нужного места) таблицу чисел Лаха, а затем найти количество способов построить 10 человек в 5 шеренг. Проверить полученный результат, используя равенство $L_n^k = C_{n-1}^{k-1} \cdot \frac{n!}{k!}$.

14. Используя рекуррентное соотношение $P_n^k = P_{n-1}^{k-1} + P_{n-k}^k$, и условия $P_0^0 = 1,\ P_0^k = 0, \mathrm{k} \geq 1,\ P_n^0 = 0, \mathrm{n} \geq 1$, заполнить (до нужного места) таблицу значений количества разбиений целого неотрицательного числа n на k слагаемых, а затем найти количество способов разбить число 17 на 7 слагаемых.

15. Найти коэффициент при x^{56} в разложении $(x^9 - x^2 + 3)^{29}$ по мультиномиальной формуле, полученный после приведения подобных членов.

16. Найти число различных перестановок цифр набора 3744753, в которых никакие 2 одинаковые цифры не идут друг за другом.

17. Сколько способов переставить, выстроенные в ряд 9 различных предметов, так, что на свои первоначальные места попадут ровно 5 предметов?

18. Сколькими способами можно разложить 8 различных шариков в 5 коробок? Рассмотреть два случая: различимых и неразличимых коробок, и в каждом из этих случаев - два подслучая: когда все коробки окажутся непустыми и когда возможны пустые коробки.

19. Сколько способов представления числа 13 в виде суммы 7 целых слагаемых? Рассмотреть два случая: когда порядок слагаемых существенен и когда не существенен, и в каждом из этих случаев - два подслучая: когда все слагаемые положительны и когда возможны нулевые слагаемые.

20. Сколько натуральных чисел от 1 до 2000 делится на хотя бы на одно из чисел 6, 26, 39?

21. Найдите количество всех четырехзначных чисел, обладающих хотя бы одним из двух свойств: 1) первая цифра числа равна 3; 2) последовательность цифр является неубывающей.

22. Найдите количество всех четырехзначных чисел, обладающих хотя бы одним из двух свойств: 1) последняя цифра числа равна 2; 2) последовательность цифр является невозрастающей.

23. Код замка чемодана состоит из четырех цифр, последовательность цифр упорядоченная. Найдите количество всех таких кодов, обладающих хотя бы одним из двух свойств: 1) последняя цифра кода — 7; 2) последовательность цифр является неубывающей.

24. Для последовательности (a_n) имеет место рекуррентное соотношение: $a_n = -3 \cdot a_{n-1} + 10 \cdot a_{n-2}$ и заданы начальные значения $a_0 = 0, a_1 = 1$.

Записать производящую функцию последовательности $\left(a_n\right)$.

Найти формулу общего члена этой последовательности.

25. Используя теорию Пойа, найти число различных ожерелий из 4 красных бусинок и 7 зеленых бусинок.

ГЛАВА 3. БУЛЕВЫ ФУНКЦИИ

3.1. Булевы функции, основные понятия

Определение. Напомним обозначения: множество $\mathbf{B} = \{0; 1\}$, $\mathbf{B^n} = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n) : x_i \in \mathbf{B}\}$.

Булевой функцией (функцией алгебры логики) n *переменных* называется отображение: $f : \mathbf{B}^n \to \mathbf{B}$.

Булева функция может быть задана таблично: таблицей всех своих значений при всевозможных значениях аргументов. Такие таблицы принято называть *таблицами истинности*.

Наборы значений аргументов (*бинарные наборы*) в таблице истинности принято приводить в так называемом *лексикографическом порядке*, что соответствует возрастающему порядку чисел, если эти наборы рассматривать как запись чисел в двоичной системе счисления.

Пример:

x y	f
0 0	1
0 1	0
1 0	0
1 1	1

Ввиду того, что порядок записи бинарных наборов в таблице истинности фиксирован, булеву функцию можно задать *строкой* (или, говорят, *вектором*) *ее значений*. Например, для рассматриваемой функции так: $f = (1001)$.

Булеву функцию двух переменных можно задать также с помощью *бинарного куба* размерности 2, то есть бинарного квадрата.

Напомним, что $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n) : x_i \in \mathbf{B}\}$ - это множество упорядоченных наборов длины n, состоящих из нулей и единиц. Мы можем считать эти наборы координатами точек в пространстве, в таком случае элементы $\mathbf{B}^n$ представлены вершинами n-мерного куба.

Бинарный квадрат – это набор из четырех точек на координатной плоскости, являющихся вершинами квадрата (рис. 3.1).

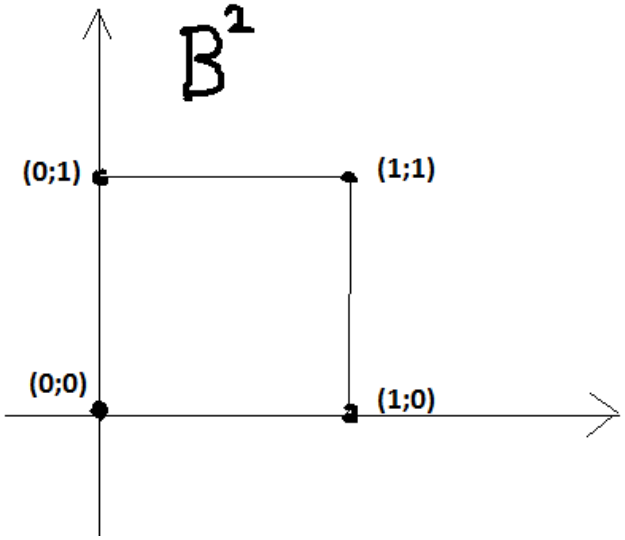


Рисунок 3.1

Булеву функцию двух переменных мы можем теперь задать, выделив в бинарном квадрате вершины, соответствующие тем наборам, на которых функция принимает значение 1. Например, для рассмотренной выше функции это будет выглядеть так (рис. 3.2.):

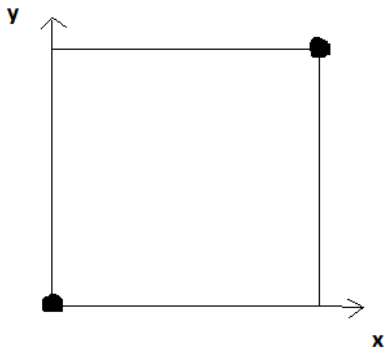


Рисунок 3.2

Булеву функцию 2-х переменных можно также задать с помощью *карты Карно*.

Картой Карно называем прямоугольную таблицу, в данном случае состоящую из 4-х клеток. Каждая клетка этой таблицы соответствует вершине бинарного квадрата, соседние клетки соответствуют соседним вершинам. Далее клетки, соответствующие выделенным вершинам в бинарном квадрате, мы выделяем тем или иным образом. Например, для рассмотренной выше функции получаем (рис. 3.3):

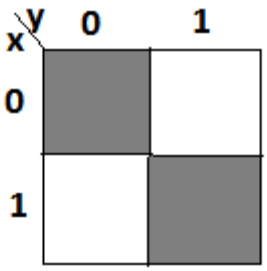


Рисунок 3.3

Подобным же образом мы можем действовать и при рассмотрении булевых функций 3-х переменных.

Булеву функцию 3-х переменных можно задать с помощью таблицы истинности, например:

x y z	f
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	1
1 0 0	0
1 0 1	0
1 1 0	1
1 1 1	1

И опять ввиду того, что порядок записи бинарных наборов в таблице истинности фиксирован, булеву функцию можно задать *строкой* (или, говорят, *вектором*) *ее значений*.

Например, для рассматриваемой функции так: $f = (01110011)$.

Булеву функцию двух переменных можно задать также с помощью *бинарного куба* размерности 3, выделяя вершины, соответствующие наборам, на которых функция принимает значение 1, например, для рассматриваемой функции (рис. 3.4):

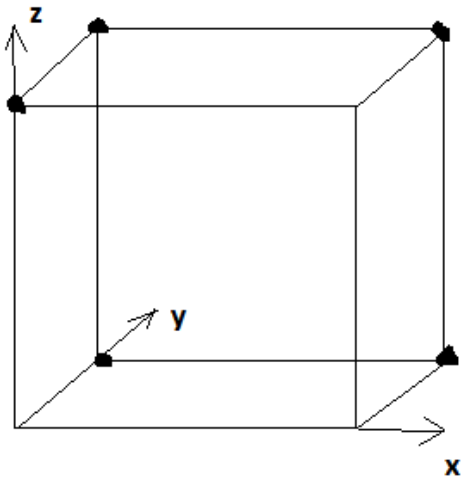


Рисунок 3.4

Булеву функцию 3-х переменных можно также задать с помощью *карты Карно*.

Картой Карно в данном случае будет состоять из 8-ми клеток. Каждая клетка этой таблицы соответствует вершине бинарного квадрата, соседние клетки соответствуют соседним вершинам. Причем считается, что верх таблицы соединен с низом, а правая часть соединена с левой. Клетки, соответствующие выделенным вершинам в бинарном кубе, мы выделяем тем или иным образом. Например, для рассмотренной выше функции (рис. 3.5):

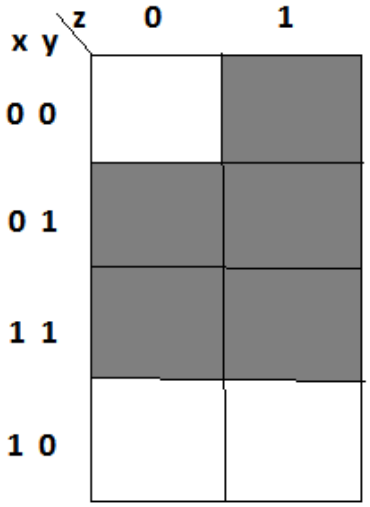


Рисунок 3.5

Поскольку смежные вершины (имеющие общее ребро) на кубе отличаются ровно одной координатой (у одной из вершин эта координата ноль, у второй – единица), бинарные наборы для первых двух координат в карте Карно перечислены не в лексикографическом порядке, а в порядке *кода Грея* (соседние наборы

отличаются только в одной цифре).

На следующем рисунке (рис. 3.6) показано как из изображения на бинарном кубе получается изображение на карте Карно.

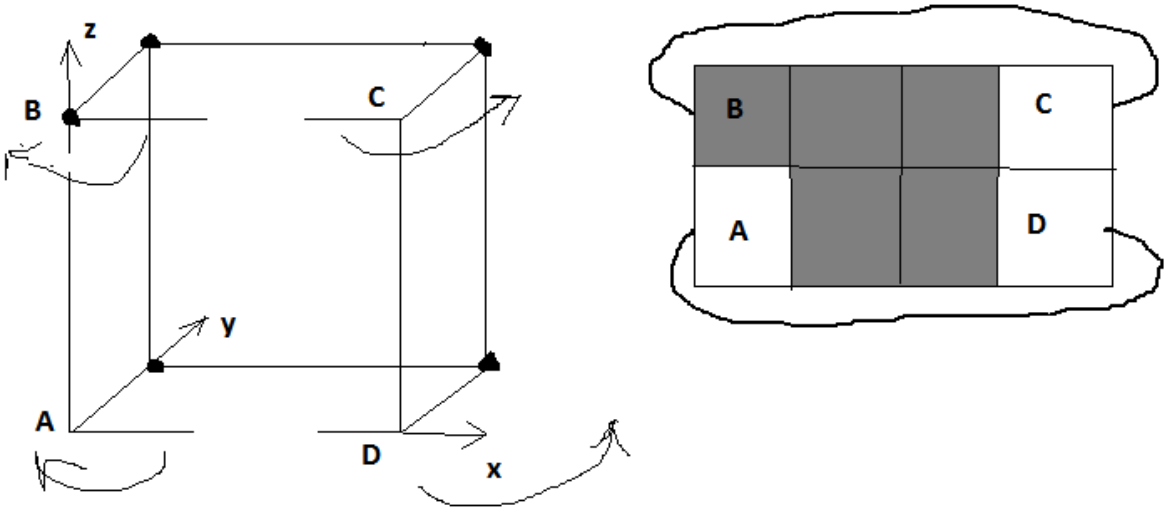


Рисунок 3.6

Можно видеть, что клетки левой стороны считаются соседними с соответствующими клетками правой стороны, поскольку соответствуют смежным вершинам.

Булеву функцию 4-х переменных можно задать таблицей истинности, вектором значений. Использование карты Карно здесь также удобно.

Бинарный куб размерности четыре изобразить в виде картинки на плоскости можно достаточно удобно, если заботиться лишь о том, чтобы смежные вершины на картинке оказались соединенными ребром.

Трехмерный куб, действуя в таком стиле можно так изобразить на плоскости (рис. 3.7):

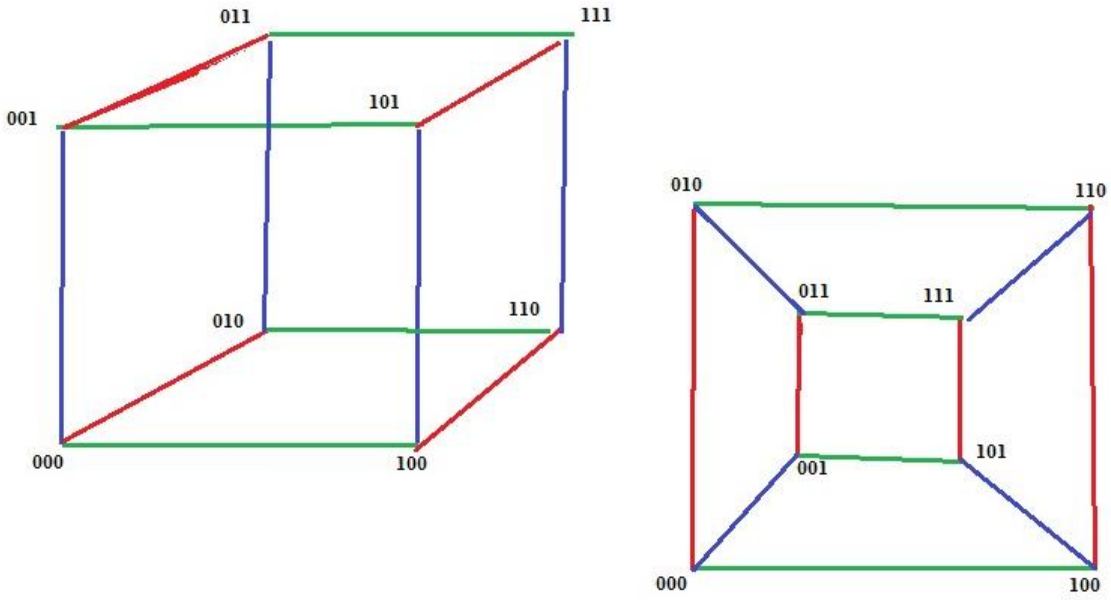


Рисунок 3.7

Мы уменьшили верхнюю грань, а затем спроецировали картинку на нижнюю плоскость.

Подобным же образом можно поступить с четырехмерным кубом.

В результате получится следующее изображение (рис. 3.8):

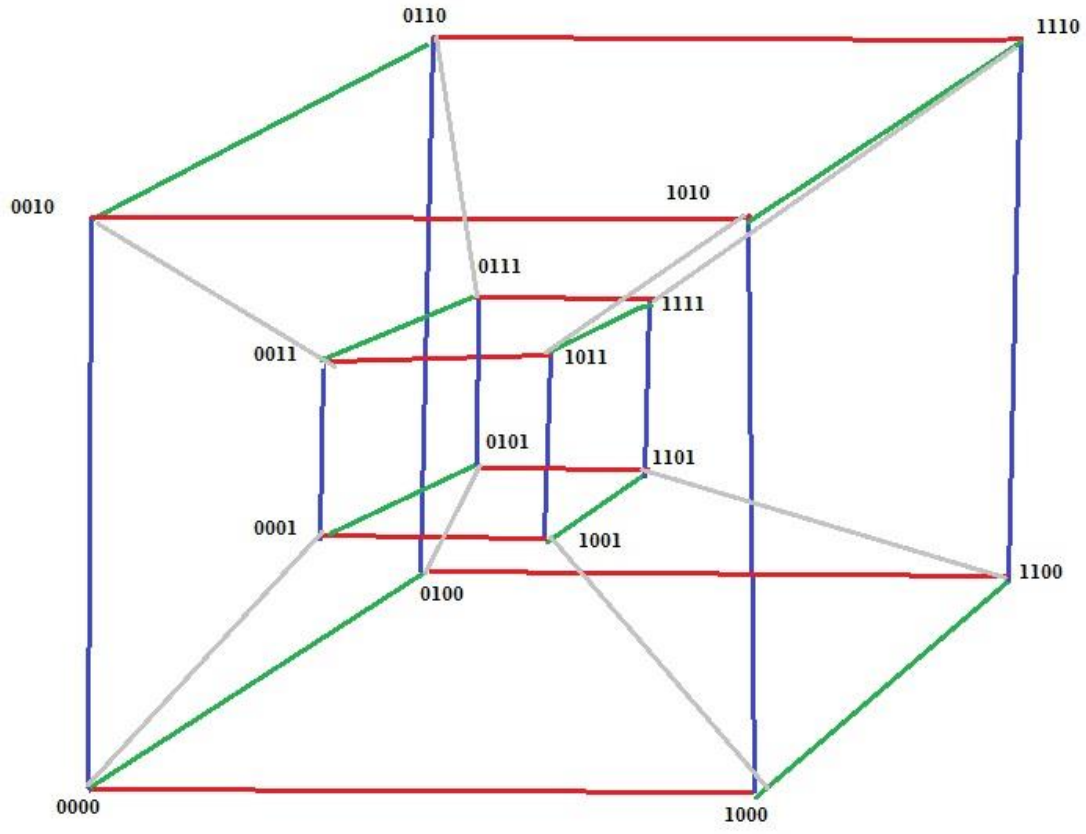


Рисунок 3.8

В роли трехмерных граней этого четырехмерного куба на картинке выступают большой куб, малый куб внутри и шесть усеченных пирамид с основаниями на большом и малом кубах.

Карта Карно в четырехмерном случае изображает 16 вершин четырехмерного куба и состоит из 16 клеток, составляющих квадрат (рис. 3.9):

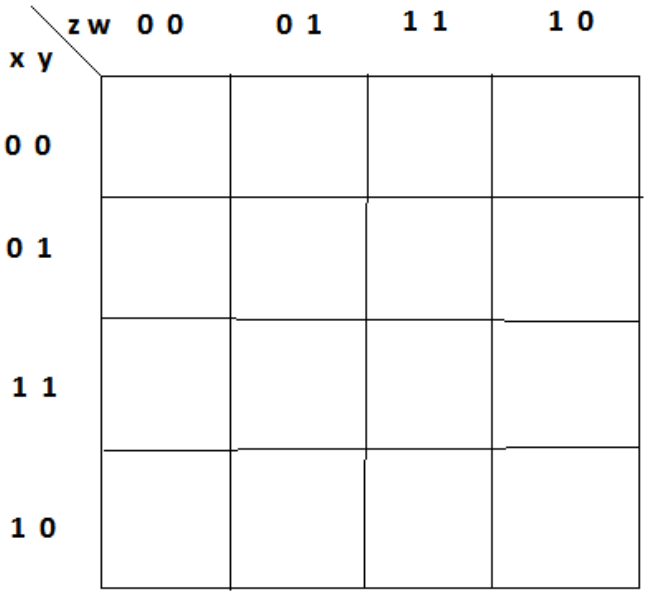


Рисунок 3.9

Здесь считается, что верх таблицы соединен с низом, а правая часть соединена с левой. Если выполнить это соединение, то получится, что таблица являет собой поверхность *тора* (бублика) (рис. 3.10).

