Министерство образования Республики Беларусь

Учреждение образования
«Гомельский государственный технический
университет имени П. О. Сухого»

Кафедра «Высшая математика»

А. А. Бабич

ДИСКРЕТНАЯ МАТЕМАТИКА

КУРС ЛЕКЦИЙ
по одноименной дисциплине для студентов инженерно-технических специальностей заочной формы обучения

Электронный аналог печатного издания

Гомель 2010

УДК 519.854(075.8)
ББК 22.176я73
Б12

Рекомендовано к изданию научно-методическим советом факультета автоматизированных и информационных систем ГГТУ им. П. О. Сухого
(*протокол № 1 от 14.09.2009 г.*)

Рецензент: канд. физ.-мат. наук, доц. *Л. Л. Великович*

Бабич, А. А.

Б12 Дискретная математика : курс лекций по одноим. дисциплине для студентов инженер.-техн. специальностей заоч. формы обучения / А. А. Бабич. – Гомель : ГГТУ им. П. О. Сухого, 2010. – 64 с. – Систем. требования: PC не ниже Intel Celeron 300 МГц ; 32 Mb RAM ; свободное место на HDD 16 Mb ; Windows 98 и выше ; Adobe Acrobat Reader. – Режим доступа: http://lib.gstu.local. – Загл. с титул. экрана.

ISBN 978-985-420-951-7.

Изложены элементы теории конечных множеств, основные сведения комбинаторного анализа, теории алгебр и групп, математической логики, булевых функций, теории графов. Подготовлен в соответствии с программой курса «Дискретная математика».

Для студентов инженерно-технических специальностей заочной формы обучения.

УДК 519.854(075.8)
ББК 22.176я73

ISBN 978-985-420-951-7

ПРЕДИСЛОВИЕ

Настоящее издание представляет собой курс лекций по дисциплине «Дискретная математика» и предназначено главным образом для студентов инженерно-технических специальностей заочной формы обучения. Данный курс лекций охватывает все основные разделы, которые обычно включаются в данную дисциплину, и разбит на 8 лекций. При написании пособия автор основывался на опыте преподавания дискретной математики для студентов различных специальностей, в том числе и для студентов специальности 1-40 01 73 «Программное обеспечение информационных систем», получающих вторую специальность на