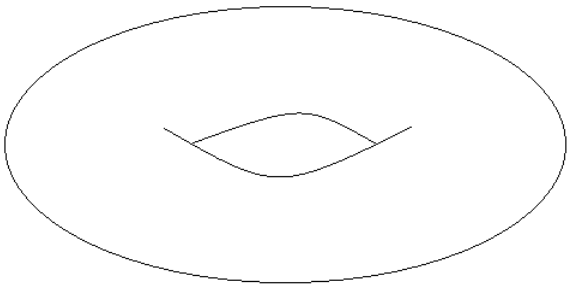


Рисунок 3.10

То, что вершины четырехмерного куба можно представлять себе лежащими на поверхности тора, хорошо видно и на нашем искаженном изображении четырехмерного куба.

3.2. Операции над булевыми переменными (логические связки)

Булевы переменные принимают значения из множества $\mathbf{B} = \{0; 1\}$, его элементы трактуются как логические значения ЛОЖЬ и ИСТИНА.

Таким образом, рассматриваемые операции – это операции над элементами множества $\mathbf{B}$, результаты операций – это снова элементы множества $\mathbf{B}$. Поэтому унарная операция может рассматриваться как булева функция 1-й переменной, а бинарные операции могут рассматриваться как булевы функции 2-х переменных.

Операция отрицания

Это унарная операция, то есть это булева функция 1-й переменной, имеющая следующую таблицу истинности:

x	$f(x)=\overline{x}$
0	1
1	0

Обозначения: $\overline{x}$, $\neg x$.

Конъюнкция (логическое «и», AND)

Это бинарная операция. Результат этой операции будет равен 1 только в случае, когда оба операнда примут значение 1.

Обозначения: xy, $x \wedge y$, $x\&y$.

Таблица истинности:

x	y	x&y
0	0	0
0	1	0
1	0	0
1	1	1

Дизъюнкция (логическое «или», OR)

Это бинарная операция. Результат этой операции будет равен 0 только в случае, когда оба операнда примут значение 0.

Обозначение: $x \vee y$.

Таблица истинности:

x	y	x&y
0	0	0
0	1	0
1	0	0
1	1	1

Сумма по модулю 2 (логическое «исключающее или», XOR)

Это бинарная операция. Результат этой операции будет равен остатку при делении на 2 арифметической суммы значений операндов. Результат будет равен 1 только если ровно один из операндов равен 1.

Обозначение: $x \oplus y$.

Таблица истинности:

x	y	x ⊕ y
0	0	0
0	1	1
1	0	1
1	1	0

Импликация (логическое «следствие»)

Это бинарная операция. Результат этой операции будет равен 0 только в случае, когда первый операнд равен 1, а второй операнд равен 0 (из лжи вытекает все, что угодно, а из истины может вытекать лишь истина).

Обозначение: $x \to y$.

Таблица истинности:

x	y	x→y
0	0	1
0	1	1
1	0	0
1	1	1

Обратная импликация формально другая операция, но она получается из импликации переменой местами операндов. Обозначение: $x \leftarrow y$.

Равнозначность

Это бинарная операция. Результат этой операции будет равен 1 только в случаях, когда оба операнда примут одинаковые значения.

Обозначения: $x \leftrightarrow y$, $x \equiv y$, $x \sim y$. Таблица истинности:

x	y	x~y
0	0	1
0	1	0
1	0	0
1	1	1

Штрих Шеффера (отрицание конъюнкции, NAND)

Это бинарная операция. Результат этой операции будет равен 0, только в случае, когда оба операнда примут значение 1.

Обозначения: $x|y$, $x \uparrow y$.

Таблица истинности:

x	y	x|y
0	0	1
0	1	1
1	0	1
1	1	0

Стрелка Пирса (отрицание дизъюнкции, NOR)

Это бинарная операция. Результат этой операции будет равен 1, только в случае, когда оба операнда примут значение 0.

Обозначение: $x \downarrow y$.

Таблица истинности:

x	y	x↓y
0	0	1
0	1	0
1	0	0
1	1	0

Константы

Элементы множества **B**, *константы* **0** и **1** (ЛОЖЬ и ИСТИНА) могут рассматриваться как функции любого числа переменных (значения которых, правда, не зависят от значений переменных – все переменные оказываются фиктивными).

Некоторые авторы называют их результатами «нуль-арных» операций, или

функциями 0 переменных.

Фиктивные и существенные переменные

Переменная x_1 булевой функции $f(x_1, x_2, \ldots, x_n)$ является *фиктивной*, если $f(0, x_2, \ldots, x_n) = f(1, x_2, \ldots, x_n)$, то есть значение функции не зависит от значений этой переменной. Переменная, не являющаяся фиктивной, называется *существенной*. Подобным же образом определяется, являются ли остальные переменные фиктивными или существенными.

Для функции 3-х (и тем более - 2-х) переменных выявление фиктивных переменных удобно осуществлять с помощью бинарного куба.

Пример. Рассмотрим булеву функцию 3-х переменных, заданную строкой ее значений на бинарных наборах: $f = (e_1\ e_2\ e_3\ e_4\ e_5\ e_6\ e_7\ e_8)$.

Булеву функцию трех переменных можно задать, выделив жирными точками на кубе вершины, соответствующие *единичным наборам* (наборам, на которых функция принимает значение равное единице), например (рис. 3.11).

f=(01011010)

	x1	x2	x3	f
1)	0	0	0	0
2)	0	0	1	1
3)	0	1	0	0
4)	0	1	1	1
5)	1	0	0	1
6)	1	0	1	0
7)	1	1	0	1
8)	1	1	1	0

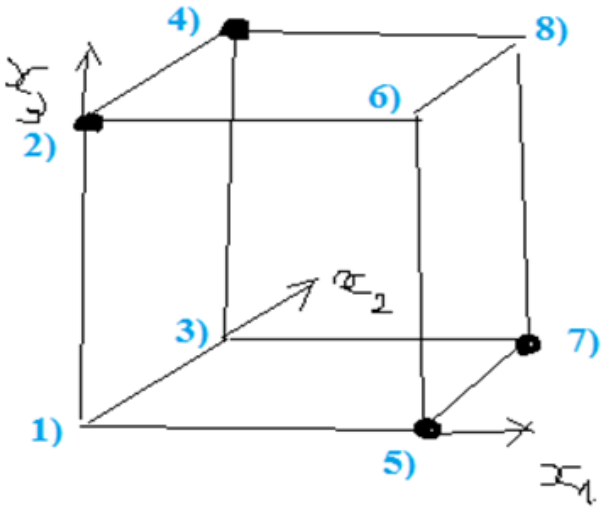


Рисунок 3.11

Имея такое изображение булевой функции мы можем мгновенно определить, какие переменные будут существенными, а какие фиктивными. 1) Поскольку при проецировании грани 5) 6) 8) 7) на грань 1) 2) 4) 3) жирные точки ***не*** совпадают, можно сделать вывод что переменная x1 – *существенная* переменная,

2) Поскольку при проецировании грани 3) 4) 8) 7) на грань 1) 2) 6) 5) жирные точки совпадают, можно сделать вывод что переменная x2 – *фиктивная* переменная,

3) Поскольку при проецировании грани 2) 4) 8) 6) на грань 1) 3) 7) 5) жирные

точки ***не*** совпадают, можно сделать вывод что переменная x3 – *существенная* переменная.

Далее мы можем получить таблицу истинности для функции f(x1,x3), рассмотрев ее значения на грани 1) 2) 6) 5):

	x1	x3	f
1)	0	0	0
2)	0	1	1
5)	1	0	1
6)	1	1	0

Нетрудно понять, что $f = x1 \oplus x2$.

Задание булевых функций формулами с использованием логических связок

Дав имена переменными, мы можем, используя логические связки, сформировать формулу, которая будет естественным образом определять булеву функцию.

При этом мы должны учитывать порядок выполнения логических операций, для которого принятый *по умолчанию приоритет следующий: отрицание, конъюнкция, дизъюнкция, сумма по модулю 2, импликация, равнозначность, штрих Шеффера, стрелка Пирса*. Ну и, конечно, в первую очередь порядок выполнения операций определяется скобками (отрицание, оформляемое с использованием надчерты, равноценно соответствующему использованию скобок).

Кроме того, мы должны задать порядок на множестве переменных: какая переменная первая, какая вторая и т. д.

И еще, мы должны знать, сколько всего у нас переменных, то есть функцию какого числа переменных должна задавать данная формула.

Пример:

Рассмотрим формулу $x \to y$.

Эта формула задает функцию 2-х переменных, импликацию:

$$f(x, y) = x \to y.$$

Эта же формула может задавать другую функцию 2-х переменных, обратную импликацию: $f(y, x) = x \to y$.

Также можно считать, что эта формула задает функцию 3-х переменных: $f(x, y, z) = x \to y$, или другую функцию 3-х переменных:

$f(x,z,y) = x \to y$, и еще бесконечное число возможностей.

Запись вида $f(x_1, x_2, \ldots, x_n) = \textit{формула}$, для которой все переменные из формулы присутствуют в списке $\{x_1, x_2, \ldots, x_n\}$, определяет булеву функцию однозначно.

Замечание. Понятие формулы можно расширить, разрешив использовать в записи формулы помимо имен переменных и логических связок еще и некоторые функции в стандартной записи: «Имя функции (список переменных)». Функции могут в качестве операндов выступать в логических связках и далее можно вместо переменных в выражение для функции подставлять формулы.

Логические тождества

Если две формулы выражают одну и ту же функцию (упорядоченного) набора всех переменных, присутствующих в обеих формулах, это записывают в виде тождества: *Формула1=Формула2*.

Приведем некоторые логические тождества:

1. $\overline{\overline{x}} = x$;
2. $x \vee \overline{x} = 1$, $x\&\overline{x} = 0$;
3. $\overline{x \vee y} = \overline{x} \wedge \overline{y}$, $\overline{x \wedge y} = \overline{x} \vee \overline{y}$ (законы де Моргана);
4. $(x \vee y) \vee z = x \vee (y \vee z)$, $(x \wedge y) \wedge z = x \wedge (y \wedge z)$, $(x \oplus y) \oplus z = x \oplus (y \oplus z)$ (ассоциативность дизъюнкции, конъюнкции и суммы по модулю 2);
5. $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$, $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$ (дистрибутивность конъюнкции относительно дизъюнкции и дизъюнкции относительно конъюнкции);
6. $(x \oplus y)z = (xz) \oplus (yz)$ (дистрибутивность конъюнкции относительно суммы по модулю 2);
7. $x \oplus 1 = \overline{x}$;
8. $x \to y = \overline{x} \vee y$;
9. $x|x = \overline{x}$;
10. $x \downarrow x = \overline{x}$;
11. $x\&y = (x|y)|(x|y)$;
12. $x \vee y = (x \downarrow y) \downarrow (x \downarrow y)$;
13. $x \oplus y = \overline{x \leftrightarrow y}$.

3.3. Дизъюнктивные и конъюнктивные нормальные формы булевой функции

Дизъюнктивные нормальные формы булевой функции

Мы рассматриваем функции n переменных $x_1, x_2, \ldots, x_n$.

Обозначение. Для булевой переменной x будем (где это будет удобно) использовать обозначение $x^0 = \overline{x}$, $x^1 = x$.

Определение. *Элементарной конъюнкцией ранга k* называется выражение вида $x_{i_1}^{p_1} \cdot x_{i_2}^{p_2} \cdot \ldots \cdot x_{i_k}^{p_k}$, здесь к переменные или к их отрицания участвуют в операции конъюнкции, $i_1, i_2, \ldots, i_k$ - различные числа не превосходящие n.

Константу 1 будем считать элементарной конъюнкцией ранга 0.

Примеры:

$x_1\overline{x_3}$, x_2x_3, $\overline{x_1x_2}$ - элементарные конъюнкции ранга 2,

$\overline{x_3}$, x_2 - элементарные конъюнкции ранга 1,

$\overline{x_1}x_2\overline{x_3}$ - элементарная конъюнкция ранга 3.

Определение. *Областью истинности* булевой функции $f(x_1, x_2, \ldots, x_n)$ мы назовем множество бинарных наборов, на которых эта функция принимает значение, равное 1.

Пример: Для булевой функции, заданной таблицей истинности:

x y z	f
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	1
1 0 0	0
1 0 1	0
1 1 0	1
1 1 1	1

областью истинности будет множество наборов {(0 0 1), (0 1 0), (0 1 1), (1 1 0), (1 1 1)}. Эту область истинности мы изображаем на бинарном кубе, выделяя точки, или на карте Карно помечая клетки (рис. 3.12):

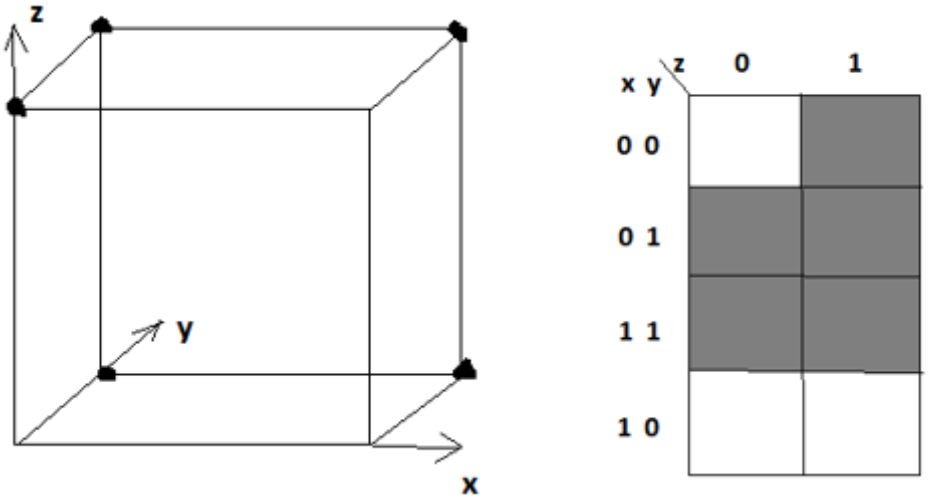


Рисунок 3.12

Определение. *Бинарным подкубом размерности* m *бинарного куба размерности* n, $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n): x_i \in \mathbf{B}\}$ называется множество бинарных наборов $(x_1; x_2; \ldots, x_n)$, в каждом из которых одни и те же $n - m$ переменных имеют фиксированные значения (0 или 1).

Например, для $n = 3$ на рисунке ниже (рис. 3.13) бинарные подкубы размерности 2 это множества из 4-х наборов, соответствующих углам граней этого куба, бинарные подкубы размерности 1 – это множества из 2-х наборов, соответствующие концам ребер куба, бинарные подкубы размерности 0 – это наборы соответствующие вершинам куба.

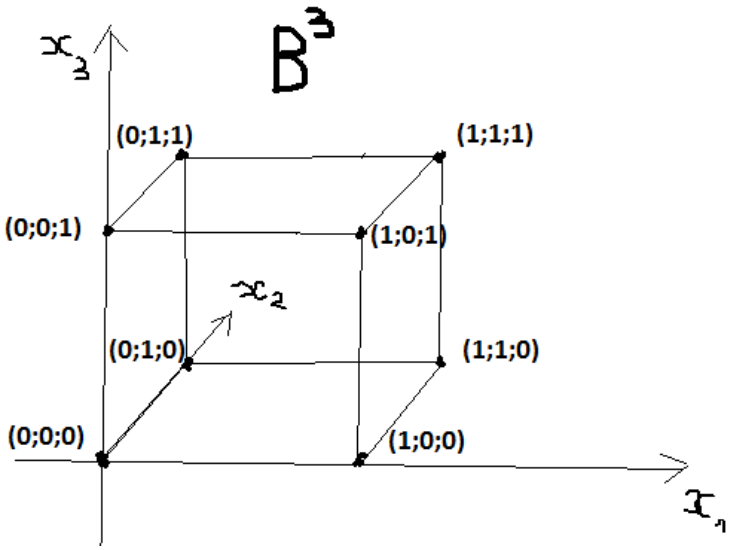


Рисунок 3.13

Утверждение. Областью истинности элементарной конъюнкции ранга k является бинарный подкуб размерности $n - k$.

Доказательство. Область истинности элементарной конъюнкции $x_{i_1}^{p_1} \cdot x_{i_2}^{p_2} \cdot \ldots \cdot x_{i_k}^{p_k}$ состоит из наборов, в которых ровно $n - (n - k) = k$ конкретных переменных имеют фиксированные значения: $x_{i_1} = p_1, \ldots, x_{i_k} = p_k$, поэтому – это бинарный подкуб размерности $n - k$.

Также легко доказать следующее утверждение.

Утверждение. Любой бинарный подкуб размерности m является областью истинности некоторой элементарной конъюнкции ранга $n - m$.

Примеры:

1. Выделенными точками на бинарном кубе изображена область истинности для конъюнкции x (рис. 3.14).

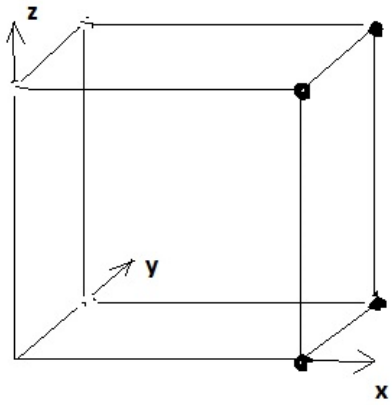


Рисунок 3.14

2. Выделенными точками на бинарном кубе изображена область истинности для конъюнкции $\overline{z}$ (рис. 3.15).

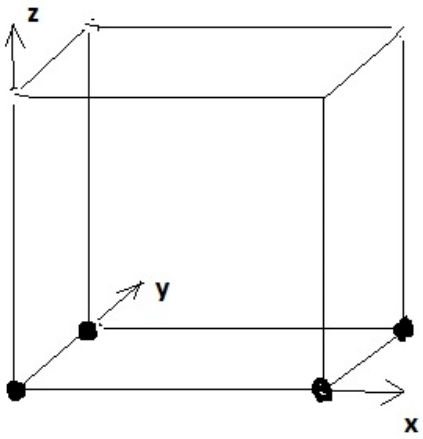


Рисунок 3.15

3. Выделенными точками на бинарном кубе изображена область истинности для конъюнкции $x\overline{z}$ (рис. 3.16).

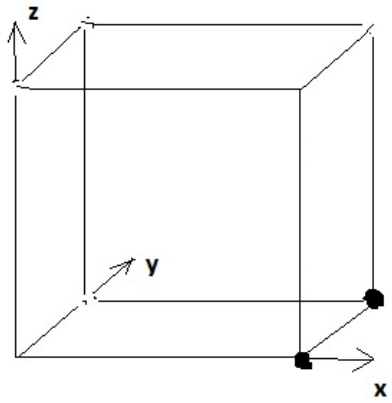


Рисунок 3.16

3. Выделенной точкой на бинарном кубе изображена область истинности для конъюнкции $x\overline{y}z$ (рис. 3.17).

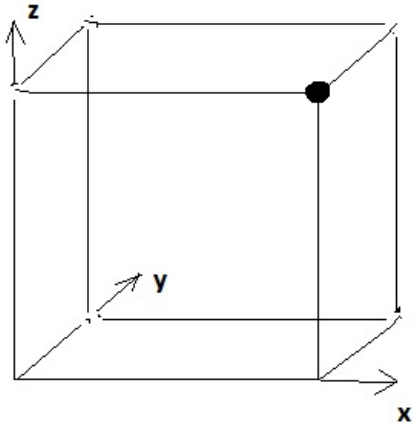


Рисунок 3.17

Имеет место очевидное утверждение.

Утверждение. Область истинности булевой функции $f = f_1 \vee f_2$ является объединением областей истинности функций f_1 и f_2.

Определение. *Дизъюнктивной нормальной формой булевой функции (ДНФ)* называется представление этой функции формулой, являющейся дизъюнкцией элементарных конъюнкций.

Пример: $f(x, y, z) = y \vee \overline{z} \vee xz \vee x\overline{y} \vee \overline{x}yz$

Представление булевой функции в форме ДНФ равноценно представлению области истинности этой функции в виде объединения бинарных подкубов.

Определение. ДНФ булевой функции n переменных $f(x_1, x_2, \ldots, x_n)$ называется полной или *совершенной дизъюнктивной нормальной формой (СДНФ)*, если все элементарные конъюнкции в ней имеют максимальный ранг n.

Областью истинности конъюнкции максимального ранга является бинарный подкуб размерности 0, то есть эта область состоит из одной точки (одного бинарного набора). Поэтому представление булевой функции в форме СДНФ равноценно представлению области истинности в виде дизъюнктного объединения своих точек. Ввиду этого знаки дизъюнкции («или») в СДНФ могут быть заменены на знаки суммы по модулю 2 («исключающее или»). Так, вообще говоря, нельзя делать в произвольной (не совершенной) ДНФ, поскольку подкубы, задаваемые элементарными конъюнкциями, могут пересекаться.

Пример: Построим СДНФ для следующей булевой функции (рис. 3.18).

f=(01011010)

	x1	x2	x3	f
1)	0	0	0	0
2)	0	0	1	1
3)	0	1	0	0
4)	0	1	1	1
5)	1	0	0	1
6)	1	0	1	0
7)	1	1	0	1
8)	1	1	1	0

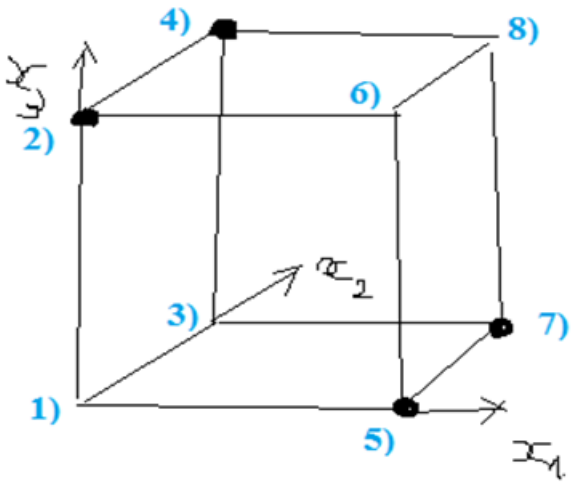


Рисунок 3.18

Область истинности этой функции состоит из 4-х наборов, помеченных в таблице истинности номерами 2, 4, 5 и 7.

Элементарная конъюнкция ранга 3 принимающая значение 1 только на наборе 2 – это конъюнкция $\overline{x_1}\overline{x_2}x_3$, для набора 4 – это конъюнкция $\overline{x_1}x_2x_3$, для набора 5 – это конъюнкция $x_1\overline{x_2}x_3$, для набора 7 – это конъюнкция $x_1x_2\overline{x_3}$.

Итак, СДНФ для данной булевой функции будет иметь вид:

$$f = \overline{x_1}\overline{x_2}x_3 \vee \overline{x_1}x_2x_3 \vee x_1\overline{x_2}x_3 \vee x_1x_2\overline{x_3}.$$

Как мы уже отмечали в СДНФ знаки дизъюнкции могут быть заменены на знаки суммы по модулю 2:

$$f = \overline{x_1}\overline{x_2}x_3 \oplus \overline{x_1}x_2x_3 \oplus x_1\overline{x_2}x_3 \oplus x_1x_2\overline{x_3}.$$

Отметим в виде теоремы очевидное утверждение.

Теорема. Всякая булева функция, кроме константы 0, может быть единственным образом представлена в форме СДНФ.

Конъюнктивные нормальные формы булевой функции

Мы рассматриваем функции n переменных $x_1, x_2, \ldots, x_n$.

Для булевой переменной x будем (где это будет удобно) использовать обозначение $x^0 = \overline{x}$, $x^1 = x$.

Определение. *Элементарной дизъюнкцией ранга* k называется выражение вида $x_{i_1}^{p_1} \vee x_{i_2}^{p_2} \vee \ldots \vee x_{i_k}^{p_k}$, здесь *k* переменные или *k* их отрицания участвуют в операции дизъюнкции, $i_1, i_2, \ldots, i_k$ - различные числа не превосходящие n.

Константу 0 будем считать элементарной дизъюнкцией ранга 0.

Примеры:

$x_1 \vee \overline{x_3}$, $x_2 \vee x_3$, $\overline{x_1} \vee \overline{x_2}$ - элементарные конъюнкции ранга 2,

$\overline{x_3}$, x_2- элементарные дизъюнкции ранга 1,

$\overline{x_1} \vee x_2 \vee \overline{x_3}$- элементарная дизъюнкция ранга 3.

Определение. *Областью ложности* булевой функции $f(x_1, x_2, \ldots, x_n)$ мы назовем множество бинарных наборов, на которых эта функция принимает значение, равное 0.

Пример: Для булевой функции, заданной таблицей истинности:

x y z	f
0 0 0	0
0 0 1	1
0 1 0	1
0 1 1	1
1 0 0	0
1 0 1	0
1 1 0	1
1 1 1	1

областью ложности будет множество наборов {(0 0 0), (1 0 0), (1 0 1)}.

Эту область истинности мы видим в виде множества невыделенных точек на бинарном кубе, выделяя точки, или в виде непомеченных клеток на карте Карно (рис. 3.19).

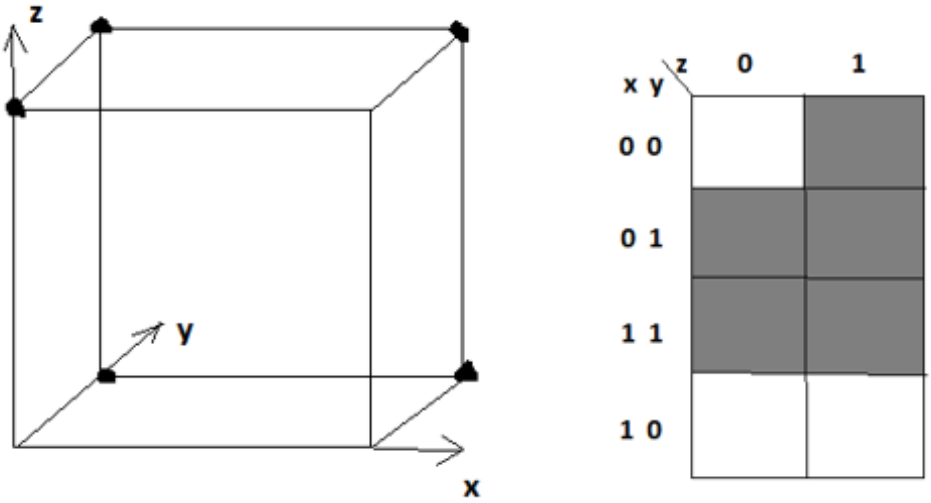


Рисунок 3.19

Утверждение. Областью ложности элементарной дизъюнкции ранга k является бинарный подкуб размерности $n-k$.

Доказательство

Область ложности элементарной дизъюнкции $x_{i_1}^{p_1} \vee x_{i_2}^{p_2} \vee \ldots \vee x_{i_k}^{p_k}$ состоит из наборов, в которых ровно $n-(n-k)=k$ конкретных переменных имеют фиксированные значения: $x_{i_1} = \overline{p_1}, \ldots, x_{i_k} = \overline{p_k}$, поэтому – это бинарный подкуб размерности $n-k$.

Также легко доказать следующее утверждение.

Утверждение. Любой бинарный подкуб размерности m является областью ложности некоторой элементарной дизъюнкции ранга $n-m$.

Примеры:

1. Выделенными кругами точками на бинарном кубе изображена область ложности для дизъюнкции x (рис. 3.20).

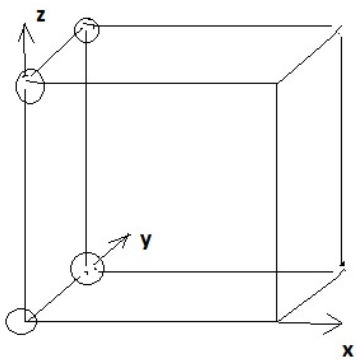


Рисунок 3.20

2. Выделенными кругами точками на бинарном кубе изображена область ложности для дизъюнкции $\overline{z}$ (рис. 3.21).

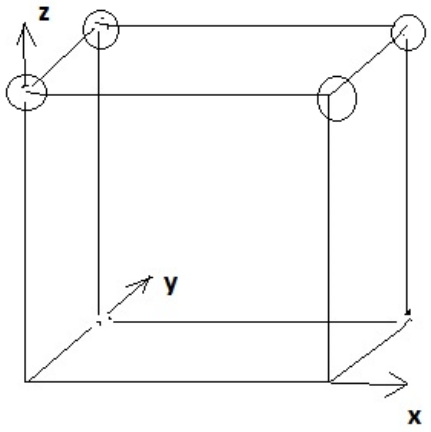


Рисунок 3.21

3. Выделенными кругами точками на бинарном кубе изображена область ложности для дизъюнкции $x \vee \overline{z}$ (рис. 3.22).

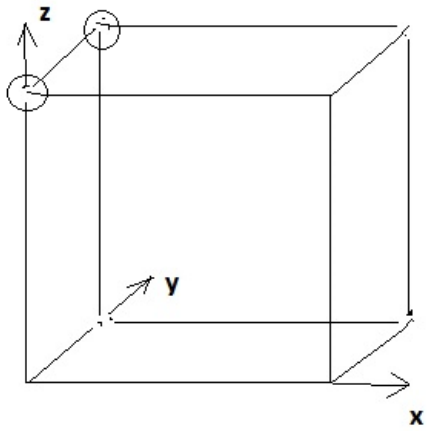


Рисунок 3.22

4. Выделенным кругом точкой на бинарном кубе изображена область ложности для дизъюнкции $x \vee \overline{y} \vee z$ (рис. 3.23).

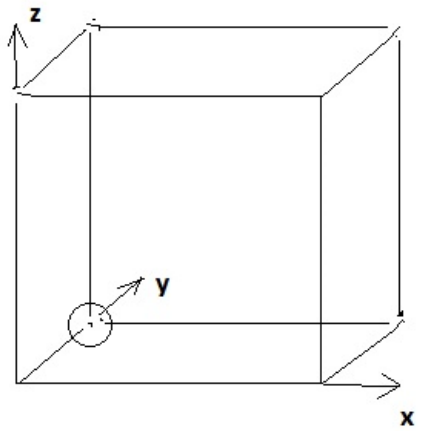


Рисунок 3.23

Имеет место очевидное утверждение.

Утверждение. Область ложности булевой функции $f = f_1 \& f_2$ является объединением областей ложности функций f_1 и f_2.

Определение. *Конъюнктивной нормальной формой булевой функции (КНФ)* называется представление этой функции формулой, являющейся дизъюнкцией элементарных конъюнкций.

Пример: $f(x, y, z) = y\&\overline{z}\&(x \vee z)\&(x \vee \overline{y})\&(\overline{x} \vee y \vee z)$.

Представление булевой функции в форме КНФ равноценно представлению области ложности этой функции в виде объединения бинарных подкубов.

Определение. КНФ булевой функции n переменных $f(x_1, x_2, \ldots, x_n)$ называется полной или *совершенной конъюнктивной нормальной формой (СКНФ)*, если все элементарные дизъюнкции в ней имеют максимальный ранг n.

Областью ложности дизъюнкции максимального ранга является бинарный подкуб размерности 0, то есть эта область состоит из одной точки (одного бинарного набора). Поэтому представление булевой функции в форме СКНФ равноценно представлению области ложности в виде дизъюнктного объединения своих точек. Ввиду этого знаки конъюнкции в СКНФ могут быть заменены на знаки равнозначности. Так, вообще говоря, нельзя делать в произвольной (не совершенной) КНФ, поскольку подкубы, задаваемые элементарными дизъюнкциями, могут пересекаться.

Пример: Построим СКНФ для следующей булевой функции (рис. 3.24)

f=(01011010)

	x1	x2	x3	f
1)	0	0	0	0
2)	0	0	1	1
3)	0	1	0	0
4)	0	1	1	1
5)	1	0	0	1
6)	1	0	1	0
7)	1	1	0	1
8)	1	1	1	0

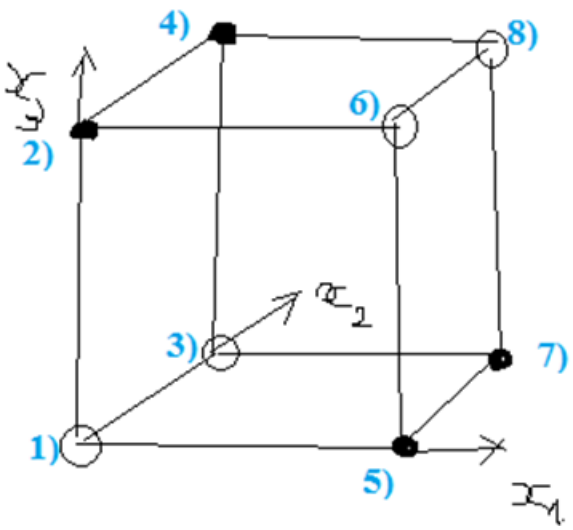


Рисунок 3.24

Область ложности этой функции состоит из 4-х наборов, помеченных в таблице истинности номерами 1, 3, 6 и 8.

Элементарная дизъюнкция ранга 3 принимающая значение 0 только на наборе 1 – это дизъюнкция $x_1 \vee x_2 \vee x_3$, для набора 3 – это конъюнкция $x_1 \vee \overline{x_2} \vee x_3$, для набора 6 – это дизъюнкция $\overline{x_1} \vee x_2 \vee \overline{x_3}$, для набора 8 – это дизъюнкция $\overline{x_1} \vee \overline{x_2} \vee \overline{x_3}$.

Итак, СКНФ для данной булевой функции будет иметь вид:

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

Как мы уже отмечали в СКНФ знаки дизъюнкции могут быть заменены на знаки равнозначности:

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

Отметим в виде теоремы очевидное утверждение.

Теорема. Всякая булева функция, кроме константы 1, может быть единственным образом представлена в форме СКНФ.

3.4. Минимизация ДНФ

Определение. ДНФ булевой функции n переменных $f(x_1, x_2, \ldots, x_n)$ называется *минимальной*, если сумма рангов элементарных конъюнкций, входящих в ДНФ, имеет наименьшее значение из всех значений для всевозможных ДНФ, представляющих данную функцию.

Определение. Бинарный подкуб, являющийся подмножеством множества бинарных наборов M, называется *максимальным для* M, если он не является собственным подмножеством другого подкуба, также вложенного в M.

Определение. Элементарная конъюнкция $x_{i_1}^{p_1} \cdot x_{i_2}^{p_2} \cdot \ldots \cdot x_{i_k}^{p_k}$ называется *импликантом* для функции n переменных $f(x_1, x_2, \ldots, x_n)$, если ее область истинности является подмножеством области истинности функции f.

Определение. Импликант $x_{i_1}^{p_1} \cdot x_{i_2}^{p_2} \cdot \ldots \cdot x_{i_k}^{p_k}$ является *простым импликантом*, если нельзя убрать ни одной переменной $x_{i_j}^{p_j}$ из этого выражения так, что оставшаяся элементарная конъюнкция была импликантом для функции f.

Очевидно, что это равносильно тому, что область истинности этого импликанта является максимальным подкубом для области истинности функции f.

Утверждение. Минимальная ДНФ булевой функции является дизъюнкцией некоторых простых импликантов.

Доказательство. Если в минильной ДНФ присутствует импликант, не являющийся простым, можно удалить лишний символ в этой конъюнкции, снизив тем самым ее ранг.

Итак, задача нахождения минимальной ДНФ для данной функции сводится к подбору множества простых импликантов для данной функции, таких, чтобы дизъюкция этих импликантов образовывала ДНФ для этой функции и имела бы наименьшую сумму рангов конъюнкций. Это равносильно подбору покрытия области истинности данной функции максимальными для этой области подкубами, так, чтобы сумма чисел $n - d_i$ (где d_i - размерности подкубов) была минимальной.

Для $n = 2,3,4$ эта задача легко решается геометрически, используя бинарный куб или карту Карно.

Примеры:

Рассмотрим функции, заданные выделенными точками на бинарном кубе (рис. 3.25-3.27). Построим для них минимальную ДНФ.

1)

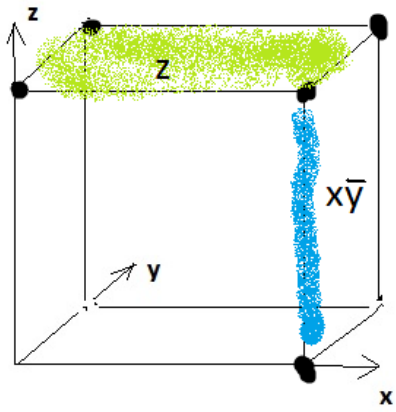


Рисунок 3.25

Минимальная ДНФ имеет вид: $f(x,y,z) = z \vee x\bar{y}$.

2)

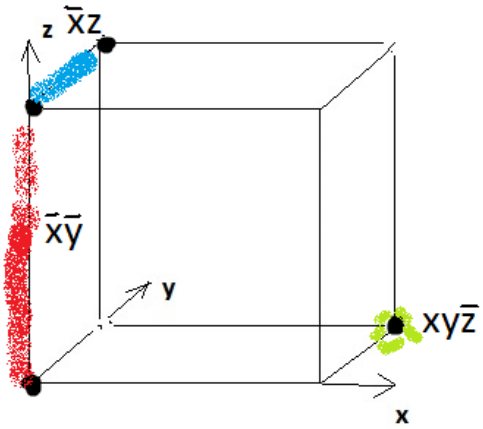


Рисунок 3.26

Минимальная ДНФ имеет вид: $f(x,y,z) = \overline{xy} \vee \bar{x}z \vee xy\bar{z}$.

3)

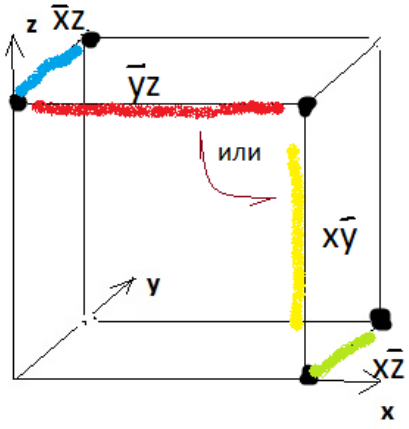


Рисунок 3.27

Минимальная ДНФ имеет вид:
$f(x,y,z) = xz \vee x\overline{z} \vee x\overline{y}$ или $f(x,y,z) = xz \vee x\overline{z} \vee \overline{y}z$.

Пример:

Рассмотрим функцию 4-х переменных, заданную выделенными точками на бинарном кубе (рис. 3.28). Построим для нее минимальную ДНФ. Затем найдем минимальную ДНФ этой функции, используя карту Карно.

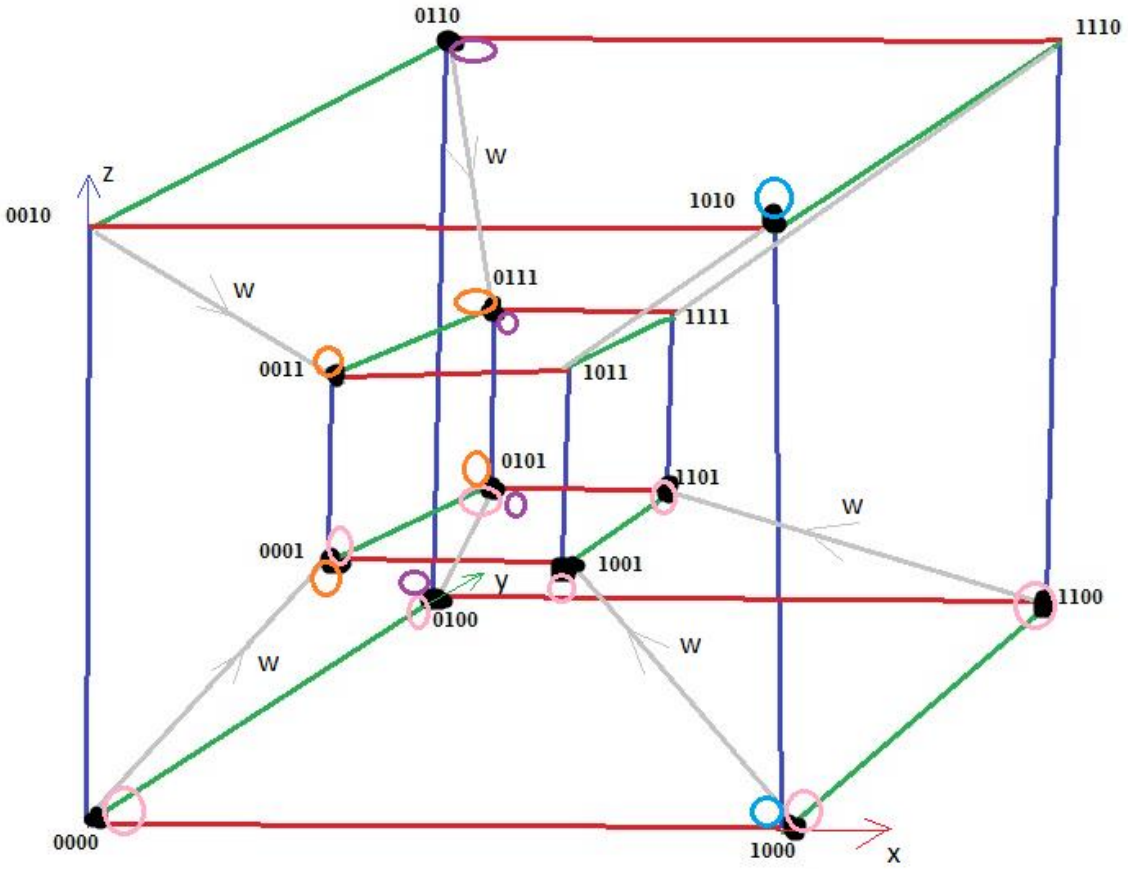


Рисунок 3.28

Минимальная ДНФ имеет вид: $f(x,y,z) = \overline{z} \vee \overline{x}w \vee \overline{x}y \vee x\overline{y}\overline{w}$.

Здесь:

1) усеченная пирамида изображает бинарный подкуб размерности 3, являющийся областью истинности первой конъюнкции,

2) вертикальный квадрат на маленьком внутреннем кубике (бинарный подкуб размерности 2) – это область истинности второй конъюнкции,

3) трапеция (бинарный подкуб размерности 2), помеченная фиолетовыми кружками – область истинности третьей конъюнкции,

4) ребро (бинарный подкуб размерности 1), помеченное синими кружками – область истинности четвертой конъюнкции.

Ось четвертой переменной всюду направлена к центру картинки.

Найдем минимальную ДНФ этой функции, используя карту Карно (рис. 3.29).

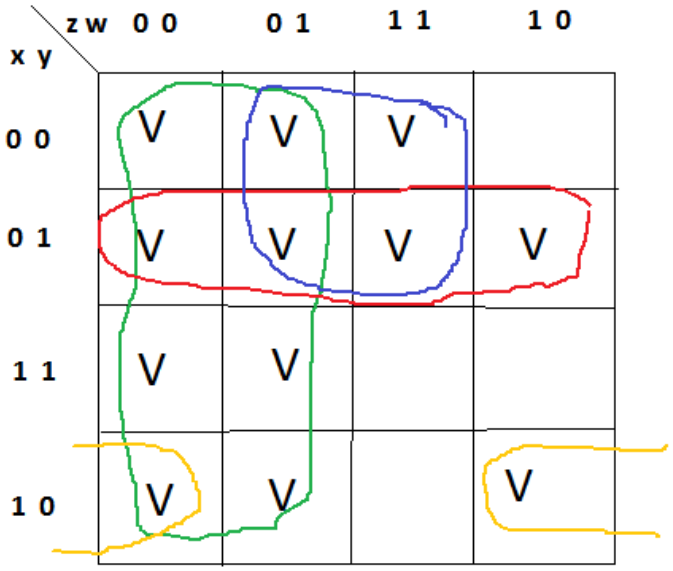


Рисунок 3.29

Минимальная ДНФ имеет вид: $f(x, y, z) = \overline{z} \vee \overline{x}w \vee \overline{x}y \vee x\overline{yw}$.

Здесь бинарные подкубы изображаются прямоугольниками, состоящими из 1, 2, 4, и 8 клеток.

1) Обведенный зеленым прямоугольник из 8 клеток соответствует бинарному подкубу размерности 3 – это область истинности первой конъюнкции,

2) обведенный синим прямоугольник прямоугольник из 4 клеток соответствует бинарному подкубу размерности 2 – это область истинности второй конъюнкции,

3) обведенный красным прямоугольник прямоугольник из 4 клеток соответствует бинарному подкубу размерности 2 – это область истинности третьей конъюнкции,

4) обведенный желтым прямоугольник прямоугольник из 2 клеток (правая и левая сторона таблицы считаются соединенными) соответствует бинарному подкубу размерности 1 – это область истинности четвертой конъюнкции.

Использование изображения бинарного куба или карт Карно для поиска минимальной ДНФ булевой функции более 4-х переменных делается невозможным. В этом случае используют другие подходы.

Для булевой функции большого числа переменных сначала находят все простые импликанты.

Дизъюнкция всех простых импликантов данной булевой функции является

ДНФ этой функции и называется *канонической формой Блейка-Порецкого* (некоторые авторы называют ее неудачным термином «сокращенная ДНФ»).

Каноническую форму Блейка-Порецкого можно найти, открыв скобки в выражении СКНФ данной функции и далее применяя тождество поглощения $K_1K_2 \vee K_1 = K_1$.

Есть и другие способы, например, применение склейки по переменным в конъюнкциях, составляющих СДНФ ($xK \vee \overline{x}K = K$).

Далее выбор из канонической формы Блейка-Порецкого части, образующей минимальную ДНФ можно осуществить, используя алгоритм Петрика-Квайна-Мак-Класки.

Количество простых импликантов для булевой функции (даже не очень) большого числа переменных может быть чудовищно большим. Поэтому использование известных точных алгоритмов для нахождения минимальной ДНФ становится неподъемной задачей даже для современных компьютеров. В современной практике используют более быстрые алгоритмы, обеспечивающие приближенное нахождение минимальной ДНФ (ESPRESSO).

3.5. Самодвойственные, монотонные и линейные функции. Полиномы Жегалкина

Самодвойственные функции

Определение. Рассмотрим булеву функцию n переменных $f(x_1, x_2, \ldots, x_n)$.

Функция $\hat{f}(x_1, x_2, \ldots, x_n)$, значения которой определяется равенством $\hat{f}(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$, называется двойственной к f функцией.

Очевидно, что двойственная к двойственной функции будет исходная функция.

Примерами двойственных пар функций являются конъюнкция и дизъюнкция (понимаемые как функции 2-х переменных), штрих Шеффера и стрелка Пирса, сумма по модулю 2 и равнозначность.

Определение. Функция называется *самодвойственной*, если двойственная к ней функция совпадает с исходной функцией.

Утверждение. Для самодвойственной функции на всех бинарных наборах выполнено равенство $\overline{f(x_1, x_2, \ldots, x_n)} = f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})$, то есть значение этой функции на противоположных наборах противоположны.

Доказательство

$$f(x_1, x_2, \ldots, x_n) = \hat{f}(x_1, x_2, \ldots, x_n) = \overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}$$

$$\overline{f(x_1, x_2, \ldots, x_n)} = \overline{\overline{f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n})}} = f(\overline{x_1}, \overline{x_2}, \ldots, \overline{x_n}).$$

Бинарные наборы упорядочены в таблице истинности таким образом, что противоположные наборы расположены симметрично относительно середины (рис. 3.30).

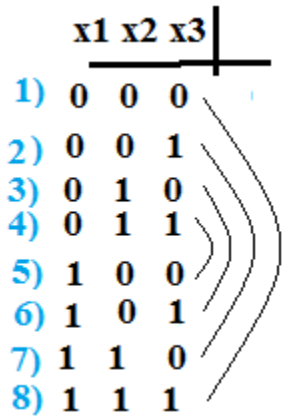
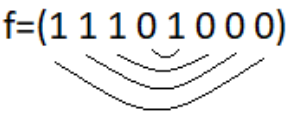


Рисунок 3.30

Отсюда немедленно вытекает утверждение.

Утверждение (критерий самодвойственности). Булева функция будет самодвойственной тогда и только тогда, когда в векторе ее значений симметрично относительно середины расположенные значения будут противоположны.

Пример:



Эта булева функция 3-х переменных, заданная вектором значений, будет самодвойственной.

Непостоянные функции 1-й переменной $f(x) = x$ и $f(x) = \overline{x}$ будут самодвойственными.

Нетрудно показать, используя критерий самодвойственности, что не существует самодвойственных функций 2-х переменных, в которых обе переменные будут существенными.

Класс (множество) всех самодвойственных булевых функций мы будем обозначать буквой S.

Монотонные функции

Определение. Рассмотрим булеву функцию n переменных $f(x_1, x_2, \ldots, x_n)$. Определим частичный порядок на бинарных наборах: бинарный набор $(a_1 a_2 \ldots a_n) \geq (b_1 b_2 \ldots b_n)$, если $a_i \geq b_i$ для $i = 1,2,\ldots,n$.

Булева функция будет *монотонной* (обозначение: $f \in M$), если $(a_1 a_2 \ldots a_n) \geq (b_1 b_2 \ldots b_n) \Rightarrow f(a_1, a_2, \ldots, a_n) \geq f(b_1, b_2, \ldots, b_n)$.

Для функции 3-х переменных для установления наличия монотонности удобно использовать бинарный куб.

Порядок на бинарных наборах хорошо виден на бинарном кубе (порядок указан стрелками) (рис. 3.31).

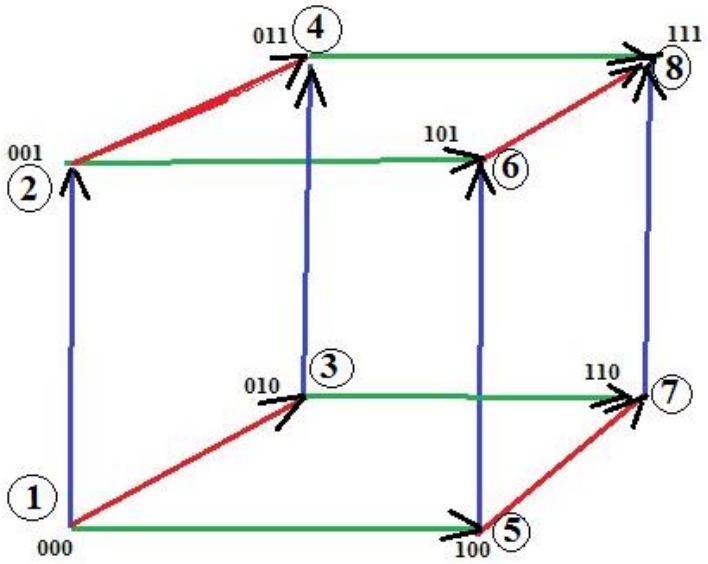


Рисунок 3.31

Здесь мы видим, что набор 8 больше всех остальных, наборы 4, 6 и 8 больше, чем набор 2 и т. д.

Булева функция 3-х переменных будет *монотонной* ($f \in M$), если $(a_1 a_2 a_3) \geq (b_1 b_2 b_3) \Rightarrow f(a_1, a_2, a_3) \geq f(b_1, b_2, b_3)$.

Пусть булева функция задана строкой ее значений на бинарных наборах: $f = (e_1\ e_2\ e_3\ e_4\ e_5\ e_6\ e_7\ e_8)$.

Если $f \in M$ и $e_1 = 1$, то очевидно, что на всех наборах значение этой функции будет равно 1, поскольку все остальные наборы больше первого набора, то есть в этом случае $f \equiv 1$ - *постоянная функция.*

Рассуждая аналогично, если $f \in M$ и $e_8 = 0$, то на всех наборах значение этой функции будет равно 0, поскольку все остальные наборы меньше восьмого

набора, то есть в этом случае $f \equiv 0$ - *постоянная функция.*

Итак, если $f \in M$ *и* $f \neq const$, *то*

1) $e_1 = 0$ *и* $e_8 = 1$.

Далее, учитывая частичный порядок на наборах, получим:

2) если $e_2 = 1$, *то* $\begin{cases} e_4 = 1, \\ e_6 = 1; \end{cases}$

3) если $e_3 = 1$, *то* $\begin{cases} e_4 = 1, \\ e_7 = 1; \end{cases}$

4) если $e_5 = 1$, *то* $\begin{cases} e_6 = 1, \\ e_7 = 1. \end{cases}$

Примеры:

$f = (0\,1\,0\,1\,1\,1\,1\,1) \in M,$

$f = (1\,1\,0\,1\,1\,1\,1\,1) \notin M,$

$f = (0\,1\,1\,1\,1\,1\,0\,1) \notin M,$

$f = (0\,1\,1\,1\,0\,1\,1\,1) \in M.$

Замечание. Можно сразу установить наличие или отсутствие монотонности функции, записав соответствующие значения функции около вершин бинарного куба со стрелками. *Для монотонной функции нельзя попасть, двигаясь по стрелкам из вершины, помеченной единицей, в вершину, помеченную нулем* (из жирной точки в нежирную).

Пример: $f = (01011010)$.

Эта функция ***не*** *является монотонной*. Из жирной точки 2), например, можно попасть в нежирную точку 6) (рис. 3.32).

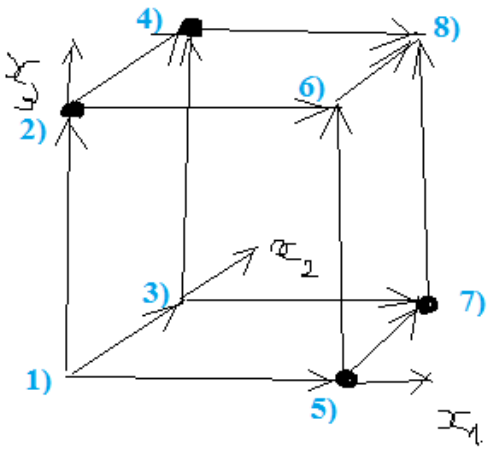


Рисунок 3.32

Для функции 2-х переменных также удобно использовать бинарный куб размерности 2 (рис. 3.33).

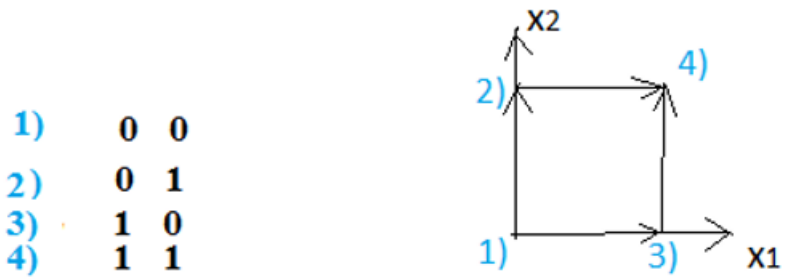


Рисунок 3.33

Используя бинарный куб легко проверить, что конъюнкция и дизъюнкция являются монотонными функциями 2-х переменных, а импликация и сумма по модулю 2 - нет.

Утверждение. Ни одно из двух множеств всех самодвойственных и всех монотонных функций не является подмножеством второго: $S\backslash M \neq \emptyset,\ M\backslash S \neq \emptyset$.

Доказательство

$f_1 = (1\,1\,1\,0\,1\,0\,0\,0)$

$f_1 \in S,\ f_1 \notin M$

$f_2 = (0\,1\,1\,1\,0\,1\,1\,1)$

$f_2 \in M,\ f_2 \notin S.$

Полиномы Жегалкина

Легко проверить, что элементарные конъюнкции, не содержащие отрицаний переменных (в том числе константа 1), являются монотонными функциями, а элементарные конъюнкции, содержащие отрицания переменных не являются монотонными функциями.

Определение. Одна монотонная элементарная конъюнкция или сумма по модулю 2 нескольких различных монотонных элементарных конъюнкций называется *полиномом Жегалкина*. Константа 0 также считается полиномом Жегалкина.

Пример: $1 \oplus x_2 \oplus x_1x_3$.

Замечание. Полином Жегалкина можно трактовать как многочлен нескольких переменных, считая аналогом умножения конъюнкцию, а аналогом сложения сумму по модулю 2. В полиноме Жегалкина не присутствуют степени большие единицы для переменных, поскольку, например, $x_1x_1x_1 = x_1$.

Полином Жегалкина, представляющий данную булеву функцию, можно получить из СДНФ этой функции. Мы уже замечали, что в СДНФ вместо знаков дизъюнкции можно ставить знаки суммы по модулю 2. Далее нужно использовать тождества $\overline{x} = x \oplus 1$, $A \oplus A = 0$, а также дистрибутивность конъюнкции относительно суммы по модулю 2.

Пример:

$$f = x_1\overline{x_2}x_3 \vee \overline{x_1x_2}x_3 = x_1\overline{x_2}x_3 \oplus \overline{x_1x_2}x_3 =$$
$$= x_1(x_2 \oplus 1)x_3 \oplus (x_1 \oplus 1)(x_2 \oplus 1)x_3 =$$
$$= x_1x_2x_3 \oplus x_1x_3 \oplus x_1x_2x_3 \oplus x_1x_3 \oplus x_2x_3 \oplus x_3 = x_2x_3 \oplus x_3.$$

Количество различных монотонных элементарных конъюнкций n переменных равно количеству всех подмножеств множества из n элементов, то есть равно 2^n. Количество полиномов Жегалкина n переменных равно количеству подмножеств множества всех монотонных элементарных конъюнкций, то есть равно 2^{2^n}. Получается, что различных полиномов Жегалкина n переменных столько же, сколько всех булевых функций n переменных. Поэтому одна и та же булева функция не может быть представлена двумя различными полиномами Жегалкина.

Итак, мы доказали теорему.

Теорема. Любая булева функция единственным образом представляется полиномом Жегалкина.

Получение полинома Жегалкина преобразованием СДНФ является трудоемким методом. Рассмотрим быстрый метод.

Быстрый способ получения полинома Жегалкина булевой функции 3-х переменных (метод А.Н. Выборнова)

Напомним, уже определенный выше частичный порядок на бинарных наборах: бинарный набор $a_1a_2a_3 \geq b_1b_2b_3$, если $a_i \geq b_i$ для $i = 1,2,3$.

Этот порядок хорошо виден на бинарном кубе (порядок указан стрелками) (рис. 3.34).

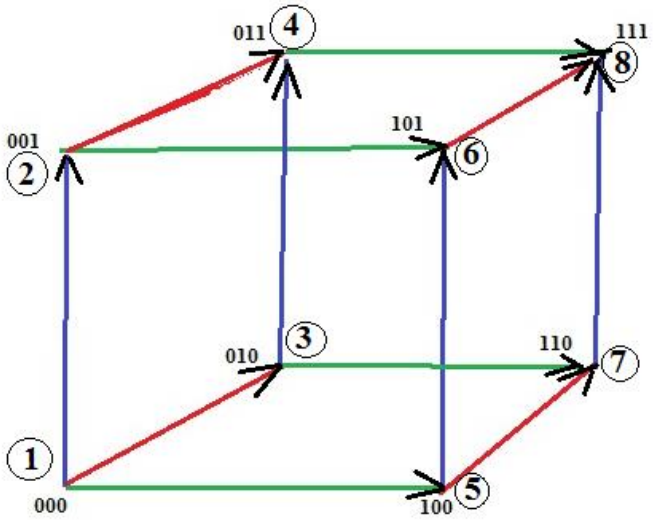


Рисунок 3.34

Изложим теперь быстрый способ получения полинома Жегалкина.

1) Запишем таблицу истинности функции.

2) Напишем столбец монотонных конъюнкций, соответствующих бинарным наборам (см. пример). Порядок его формирования ясен из примера.

3) Находим самую верхнюю единицу в столбце значений функции. Отмечаем кружком эту единицу – тем самым определяем набор, напротив которого стоит эта единица.

4) Прибавим единицу (сложение по модулю 2) ко всем значениям функции в наборах больше либо равных отмеченному набору, результаты записываем в новый столбец. Остальные значения столбца переписываем в новый столбец без изменений.

5) В новом столбце находим самую верхнюю единицу и повторяем действия 3) и 4) пока не получим столбец из нулей.

Искомый полином Жегалкина состоит из мономов, стоящих в отмеченных строках (см. пример рис. 3.35).

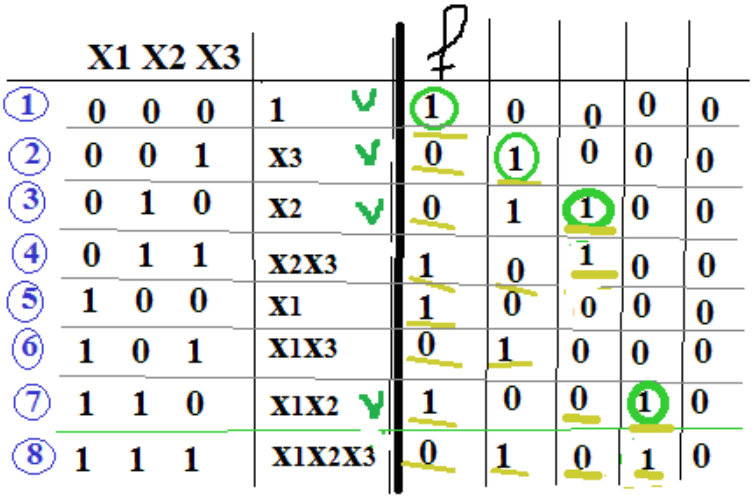


Рисунок 3.35

$$f = 1 \oplus x_3 \oplus x_2 \oplus x_1x_2.$$

Еще один пример (рис. 3.36).

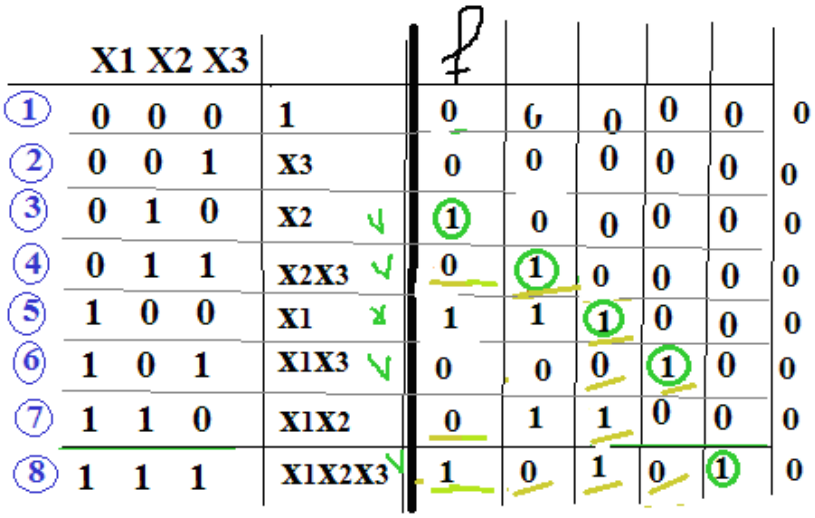


Рисунок 3.36

$$f = x_2 \oplus x_2x_3 \oplus x_1 \oplus x_1x_3 \oplus x_1x_2x_3.$$

Обоснование метода Выборнова основано на том, что в полиноме Жегалкина участвуют монотонные конъюнкции. По сути, мы накрываем область истинности нашей булевой функции подкубами, являющимися областями истинности монотонных конъюнкций, так, чтобы, каждый набор области истинности был покрыт нечетное число раз, а наборы не из области истинности оказались накрыты четное число раз.

Метод переносится на случай функций большего числа переменных (при его применении нужно учитывать частичный порядок на бинарных наборах).

Линейные (афинные) булевы функции

Определение. Булева функция называется *линейной*, если линеен ее полином Жегалкина, то есть он не содержит произведений (конъюнкций) нескольких переменных. Линейная булева функция n переменных может быть задана формулой вида: $f(x_1,\dots,x_n) = c_0 \oplus c_1x_1 \oplus\dots\oplus c_nx_n$,
где $c_i \in \mathbf{B} = \{0;1\}$.

Класс всех линейных булевых функций мы будем обозначать буквой L.

Замечание. Из-за того, что полином Жегалкина линейной булевой функции может содержать в качестве слагаемого константу 1 (что не соответствует понятию линейности в линейной алгебре), некоторые авторы называют линейные булевы функции *афинными*.

Утверждение. Количество различных линейных булевых функций n переменных равно 2^{n+1}.

Доказательство. Количество различных линейных булевых функций n переменных равно количеству различных бинарных наборов $(c_0c_1\dots c_n)$ длины $(n+1)$.

Обсудим теперь, как определять наличие или отсутствие линейности у булевой функции. Обычно здесь предлагают построить полином Жегалкина. Но это плохой, трудоемкий вариант.

Сформулируем простой критерий линейности, используя который, по вектору значений булевой функции можно почти ***мгновенно*** установить ее линейность (или нелинейность).

Рассмотрим сначала случай булевой функции 3-х переменных.

Теорема (А.Н. Выборнов). ***Критерий линейности булевой функции 3-х переменных***

Рассмотрим булеву функцию 3-х переменных, заданную строкой ее значений на бинарных наборах: $f = (e_1\ e_2\ e_3\ e_4\ e_5\ e_6\ e_7\ e_8)$.

Эта функция будет линейной тогда и только тогда, когда для всей строки $(e_1\ e_2\ e_3\ e_4\ e_5\ e_6\ e_7\ e_8)$ и для ее половины $(e_1\ e_2\ e_3\ e_4)$ выполнены условия:

а) ***симметрично,*** относительно середины, ***расположенные значения*** функции *равны,*

ИЛИ

б) ***симметрично***, относительно середины, ***расположенные значения*** функции ***противоположны*** (рис. 3.37).

Рисунок 3.37

Итак, f линейна тогда и только тогда, когда выполнены условия 1 и 2:

1. $\begin{cases} e_1 = e_4 \\ e_2 = e_3 \end{cases}$ *или* $\begin{cases} e_1 = \bar{e}_4 \\ e_2 = \bar{e}_3 \end{cases}$;

2. $\begin{cases} e_1 = e_8 \\ e_2 = e_7 \\ e_3 = e_6 \\ e_4 = e_5 \end{cases}$; *или* $\begin{cases} e_1 = \bar{e}_8 \\ e_2 = \bar{e}_7 \\ e_3 = \bar{e}_6 \\ e_4 = \bar{e}_5 \end{cases}$.

Докажем эту теорему чуть позже.

Заметим сразу, что из этой теоремы вытекает, что ***строка значений непостоянной линейной булевой функции содержит ровно 4 единицы, из них 0, 2, или все 4 единицы в первой половине строки.*** Это необходимое условие линейности позволяет во многих случаях быстро обнаруживать *отсутствие* линейности.

Примеры:

Примеры линейных функций:

$f = (1\,1\,1\,1\,1\,1\,1\,1)$,
$f = (0\,0\,0\,0\,1\,1\,1\,1)$,
$f = (1\,0\,0\,1\,1\,0\,0\,1)$,
$f = (1\,0\,0\,1\,0\,1\,1\,0)$,
$f = (0\,0\,1\,1\,1\,1\,0\,0)$,
$f = (0\,0\,1\,1\,0\,0\,1\,1)$,
$f = (0\,1\,1\,0\,1\,0\,0\,1)$.

Примеры нелинейных функций:

$f = (1\,0\,1\,1\,1\,1\,0\,1)$ (шесть единиц),
$f = (1\,0\,0\,1\,0\,1\,0\,1)$ (нет ни симметрии, ни антисимметрии на всей строке),
$f = (0\,1\,0\,1\,1\,0\,0\,0)$ (три единицы),
$f = (0\,1\,1\,0\,1\,1\,0\,0)$ (нет ни симметрии, ни антисимметрии на всей строке),
$f = (0\,0\,1\,0\,1\,0\,1\,1)$ (одна единица в первой половине строки).

Критерий линейности булевой функции 3-х переменных вытекает из следующей общей теоремы.

Теорема (*А.Н. Выборнов*). ***Критерий линейности булевой функции n переменных***

Рассмотрим булеву функцию n переменных $f(x_1,\dots x_n) = (e_1\ e_2\ \dots e_{2^n})$.

Эта функция будет линейной тогда и только тогда, когда для каждого $k = n, n-1, \dots, 2, 1$ для функции $g_k = (e_1\ e_2\ \dots e_{2^k})$ имеет место один из случаев:

а) симметрично, относительно середины, расположенные значения функции равны, то есть: $e_1 = e_{2^k}$, $e_2 = e_{2^k-1}$, …, $e_{2^{k-1}} = e_{2^{k-1}+1}$;

б) симметрично, относительно середины, расположенные значения функции противоположны, то есть: $e_1 = \bar{e}_{2^k}$, $e_2 = \bar{e}_{2^k-1}$, …, $e_{2^{k-1}} = \bar{e}_{2^{k-1}+1}$.

Доказательство общей теоремы. Очевидно, что если функция $f = g_n$ линейна, то и все функции g_k будут линейными, поскольку переход от g_k к g_{k-1} равносилен отбрасыванию первой переменной. В линейном полиноме Жегалкина отбрасывание одной переменной приводит снова к линейному полиному Жегалкина. Нетрудно проверить, что для линейной булевой функции выполнены условия а) или б). Поэтому условия теоремы выполнены для всякой линейной булевой функции.

Поскольку существует 4 различных функций типа g_1 и количество различных функций типа g_k в два раза больше, чем количество различных функций типа g_{k-1} то, очевидно, что количество различных функций n переменных $g_n = (e_1\ e_2\ \dots e_{2^n})$, удовлетворяющих условиям теоремы, будет равно 2^{n+1} - столько же, сколько линейных функций n переменных.

Теорема доказана.

Пример: Функция $\phi(x_1, x_2, x_3, x_4) = (1001\ 1001\ 0110\ 0110)$ будет линейной, а функция $\psi(x_1, x_2, x_3, x_4) = (1001\ 1010\ 1010\ 0110)$ **не** будет линейной.

Утверждение. Ни одно из двух множеств всех самодвойственных и всех линейных функций не является подмножеством второго: $S \backslash L \neq \emptyset,\ L \backslash S \neq \emptyset$.

Доказательство

$f_1 = (1\ 1\ 1\ 0\ 1\ 0\ 0\ 0)$

$f_1 \in S,\ f_1 \notin L$

$f_2 = (0\ 1\ 0\ 1\ 1\ 0\ 1\ 0)$
$f_2 \in L,\ f_2 \notin S.$

Утверждение. Ни одно из двух множеств всех линейных и всех монотонных функций не является подмножеством второго: $L \backslash M \neq \emptyset,\ M \backslash L \neq \emptyset.$

Доказательство
$f_1 = (0\ 1\ 1\ 0\ 0\ 1\ 1\ 0)$
$f_1 \in L,\ f_1 \notin M$
$f_2 = (0\ 1\ 1\ 1\ 0\ 1\ 1\ 1)$
$f_2 \in M,\ f_2 \notin L.$

3.6. Классы Поста

Рассмотренные нами 3 класса булевых функций (самодвойственные, монотонные, линейные) относят к так называемым *классам Поста*.

Есть еще 2 класса Поста: класс T_0 и класс T_1.

Определение. Булева функция $f(x_1, \dots x_n)$ принадлежит классу T_0, или, как говорят, *сохраняет ноль*, если $f(0, \dots, 0) = 0$.

Булева функция $f(x_1, \dots x_n)$ принадлежит классу T_1, или, как говорят, *сохраняет единицу*, если $f(1, \dots, 1) = 1$.

Очевидно, что функция будет принадлежать к классу T_0 тогда и только тогда, когда в векторе ее значений первым элементом будет 0, и функция будет принадлежать к классу T_1 тогда и только тогда, когда в векторе ее значений последним элементом будет 1.

Отметим, что ***мы располагаем простыми критериями, позволяющими определять по вектору значений принадлежность функции каждому из классов Поста.*** Опираясь на это легко доказать следующие утверждения.

Утверждение. $S \backslash T_0 \neq \emptyset,\ T_0 \backslash S \neq \emptyset.$
Утверждение. $M \backslash T_0 \neq \emptyset,\ T_0 \backslash M \neq \emptyset.$
Утверждение. $L \backslash T_0 \neq \emptyset,\ T_0 \backslash L \neq \emptyset.$
Утверждение. $S \backslash T_1 \neq \emptyset,\ T_1 \backslash S \neq \emptyset.$
Утверждение. $M \backslash T_1 \neq \emptyset,\ T_1 \backslash M \neq \emptyset.$
Утверждение. $L \backslash T_1 \neq \emptyset,\ T_1 \backslash L \neq \emptyset.$
Утверждение. $T_0 \backslash T_1 \neq \emptyset,\ T_1 \backslash T_0 \neq \emptyset.$

Итак, ***для любых двух классов Поста существует булева функция, принадлежащая одному классу и не принадлежащая другому.***

Функциональная полнота систем булевых функций

Определение. Рассмотрим две булевых функции $f(x_1, x_2, \dots, x_n)$ и $g(x_1, x_2, \dots, x_k)$. Будем говорить, что функция $h(x_1, x_2, \dots, x_{n-1+k}) = f(x_1, x_2, \dots, x_{n-1}, g(x_n, x_{n+1}, \dots, x_{n-1+k}))$ получена из первой функции *подстановкой* на место последней переменной второй функции.

Эту операцию можно назвать *частичной композицией* этих функций.

Определение. Рассмотрим булеву функцию n переменных $f(x_1, x_2, \dots, x_n)$.

Определим функцию $n + m$ переменных равенством

$$F(x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_{n+m}) = f(x_1, x_2, \dots, x_n).$$

Будем говорить, что вторая функция получена из первой *добавлением фиктивных переменных*.

Пусть теперь в функции $n + m$ переменных

$$G(x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_{n+m})$$

последние m переменных являются фиктивными, определим функцию n переменных $g(x_1, x_2, \dots, x_n) = G(x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_{n+m})$.

Теперь будем говорить, что вторая функция получена из первой *исключением* (может быть не всех) *фиктивных переменных*.

Определение. Рассмотрим некоторую перестановку $(i_1, i_2, \dots, i_n)$ из чисел $(1,2, \dots, n)$. Определим функцию $g(y_1, y_2, \dots, y_n) = f(y_{i_1}, y_{i_2}, \dots, y_{i_n})$.

Мы будем говорить, что функция g получена из функции f *перестановкой переменных*.

Определение. Рассмотрим функцию $n + m$ переменных

$$F(x_1, x_2, \dots, x_n, x_{n+1}, \dots, x_{n+m}).$$

Положим $f(x_1, x_2, \dots, x_n) = F(x_1, x_2, \dots, x_n, x_n, \dots, x_n)$.

Будем говорить, что вторая функция получена из первой *отождествлением переменных*.

Определение. Пусть M - некоторое множество булевых функций.

Функциональным замыканием $[M]$этого множества называется множество всех таких булевых функций, которые могут быть получены из функций множества M применением операций: частичной композиции, добавления фиктивных переменных, исключения фиктивных переменных, перестановки переменных, отождествления переменных.

Множество булевых функций называется функционально замкнутым, если оно совпадает со своим замыканием: $[M] = M$. Функционально замкнутое множество булевых функций называется также *итеративной системой булевых функций (термин Э. Поста)*.

Теорема. Каждый из классов Поста является функционально замкнутым множеством булевых функций.

Эту теорему нетрудно доказать, нужно проверять, что применение процедур частичной композиции, добавления фиктивных переменных, исключения фиктивных переменных, перестановки переменных, отождествления переменных к функциям из рассматриваемого класса Поста не выводят за пределы этого класса.

Определение. Множество булевых функций (когда это множество конечное, употребляют слова «система булевых функций») называют *функционально полным*, если функциональное замыкание этого множества совпадает с множеством всех булевых функций.

Очевидно, что каждый из классов Поста не является функционально полным множеством, поскольку он замкнут и не совпадает с множеством всех булевых функций.

В то же время, например, система, состоящая из двух булевых функций: конъюнкции и отрицания, является функционально полной, поскольку всякую функцию можно задать в виде СДНФ, используя конъюнкцию, отрицание и дизъюнкцию, а дизъюнкцию можно выразить, используя тождество де Моргана, используя конъюнкцию и отрицание: $x \vee y = \overline{\overline{x}\&\overline{y}}$.

Более того, система, состоящая из одной булевой функции NAND (штрих Шеффера), является функционально полной, поскольку отрицание выражается с использованием штриха Шеффера: $\overline{x} = x|x$, и конъюнкция также может быть выражена: $x\&y = (x|y)|(x|y)$. (Эти тождества мы приводили ранее).

Аналогично проверяется, что система, состоящая из одной булевой функции NOR (стрелка Пирса) также является функционально полной.

Булевы функции, в одиночку образующие функционально полную систему функций, называют *шефферовыми*.

Итак, стрелка Пирса является шефферовой функцией.

Имеет место теорема Э. Поста, устанавливающая необходимое и достаточное условие того, чтобы заданное множество булевых функций было функционально полным.

Теорема Поста. Множество A булевых функций будет функционально полным в том и только в том случае. когда для каждого из пяти классов Поста во множестве A найдется функция, не принадлежащая этому классу, то есть выполнены условия: $A\backslash T_0 \neq \emptyset,\ A\backslash T_1 \neq \emptyset,\ A\backslash S \neq \emptyset,\ A\backslash M \neq \emptyset,\ A\backslash L \neq \emptyset.$

Доказательство. Пусть множество A булевых функций является функционально полным. Если бы A полностью лежало в одном из классов Поста, то его замыкание (состоящее из всех булевых функций) также бы полностью лежало в этом (замкнутом) классе, что невозможно.

Путь теперь выполнены условия

$A\backslash T_0 \neq \emptyset,\ A\backslash T_1 \neq \emptyset,\ A\backslash S \neq \emptyset,\ A\backslash M \neq \emptyset,\ A\backslash L \neq \emptyset.$

Обозначим функции

$$nt_0(x_1, \dots, x_k) \in A\backslash T_0,$$
$$nt_1(x_1, \dots, x_k) \in A\backslash T_1,$$
$$ns(x_1, \dots, x_k) \in A\backslash S,$$
$$nm(x_1, \dots, x_k) \in A\backslash M,$$
$$nl(x_1, \dots, x_k) \in A\backslash L.$$

Отождествим все переменные в функции $nt_0(x_1, \dots, x_k)$, получим функцию $\alpha(x) = nt_0(x, \dots, x)$. Тогда $\alpha(0) = 1$. Если $\alpha(1) = 1$, то функция $\alpha(x) = 1$ - константа 1. Если $\alpha(1) = 0$, то $\alpha(x) = \overline{x}$.

Рассуждая аналогично, получим, что функция $\beta(x) = nt_1(x, \dots, x)$ будет или константой 0 или $\beta(x) = \overline{x}$.

Итак, мы можем иметь в $[A]$:

1) или обе константы,

2) или отрицание и одну константу (тогда, используя отрицание, можно получить вторую константу),

3) или только отрицание.

Пусть имеет место 3-й случай.

Рассмотрим функцию $ns(x_1, \dots, x_k)$. Существует бинарный набор $(a_1 a_2 \dots a_k)$, такой, что $ns(a_1, \dots, a_k) = ns(\overline{a_1}, \dots, \overline{a_k})$.

В функции $ns(x_1, \dots, x_k)$ подставим x вместо x_i, если $a_i = 1$, и подставим $\overline{x}$ вместо x_i, если $a_i = 0$, то есть мы подставляем x^{a_i} вместо x_i (мы использовали процедуры отождествления переменных и композиции, располагая функцией отрицания). Полученную функцию 1-й переменной обозначим $\gamma(x)$.

Заметим теперь, что

$\gamma(0) = ns(0^{a_1}, \ldots, 0^{a_k}) = ns(\overline{a_1}, \ldots, \overline{a_k}) = ns(a_1, \ldots, a_k) =$

$= ns(1^{a_1}, \ldots, 1^{a_k}) = \gamma(1).$

Поэтому $\gamma(x)$ - постоянная функция, константа 0 или 1. Имея одну константу и отрицание, мы можем получить вторую константу.

Пусть имеет место 1-й случай.

Итак, в $[A]$ имеется обе константы. Докажем теперь, что подстановкой в $nm(x_1, \ldots, x_k)$ вместо переменных констант или буквы x можно получить функцию отрицания.

Функция $nm(x_1, \ldots, x_k)$ не монотонная, значит найдутся бинарные наборы $(a_1 a_2 \ldots a_n) < (b_1 b_2 \ldots b_n)$, но

$nm(a_1, a_2, \ldots, a_n) = 1 > nm(b_1, b_2, \ldots, b_n) = 0.$

В функции $nm(x_1, \ldots, x_k)$ подставим x вместо x_i, если $a_i \neq b_i$, и в противном случае подставим константу равную a_i. Полученную функцию 1-й переменной обозначим $\delta(x)$.

Заметим теперь, что

$\delta(0) = nm(a_1, \ldots, a_k) = 1$, и $\delta(1) = nm(b_1, \ldots, b_k) = 0.$

Поэтому $\delta(x) = \overline{x}$.

Мы уже доказали, что в $[A]$ присутствуют обе константы и отрицание.

Рассмотрим теперь функцию $nl(x_1, \ldots, x_k)$.

Используя ее, константы и отрицание получим конъюнкцию.

Полином Жегалкина функции $nl(x_1, \ldots, x_k)$ содержит произведения хотя бы двух переменных. Пусть это будут переменные x_1 и x_2.

Тогда можно записать: $nl(x_1, \ldots, x_k) =$

$= x_1 x_2 \phi(x_3, \ldots, x_k) \oplus x_1 \psi(x_3, \ldots, x_k) \oplus x_2 \chi(x_3, \ldots, x_k) \oplus \varepsilon(x_3, \ldots, x_k).$

Функция $\phi(x_3, \ldots, x_k)$ не является константой 0, поэтому существует набор, где $\phi(a_3, \ldots, a_k) = 1$.

Положим $\omega(x_1, x_2) = nl(x_1, x_2, a_3 \ldots, a_k) =$

$= x_1 x_2 \oplus c_1 x_1 \oplus c_2 x_2 \oplus d = (x_1 \oplus c_2)(x_2 \oplus c_1) \oplus c_1 c_2 \oplus d.$

Тогда функция $f(x_1, x_2) = \omega(x_1 \oplus c_2, x_2 \oplus c_1) \oplus c_1 c_2 \oplus d = x_1 x_2.$

Мы использовали возможность подставлять константы и отрицание переменных оформляли как сложение по модулю 2 с единицей.

Нам удалось теперь доказать, что в $[A]$ присутствует отрицание и конъюнкция. Поэтому это множество булевых функций является функционально полным.

Теорема доказана.

Следствие. Если к любому классу Поста добавить любую функцию, не принадлежащую этому классу, мы получим функционально полное множество.

Доказательство. В любом классе Поста есть функции, не принадлежащие остальным классам Поста. Добавленная функция не принадлежит рассматриваемому классу Поста. Мы получили множество, целиком не лежащее ни в одном из 5 классов Поста, по теореме Поста это множество функционально полно.

Задачи к главе 3

1. Для булевой функции, заданной вектором ее значений $f(x,y,z) = (1\ 1\ 1\ 1\ 0\ 0\ 1\ 1)$выяснить какие ее переменные являются существенными.

Выразить эту функцию формулой, содержащей лишь существенные переменные.

Указание: использовать бинарный куб.

2. Для булевой функции заданной формулой $f(x,y,z) = x\overline{y}z \vee xy \vee x\overline{z} \vee \overline{x}z$ выяснить какие ее переменные являются существенными.

Выразить эту функцию формулой, содержащей лишь существенные переменные.

Указание: использовать бинарный куб.

3. Используя булевы функции, проверить, является ли выполнение включения $A \subseteq B \setminus C$ необходимым и достаточным условием выполнения равенства $A \cup C = (C \setminus A) \cup \big((A \cap B) \setminus C\big)$. Здесь A, B, C - произвольные множества.

4. Найти СДНФ, СКНФ и полином Жегалкина булевой функции $f(x,y,z) = (1\ 1\ 0\ 1\ 1\ 0\ 0\ 0)$.

5. Поставить на место звездочек в векторе значений булевой функции 0 или 1 так, чтобы доопределенная функция оказалась самодвойственной, $f(x,y,z) = (*\ 1\ 0\ *\ 0\ **\ 1)$.

6. Поставить на место звездочек в векторе значений булевой функции 0 или 1 так, чтобы доопределенная функция оказалась монотонной, $f(x,y,z) = (*\ 1\ ****\ 0\ *)$.

7. Поставить на место звездочек в векторе значений булевой функции 0 или 1 так, чтобы доопределенная функция оказалась линейной, $f(x,y,z) = (*\ 1\ *\ 1\ 1\ **\ 0)$.

8. Определить, является булева функция f = (11011010) шефферовой. Если она не шефферова, укажите все классы Поста, которым принадлежит функция.

9. Определить, является булева функция f = (01011010) шефферовой. Если она не шефферова, укажите все классы Поста, которым принадлежит функция.

10. Определить, является ли функционально полной заданная система трех булевых функций: f_1 = (01010111), f_2 = (10) и константа 1. В случае неполноты системы укажите все классы Поста, которым принадлежат все три функции.

11. Для булевых функций, используя бинарный куб, найти их минимальные ДНФ:

1) $f(x,y,z) = (1\ 1\ 1\ 1\ 1\ 0\ 1\ 0)$;

2) $f(x,y,z) = (1\ 0\ 1\ 0\ 1\ 0\ 1\ 1$;

3) $f(x,y,z) = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 1)$;

4) $f(x,y,z) = (0\ 1\ 1\ 1\ 1\ 1\ 1\ 0)$;

5) $f(x,y,z) = (0\ 1\ 1\ 0\ 1\ 1\ 0\ 1)$.

12. Для булевых функций, используя карту Карно, найти их минимальные ДНФ:

1) $f(x,y,z) = (1\ 1\ 1\ 1\ 1\ 0\ 1\ 0)$;

2) $f(x,y,z) = (1\ 0\ 1\ 0\ 1\ 0\ 1\ 1)$;

3) $f(x,y,z) = (0\ 1\ 1\ 0\ 1\ 0\ 0\ 1)$;

4) $f(x,y,z) = (0\ 1\ 1\ 1\ 1\ 1\ 1\ 0)$;

5) $f(x,y,z) = (0\ 1\ 1\ 0\ 1\ 1\ 0\ 1)$.

13. Для булевых функций, используя бинарный куб, найти их минимальные ДНФ:

1) $\phi(x,y,z,w) = (1001\ 1001\ 0110\ 0110)$;

2) $\psi(x,y,z,w) = (1111\ 1011\ 1110\ 0110)$.

14. Для булевых функций, используя карту Карно, найти их минимальные ДНФ:

1) $\phi(x,y,z,w) = (1001\ 1001\ 0110\ 0110)$;

2) $\psi(x,y,z,w) = (1111\ 1011\ 1110\ 0110)$.

ГЛАВА 4. ГРАФЫ

4.1. Основные понятия и определения

Определение. *Простой* (неориентированный) *граф* $G = (V, E)$ определяется заданием двух множеств V и E. Элементы первого множества V называют *вершинами* графа, а элементы второго множества E называют *ребрами* графа. В простом графе каждому ребру взаимно однозначно соответствует неупорядоченная пара различных вершин (концы ребра). Поэтому можно отождествить E с подмножеством множества всех неупорядоченных пар элементов V.

Если соответствие между ребрами и неупорядоченными парами вершин не взаимно однозначное, то есть у различных ребер могут быть одинаковые концы, то говорят о *мультиграфе*. E можно трактовать как мультимножество.

Если ребро может иметь одинаковые концы, то говорят о *псевдографе* или *графе с разрешенными петлями*.

Мы будем рассматривать лишь конечные графы, то есть множества V и E должны быть конечными.

Определение. В *ориентированном* (или *направленном*) графе, называемом также *орграфом*, элементам множества E ставятся во взаимно однозначное соответствие упорядоченные пары различных вершин, и элементы этого множества называют *дугами.* Тем самым для каждой дуги определена начальная и концевая вершина, можно сказать, что дуга имеет направление. Здесь уже возможны две дуги, соединяющие одну и ту же пару вершин, но в противоположных направлениях.

Граф может не иметь ребер (или дуг), но должен иметь хотя бы одну вершину.

На рисунках (рис. 4.1) вершины графа изображаются точками или кружками, ребра – линиями, соединяющими эти точки, для орграфов дуги изображают стрелками.

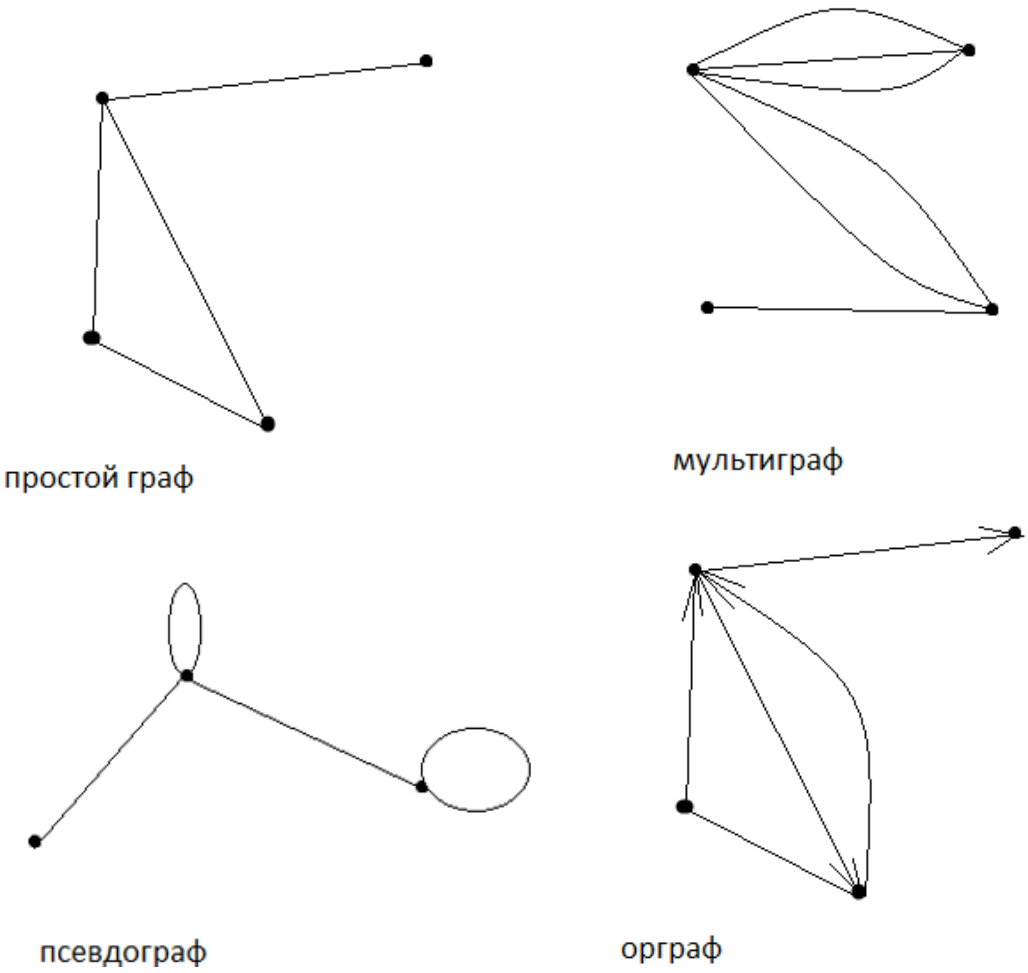


Рисунок 4.1

Матрица смежности

С каждым бинарным отношением на множестве вершин V можно связать ориентированный псевдограф, поскольку упорядоченные пары вершин, составляющие отношение – это и есть дуги псевдографа. Можно отождествить псевдограф и бинарное отношение на множестве V.

Для орграфа соответствующее бинарное отношение на V будет иррефлексивным, поскольку в орграфе отсутствуют петли.

Бинарное отношение на множестве $V = \{v_1, \ldots, v_n\}$ может быть задано матрицей M_G размера $n \times n$, состоящей из нулей и единиц. Элемент матрицы M_G, стоящий в i - ой строке и j - м столбце равен 1, если в отношении присутствует пара $(v_i\ v_j)$, или равен 0, если отсутствует. Поэтому и ориентированный псевдограф (а значит и просто орграф) может быть задан матрицей, построенной по указанному принципу. Эта матрица называется *матрицей смежности* данного *орграфа*, поскольку вершины, связанные ребром (или направленным ребром –

дугой) называются смежными вершинами.

Пример:

Построим матрицу смежности для следующего ориентированного псевдографа (рис. 4.2): $M_G = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 0 & 1 \end{pmatrix}$.

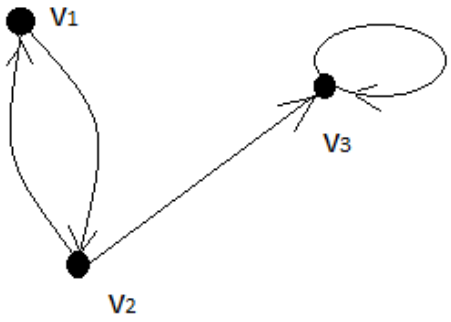


Рисунок 4.2

Рассмотрим теперь простые графы. Каждому простому графу взаимно однозначно соответствует орграф, имеющий то же множество вершин и имеющий две противоположно направленные дуги там, где простой граф имеет ребро. Соответствующее этому орграфу отношение будет иррефлексивно и симметрично, а матрица смежности для этого орграфа будет симметричной, а главная диагональ в ней будет состоять из нулей. Эта матрица называется также *матрицей смежности* рассматриваемого *простого графа*.

Пример. Построим матрицу смежности для следующего простого графа (рис. 4.3): $M_G = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$.

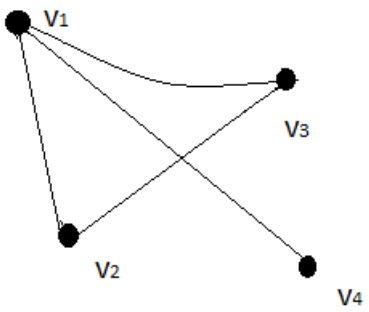


Рисунок 4.3

Степени вершин графа

Определение. Если вершина является концевой для некоторого ребра, то говорят, что эта вершина и это ребро *инцидентны*.

Степенью данной *вершины* простого графа называется количество ребер, инцидентных данной вершине. Обозначение: $deg(v)$.

Очевидно, что степень i - ой вершины графа равна сумме элементов i - ой строки матрицы этого графа.

В орграфе степень вершины является суммой *полустепени захода* (количество дуг, для которых эта вершина является концом) и *полустепени исхода* (количества дуг, для которых эта вершина является началом).

Типы графов

Определение. Простой граф с n вершинами называется *полным графом* и обозначается K_n, если в нем каждая пара вершин соединена ребром.

Примеры полных графов (рис. 4.4).

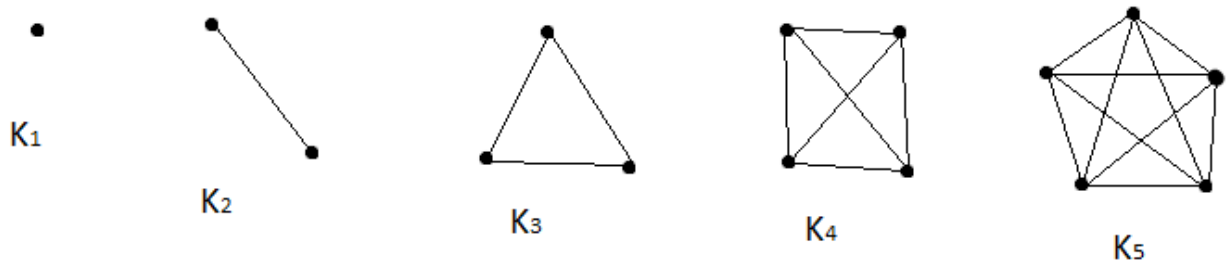


Рисунок 4.4

Определение. Простой граф с n вершинами, в котором нет ребер называется *пустым графом* и обозначается O_n.

Определение. Простой граф с множеством вершин $V = \{v_1, \ldots, v_n\}$, имеющий ребра $\{v_i, v_{i+1}\}$ для $i = 1, \ldots, n-1$, а также ребро $\{v_n, v_1\}$, называется *циклическим графом* и обозначается C_n (рис. 4.5).

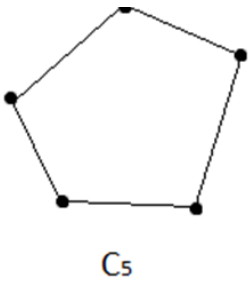


Рисунок 4.5

Определение. *Двудольным графом* называется простой граф, у которого множество вершин можно разбить на две непересекающиеся части $V = V_1 \cup V_2,\ V_1 \cap V_2 = \emptyset$ так, что все ребра этого графа соединяют лишь вершины из разных частей.

Полный двудольный граф $K_{m,n}$ – это двудольный граф, в котором для любой пары вершин из разных долей есть ребро, их соединяющее; в одной доле m вершин, в другой доле n вершин (рис. 4.6).

Рисунок 4.6

Изоморфизм графов. Подграфы

Определение. Два графа (орграфа, мультиграфа, псевдографа) $G_1 = (V_1, E_1)$ и $G_2 = (V_2, E_2)$ называются *изоморфными*, если существуют биекции $f_v: V_1 \to V_2$ и $f_E: E_1 \to E_2$, такие, что каждое ребро (дуга), соединяющее некоторые две вершины переходит при биекции $f_E: E_1 \to E_2$ в ребро (дугу), соединяющее образы этих вершин при биекции $f_v: V_1 \to V_2$.

Пример:

На рисунке (рис. 4.7) изображены два изоморфных графа.

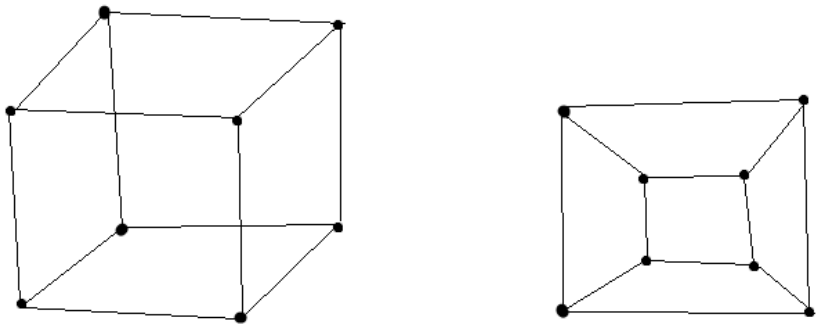


Рисунок 4.7

Определение. Если в простом графе взять некоторую часть вершин (можно и все вершины) и некоторые ребра, соединяющие взятые вершины, то тем самым можно образовать новый граф, который называется *подграфом* данного графа.

Если мы взяли в подграф все вершины исходного графа, то полученный подграф называется *остовным подграфом*.

Если в подграфе присутствуют все ребра исходного графа, соединяющие вершины подграфа, то говорят, что подграф *индуцирован* своим множеством вершин.

Определение. Подмножество множества вершин графа называется *кликой*, если индуцированный этим подмножеством вершин граф является полным графом. Для данного графа максимальная мощность клики называется *кликовым числом*.

Определение. Подмножество множества вершин графа называется *независимым подмножеством*, если индуцированный этим подмножеством вершин граф является пустым графом, то есть в исходном графе нет ребер, соединяющих вершины этого подмножества. Для данного графа максимальная мощность независимого подмножества вершин называется *числом независимости*.

Пример: Для графа, изображенного на предыдущем рисунке кликовое число равно 2, число независимости равно 4.

Проблема Келли-Улама

Каждый подграф рассматриваемого графа может быть получен удалением из исходного графа некоторых ребер и некоторых вершин (при удалении вершины нужно удалять все ребра ей инцидентные).

Проблема Келли-Улама формулируется так:

Для данного графа рассмотрим множество подграфов, получающихся удалением из графа каждой его вершины.

Существует ли два неизоморфных графа с числом вершин не меньше 3-х с одинаковыми получающимися семействами подграфов?

Проблема была поставлена в 1957 году, но по сей день остается нерешенной.

4.2. Связность графа

Определение. *Маршрут* в графе с начальной вершиной v_1 и конечной вершиной v_n определяется заданием последовательности вершин $v_1, v_2, \ldots, v_n$. Для каждой пары последовательных вершин этой последовательности в графе должно существовать ребро, их соединяющее. Эти ребра мы называем ребрами этого маршрута, и *длиной маршрута* называется количество ребер этого маршрута.

Цепью называется такой маршрут, в котором все ребра различные. *Простой цепью* называется цепь, в которой все вершины различны. В орграфе простая цепь называется *путём*.

Маршрут с совпадающими начальной и конечной вершиной называют *замкнутым*. Замкнутая цепь называется *циклом* (для орграфа используют термин *контур*). Цикл, в которой лишь начальная и конечная вершина совпадают, называется *простым циклом*.

Определение. Рассмотрим две вершины в простом графе. Скажем, что эти вершины *достижимы* друг от друга, если существует связывающий их маршрут, то есть маршрут с начальной первой вершиной и конечной второй вершиной.

Простой граф называется *связным*, если любые две вершины этого графа достижимы друг от друга.

Расстоянием между двумя вершинами связного графа назовем наименьшую длину маршрута, связывающего их.

Отношение достижимости на множестве всех вершин графа является отношением эквивалентности. Классы эквивалентности для этого отношения состоят вершин достижимых друг от друга. Индуцированные этими классами вершин подграфы называются *компонентами связности* данного простого графа.

Пример:

На рисунке (рис. 4.8) овалом обведен граф с шестью вершинами, имеющий 3 компоненты связности.

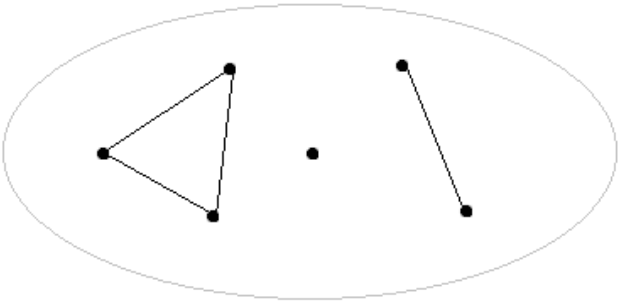


Рисунок 4.8

Теорема Кёнига. Простой граф является двудольным тогда и только тогда, когда в нем нет циклов нечетной длины.

Доказательство. Пусть граф двудольный. Рассмотрим любой цикл. Двигаясь по вершинам цикла, мы переходим из доли в долю и должны вернуться на место, это невозможно сделать нечетным числом шагов.

Пусть в графе нет циклов нечетной длины. Для каждой компоненты связности выберем и зафиксируем в ней любую вершину и отнесем в первую долю все

вершины, лежащие от этой фиксированной вершины на четном расстоянии, а во вторую долю – на нечетном.

Деревья. Леса

Определение. Связный граф, не имеющий циклов, называется *деревом* (рис. 4.9).

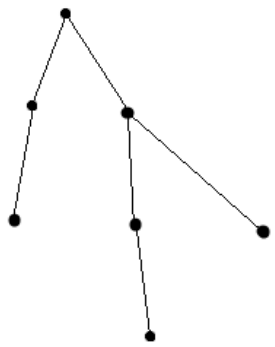


Рисунок 4.9

Определение. Вершина в простом графе, имеющая степень 1, называется *висячей вершиной.*

Утверждение. В любом дереве количество вершин на 1 больше количества ребер.

Доказательство. Рассмотрим любую простую цепь. В дереве нет циклов, поэтому, двигаясь по цепи мы достигнем висячей вершины.

Уберем из графа висячую вершину вместе с ребром, ей инцидентным. Полученный граф останется деревом. Разность между количеством вершин и ребер при этом не изменится. Будем продолжать эти действия до тех пор, пока не останется одна вершина. Значит разность между количеством вершин и ребер в исходном графе равнялась 1.

Утверждение. В любом дереве для любых двух различных вершин существует ровна одна цепь, связывающая их.

Доказательство. Дерево – связный граф, поэтому есть маршрут, связывающий две вершины, если на маршруте будут повторяющиеся вершины, то будет цикл, чего в дереве быть не может. Поэтому этот маршрут будет простой цепью.

Если найдется еще одна цепь, связывающая эти вершины, то из этих двух цепей образуется цикл, чего в дереве быть не может.

Утверждение. В любом связном графе существует остовной подграф, являющийся деревом.

Доказательство. Удаляя одно ребро в цикле, если таковой есть в графе, мы получаем остовной связный подграф. Повторяем эту операцию до тех пор, пока не исчезнут все циклы.

Определение. *Лесом* называется граф без циклов. Очевидно, что компоненты связности леса являются деревьями (рис. 4.10).

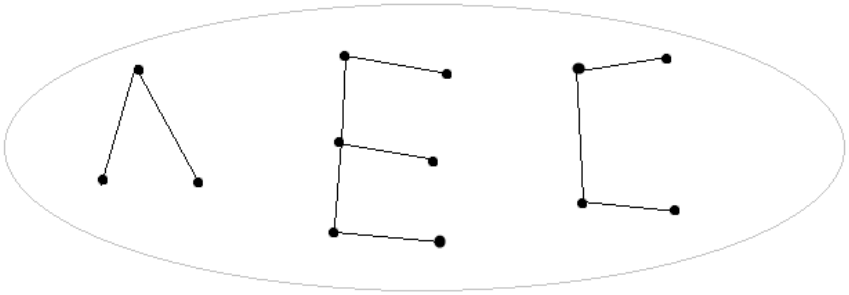


Рисунок 4.10

Поскольку в лесе нет циклов, а значит нет циклов нечетной длины, из теоремы Кёнига вытекает утверждение.

Утверждение. Всякий лес (в частности, дерево) является двудольным графом.

На простом графе, являющемся деревом, можно ввести так называемую *корневую структуру*, превратив его в орграф, следующим образом.

Любую вершину графа можно взять в качестве *корневой*. Для любой другой вершины существует единственная простая цепь, связывающая корневую вершину и эту вершину. Снабдим направлением ребра этой цепи, совпадающим с направлением движения по цепи от корневой вершины к этой вершине. Рассмотрев все другие вершины, мы дадим направление всем ребрам графа. Нетрудно показать, что предлагаемый алгоритм корректен – если по ходу его применения возникнет необходимость менять направление на уже снабженным направлением ребре, то будет получаться, что существует две несовпадающих простых цепей, связывающих одни и те же вершины, что невозможно.

В итоге получается орграф, в котором для всех вершин, кроме корневой, полустепень захода равна 1.

Пример: На рисунке приведены всевозможные корневые структуры на простом графе, являющимся деревом (рис. 4.11).

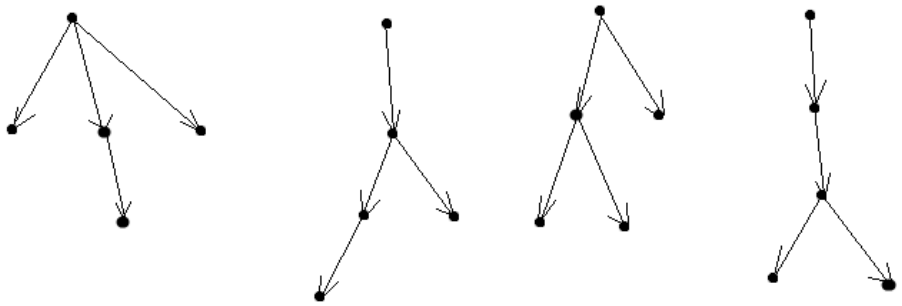


Рисунок 4.11

Замечание. Корневы деревья принято изображать корнем вверх и не отображать направление дуг орграфа, считая, что все дуги направлены сверху вниз.

4.3. Планарные графы

Определение. Граф называется *планарным*, если его можно изобразить на плоскости так, что ребра (изображенные кривыми линиями, соединяющими кружки, изображающие вершины) не будут пересекаться.

Пример:

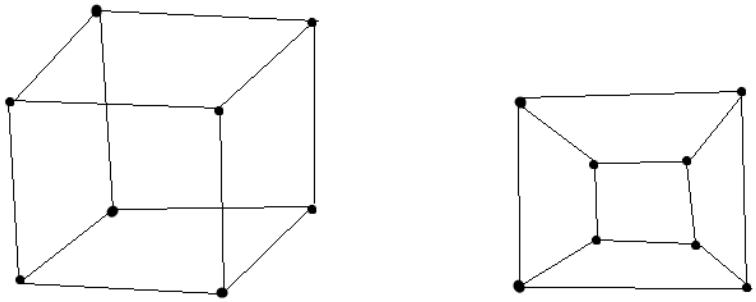


Рисунок 4.12

На этом рисунке два изображения одного и того же графа (рис. 4.12). Как видно из правого изображения, рассматриваемый граф является планарным.

Непланарность некоторых графов можно установить, опираясь на теорему, которую сформулировал и доказал О. Коши при доказательстве теоремы Эйлера о выпуклых многогранниках.

Теорема Эйлера о выпуклых многогранниках (1750 год)

Для любого выпуклого многогранника выполнено равенство:

$$В + Г = Р + 2,$$

где В – число вершин, Г – число граней, Р – число ребер.

О. Коши в 1811 году вывел теорему Эйлера из сформулированной и доказанной им теоремы о плоских графах.

Планарный связный граф, можно изобразить на плоскости. Естественным образом можно ввести понятие грани как области, ограниченной изображениями вершин и ребер.

Для плоского графа докажем формулу: $B + Г = P + 1$.

Пусть в графе есть цикл. Уберем одно ребро из цикла. Число ребер и число граней уменьшится на 1.

Повторяем это действие до тех пор, пока граф не превратится в дерево. Для дерева доказываемая формула, очевидно, выполнена. Поэтому она выполнена и для исходного графа, поскольку мы убрали равное число ребер и граней.

Заметим, что формула остается верной и для любого, не обязательно связного планарного графа, поскольку она верна для каждой компоненты связности.

Из доказанной формулы для планарного графа вытекает формула Эйлера для многогранников. Можно, считая ребра резиновыми, растянуть в стороны одну из граней многогранника, после чего уложить его на плоскость. В результате растянутая грань исчезнет, и вопрос сведется к рассмотрению плоского графа.

Для удобства дальнейших рассмотрений добавим еще одну грань для плоского графа: она будет состоять из точек плоскости, расположенных снаружи от изображения графа.

Итак, формула для плоского графа примет вид: $B + Г = P + 2$.

Утверждение. Граф K_5 не планарный.

Доказательство. Для этого графа В=5, Р=10. Если бы он был планарным, было бы выполнено равенство $B + Г = P + 2$. Тогда было бы Г=7.

Вычислим число инциденций типа грань-ребро.

Каждая грань инцидентна не менее 3-м ребрам, поэтому число инциденций не менее 21. С другой стороны, каждое ребро инцидентно не более 2-м граням, поэтому число инциденций не более 20. Противоречие. Значит, граф K_5 не планарный.

Аналогично доказывается следующее утверждение.

Утверждение. Граф $K_{3,3}$ не планарный.

Замечание. Широко известна интерпретация этого утверждения как невозможность протоптать непересекающиеся тропинки от трех домов к трем колодцам.

Определение. Процедура *подразбиения ребра* для графа состоит в добавлении вершины на этом ребре, разбивающей ребро на два ребра (рис. 4.13).

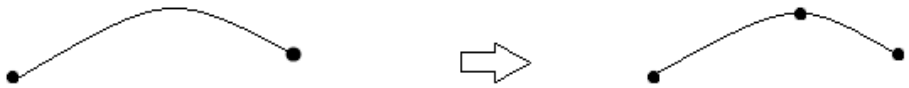


Рисунок 4.13

Теорема Куратовского (критерий планарности графа)

Простой граф планарен тогда и только тогда, когда он не содержит подграфов, которые получаются из K_5 или $K_{3,3}$ подразбиением ребер.

Замечание. Рассмотренную теорему некоторые авторы называют теоремой Понтрягина – Куратовского. Эта теорема была опубликована К.Куратовским в 1930 году. В этой же публикации, в примечании, сам Куратовский написал, что, как сообщил ему П.С. Александров, этот критерий получил в 1927 году Л.С. Понтрягин. Сам Понтрягин никаких публикаций по этой теме ни тогда, ни позже не делал.

4.4. Эйлеровы и гамильтоновы графы

Эйлеровы графы

Определение. Граф называют *эйлеровым*, если можно, выйдя из одной вершины, двигаясь по ребрам, вернуться обратно, пройдя по каждому ребру ровно один раз.

Более формально: цепь в графе назовем *эйлеровой цепью*, если в ней присутствуют все ребра графа. Цикл, являющийся эйлеровой цепью, называется *эйлеровым циклом*. Итак, граф будет эйлеровым, если для него существует эйлеров цикл.

Замечание. В 18 веке Л. Эйлер поставил и решил вопрос о возможности, выйдя из одного места, пройти по семи Кёнигсбергским мостам по одному разу и вернуться обратно. Эйлер доказал невозможность такой прогулки, по сути он доказал неэйлеровость соответствующего графа. Считается, что с этой работы Эйлера началась абстрактная теория графов.

Существует простой критерий эйлерововости графа.

Теорема Эйлера. Для того, чтобы связный граф был эйлеровым необходимо и достаточно, чтобы степени всех его вершин были четными. Критерий работает и для мультиграфа.

Доказательство. Если граф эйлеров, в нем есть эйлеров цикл. Пройдем по эйлеровому циклу снабжая ребра направлениями. Тогда в получившемся орграфе для каждой вершины полустепень захода будет, очевидно, равна полустепени исхода, поэтому степени всех вершин будут четными.

Пусть теперь в связном графе степени всех вершин четные. Построим эйлеров цикл.

Стартуя из любой вершины, двинемся по любому ребру, и с следующей вершины продолжим движение по любому другому ребру (степень четная, поэтому есть другое ребро) и так далее до тех пор, пока не вернемся в исходную вершину.

Если мы прошли все ребра, эйлеров цикл построен. Если нет, ввиду связности графа найдется вершина в пройденном цикле, для которой есть инцидентные ей ребра, еще не пройденные нами (причем четное число).

Стартуем теперь из этой вершины, двигаясь лишь по не пройдённым нами ребрам до тех пор, пока не вернемся в эту вершину. Получим второй цикл.

Соединим два цикла в один, как показано на рисунке красным цветом (рис. 4.14).

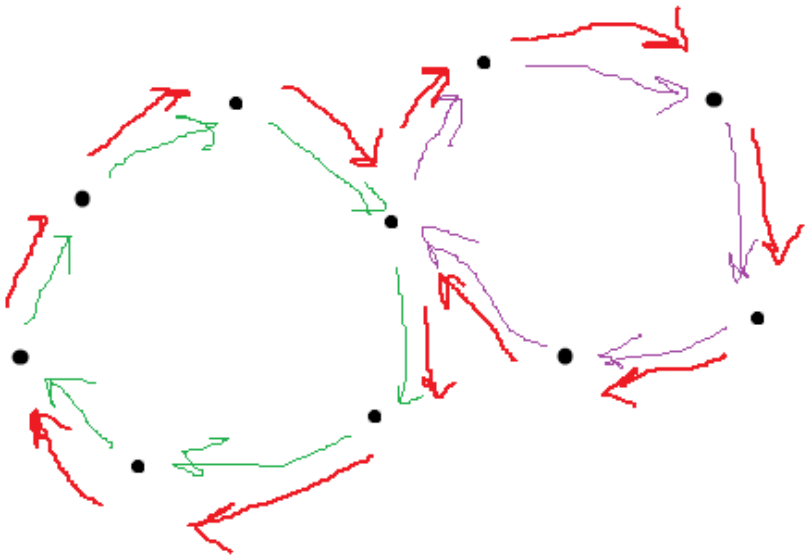


Рисунок 4.14

Для простоты мы изобразили случай, когда два цикла имеют лишь одну общую вершину, но это, как нетрудно понять не существенно.

Теперь, если расширенный цикл включает в себя все ребра эйлеров цикл построен. В противном случае продолжаем таким же образом расширять цикл.

Теорема доказана.

Имеет место теорема, являющаяся критерием существования эйлеровой цепи (то есть нам нужно пройти по всем ребрам по разу, но возвращаться обратно не обязательно.

Теорема. Эйлерова цепь в связном графе (мультиграфе) существует только тогда, когда степени всех вершин четные или в графе ровно две вершины имеют нечетную степень.

Доказательство. Действуя как в доказательстве теоремы Эйлера, начнем с цепи, связывающей вершины, имеющие нечетную степень. Такая существует ввиду связности графа и четности степеней остальных вершин. Далее удлиняем цепь, действуя как в доказательстве теоремы Эйлера.

Пример

На рисунке порядок ребер в эйлеровой цепи указан номерами (рис. 4.15).

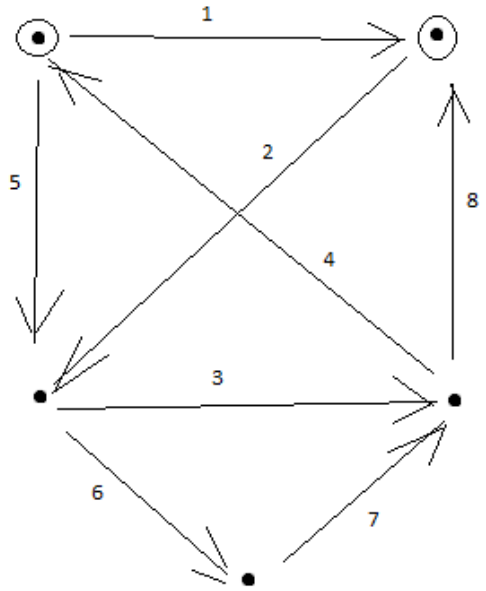


Рисунок 4.15

Гамильтоновы графы

Определение. Граф называют *гамильтоновым*, если можно, выйдя из одной вершины, двигаясь по ребрам, вернуться обратно, пройдя через каждую вершину ровно один раз. Итак, граф гамильтонов, если для него существует простой цикл, содержащий все вершины графа.

Простая цепь, содержащая все вершины графа, называется гамильтоновой цепью.

Замечание. Великий ученый В. Гамильтон в середине 19 века изобрел игру (головоломку) «Икосиан». В ней требовалось, двигаясь по ребрам додекаэдра от

вершины к вершине, пройдя по одному по одному разу через каждую вершину, вернуться на место. Эта игра была побочным результатом созданного Гамильтоном исчисления икосианов, алгебраической теории сходной с теорией кватернионов того же Гамильтона, положившей начало современной линейной алгебре (именно там возникли понятия вектора, скаляра, векторного произведения, скалярного произведения).

Примерами гамильтоновых графов могут служить графы ребер и вершин всех правильных многогранников (Платоновых тел): тетраэдра, куба, октаэдра, додекаэдра, икосаэдра.

Граф многомерного куба любой размерности также является гамильтоновым.

Утверждение. Граф вершин и одномерных ребер многомерного куба любой размерности является гамильтоновым.

Доказательство

Расположим куб в n - мерном пространстве, его вершины будут вершинами бинарного куба $\mathbf{B}^n = \mathbf{B} \times \mathbf{B} \times \ldots \times \mathbf{B} = \{(x_1; x_2; \ldots, x_n): x_i \in \mathbf{B}\}$.

Проведем индуктивное доказательство.

Граф 0-мерного куба, состоящего из одной точки, очевидно, гамильтонов.

Пусть мы умеем строить гамильтонов цикл на графе n - мерного куба. Рассмотрим $(n+1)$ - мерный куб. Точки, имеющие последнюю координаты равную нулю, являются вершинами n -мерного куба. Пусть $v_1, \ldots, v_{2^n}$ - гамильтонов цикл на этом кубе. Для каждого $i = 1, \ldots, 2^n$ обозначим $v_i^{'}$ вершину $(n+1)$ - мерного куба, имеющую n первых координат, такие же как у вершины v_i, а последнюю координату, равную единице.

Гамильтонов цикл на $(n+1)$ - мерном кубе образует следующая последовательность вершин: $v_1, \ldots, v_{2^n}, v_{2^n}^{'}, \ldots, v_1^{'}$.

На рисунке (рис. 4.16) проиллюстрирован переход от 2-мерного к 3-мерному случаю.

Утверждение доказано.

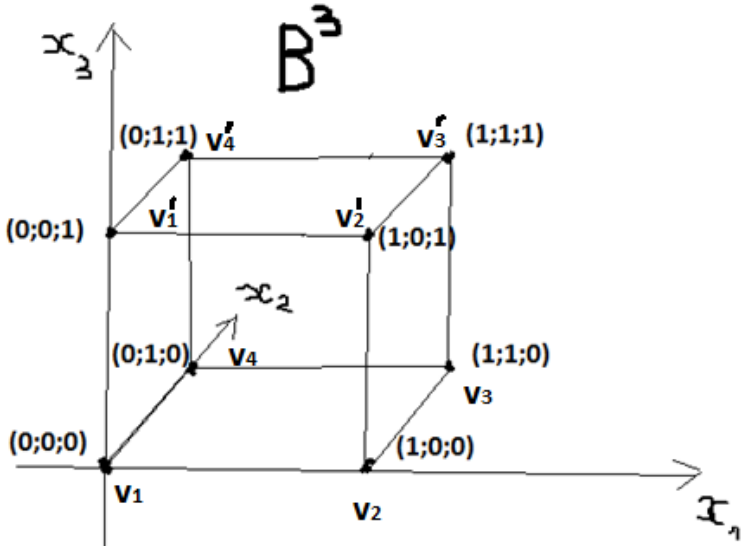


Рисунок 4.16

Замечание. В процессе доказательства мы указали алгоритм построения, широко применяемого *кода Грея*. Код Грея – это такой порядок на бинарных наборах длины n, что два соседних набора (а также первый и последний набор – порядок циклический) отличаются только в одной цифре.

Последовательность наборов координат вершин бинарного куба, перечисляемая в порядке прохода гамильтонова цикла, упорядочивается как в коде Грея. Это происходит потому, что смежные вершины графа являются концами одного ребра куба и поэтому отличаются лишь в одной координате.

Имеет место очевидное утверждение.

Утверждение. Полный граф K_n для $n \geq 3$ является гамильтоновым.

Установить гамильтоновость или ее отсутствие у произвольного графа является не столь простой задачей как установление эйлеровости. Не известно простых критериев гамильтоновости, а все известные алгоритмы являются неэффективными в том смысле, что трудоемкость их быстро возрастает с ростом числа вершин рассматриваемого графа.

Теорема Бонди-Хватала (1972 год). Граф с n вершинами будет гамильтоновым тогда и только тогда, когда его замыкание будет гамильтоновым.

Замыкание графа состоит в присоединении (до тех пор, пока это будет возможно) ребер, соединяющих несмежные вершины, у которых сумма степеней не меньше n.

Поскольку полный граф гамильтонов, из теоремы Бонди-Хватала вытекают более ранние теоремы Дирака и Оре.

Теорема Дирака (1952 год). Простой граф с n вершинами ($n \geq 3$) будет гамильтоновым, если степень каждой вершины не меньше $\frac{n}{2}$.

Теорема Оре (1960 год). Простой граф с n вершинами ($n \geq 3$) будет гамильтоновым, если для каждой пары несмежных вершин сумма их степеней не меньше n.

4.5. Описание классов графов с помощью запрещенных миноров

Определение. Простой граф H называется *минором* простого графа G, если он может быть получен из графа G удалением вершин (вместе с инцидентными им ребрами), удалением ребер и *стягиванием ребер*.

Процедура стягивания ребра состоит в удалении этого ребра и отождествлении вершин, являющихся концами этого ребра. Если после этой процедуры возникает мультиграф, то кратные ребра, соединяющие одну и ту же пару вершин, заменяют на одно ребро.

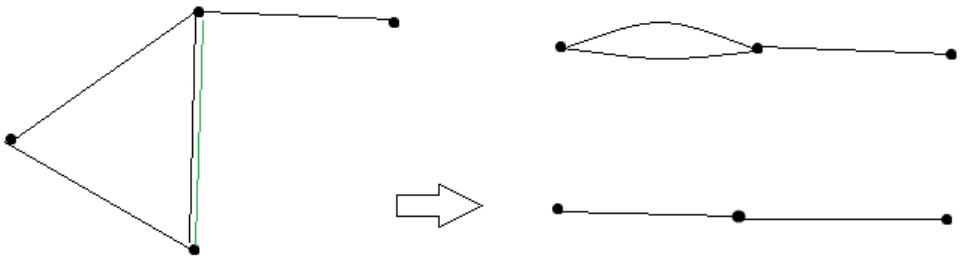


Рисунок 4.17

На рисунке (рис. 4.17) стянуто помеченное зеленым ребро. Результат справа внизу.

Таким образом, понятия минора графа является обобщением понятия подграфа.

Теория запрещенных миноров началась с теорем К. Вагнера, опубликованных в 1937 году.

Теорема 1 Вагнера. Простой граф планарен тогда и только тогда, когда у него нет миноров изоморфных K_5 или $K_{3,3}$.

Эта теорема равносильна полученной ранее теореме Куратовского.

Теорема 2 Вагнера. Простой 4- связный граф планарен тогда и только тогда, когда у него нет миноров изоморфных K_5.

Граф 4-связен, если он остается связным после удаления из него менее 4-х любых вершин.

Обе теоремы являются теоремами, в которых описание классов файлов задается указанием запрещенных миноров.

Определение. Класс графов замкнут относительно операции взятия миноров, если всякий граф, являющийся минором графа из этого класса, тоже принадлежит этому классу.

Пример: Класс планарных графов.

Теорема Робертсона-Сеймура. Всякий класс графов, замкнутый относительно операции взятия миноров, может быть описан конечным набором запрещенных миноров.

То есть, для данного класса графов существует такой набор запрещенных графов, что граф G принадлежит рассматриваемому классу тогда и только тогда, когда он не содержит в качестве минора ни один из запрещенных графов.

Робертсон и Сеймур опубликовали доказательство этой теоремы в серии из 20 статей с 1983 по 2004 годы.

4.6. Раскраска графов

Припишем вершинам графа цвета, то есть как бы покрасим каждую вершину каким-то цветом из фиксированного набора цветов. Возникает вопрос: какое минимальное число цветов необходимо для того, чтобы любые две смежные вершины имели различные цвета?

Определение. *Хроматическим числом* графа G называется наименьшее число цветов, которыми можно раскрасить вершины графа, так чтобы смежные вершины были окрашены разным цветом.

Обозначение: $\chi(G)$.

Знаменитая *проблема (гипотеза) четырех красок* может быть сформулирована так: для всякого планарного графа $\chi(G) \leq 4$.

Проблема была поставлена в 70-е годы 19 века, но лишь в 1976 году Аппель и Хакен доказали, что четырех красок достаточно, сведя вопрос к конечному перебору случаев, который осуществили с помощью вычислительной машины.

Гипотеза Хадвигера. Если $\chi(G) = n$, то существует минор этого графа, изоморфный полному графу K_n.

Вопрос поставлен в 1943 году, но до сих пор это утверждение не доказано и не опровергнуто.

Теория Рамсея

Теорема Рамсея (1930 год). Для любых двух натуральных чисел m и n существует натуральное число $R(m,n)$, такое, что при любой раскраске в два цвета ребер полного графа с числом вершин не меньшим $R(m,n)$ в этом графе либо найдется клика K_m с ребрами 1-го цвета, либо найдется клика K_n с ребрами 2-го цвета.

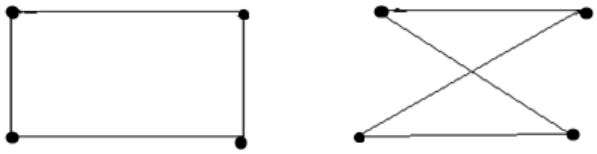
Конкретные значения чисел Рамсея $R(m,n)$ известны лишь для немногих m и n. Например, точное значение $R(5,5)$ пока неизвестно (известен диапазон $43 \le R(5,5) \le 48$).

Известно, что $R(3,3) = 6$. Это можно трактовать так: в любой группе из 6 человек либо найдется тройка попарно знакомых людей, либо тройка попарно незнакомых.

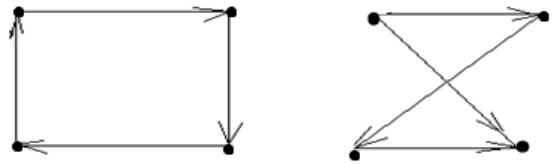
Задачи к главе 4

1. Установить, изоморфны ли изображенные два графа (орграфа) (рис. 4.18).

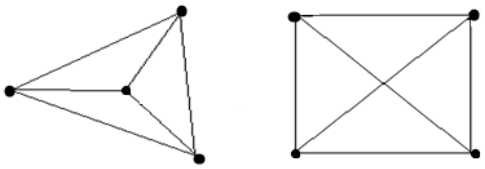
1)



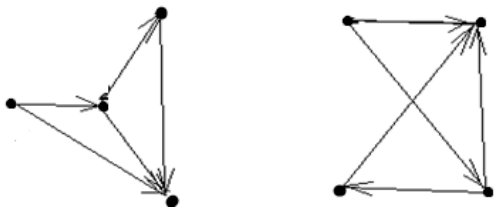
2)



3)



4)



5)

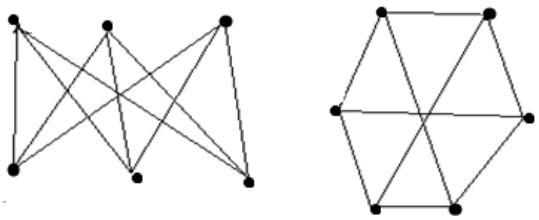


Рисунок 4.18

2. Перечислите все неизоморфные между собой подграфы данного графа (рис. 4.19).

1) 2)

Рисунок 4.19

3. Перечислите все неизоморфные между собой подграфы данного орграфа (рис. 4.20).

1) 2)

Рисунок 4.20

4. Найдите кликовое число графа (рис. 4.21).

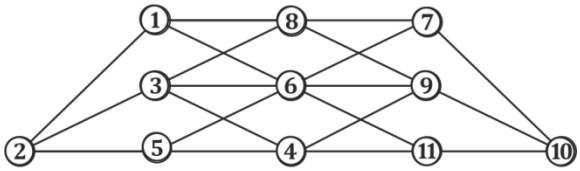


Рисунок 4.21

5. Найдите число независимости графа (рис. 4.22).

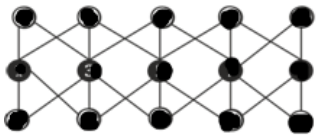


Рисунок 4.22

6. Запишите матрицу смежности графа (рис. 4.23).

1) 2)

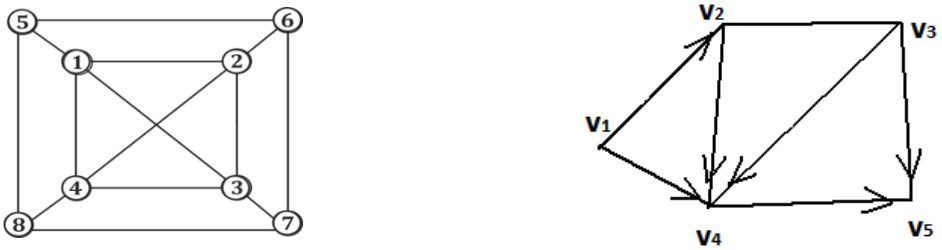


Рисунок 4.23

7. Найдите любое остовное дерево графа (рис. 4.24).

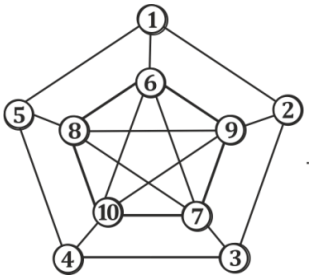


Рисунок 4.24

8. Доказать, что граф не является планарным (рис. 4.25).

1) 2)

Рисунок 4.25

9. Доказать, что граф Петерсена не является планарным (рис. 4.26).

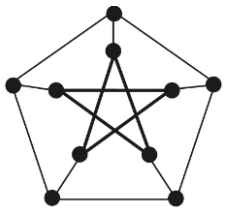


Рисунок 4.26

10. Является ли граф планарным (рис. 4.27)?

1) 2)

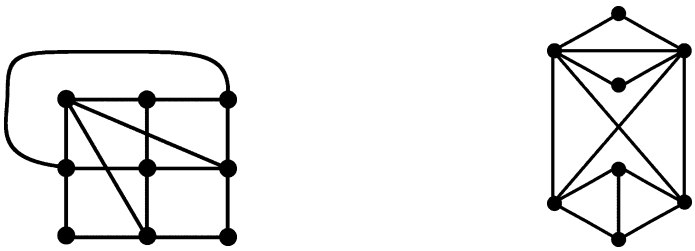


Рисунок 4.27

11. Найти эйлеров цикл на графе (рис. 4.28).

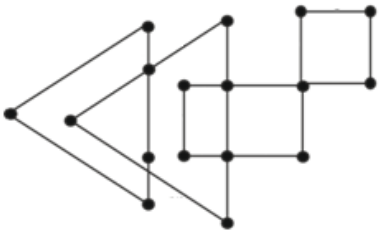


Рисунок 4.28

12. Найдите эйлерову цепь на графе (рис. 4.29).

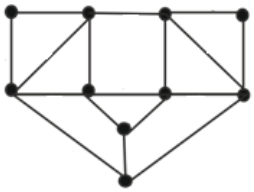
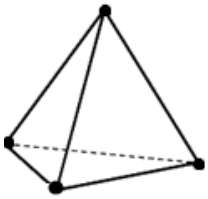


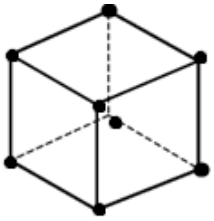
Рисунок 4.29

13. Проверьте, что графы вершин и ребер правильных многогранников являются гамильтоновыми (рис. 4.30).

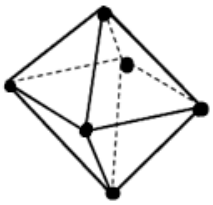
1) Тетраэдр



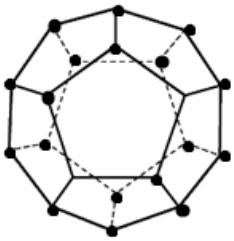
2) Куб



3) Октаэдр



4) Додекаэдр



5) Икосаэдр

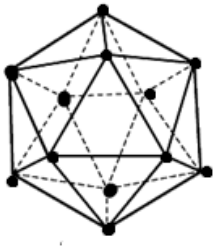


Рисунок 4.30

ЛИТЕРАТУРА

1. Александров П.С. Введение в теорию групп. М.: URSS, 2010.

2. Андерсон Дж. А. Дискретная математика и комбинаторика. М.: Вильямс, 2004.

3. Гаврилов Г.П., Сапоженко А.А. Задачи и упражнения по курсу дискретной математики. М.: Наука, 2004.

4. Грэхем Р., Кнут Д., Паташник О. Конкретная математика. М.: Мир, 1998.

5. Зуев Ю.А. Современная дискретная математика: От перечислительной комбинаторики до криптографии XXI века. М.: ЛЕНАНД, 2019.

6. Кнут Д. Искусство программирования. Т. 1. М.: Вильямс, 2000.

7. Лупанов О.Б. Курс лекций по дискретной математике. М.: МГУ, 2006.

8. Харари Ф. Теория графов М.: Книжный дом «Либроком»/URSS, 2009.

СВЕДЕНИЯ ОБ АВТОРАХ

Выборнов Александр Николаевич, к. ф.-м. н., доцент кафедры высшей математики ИКБ;

Ветренко Екатерина Александровна, к. т.н., доцент кафедры высшей математики ИКБ.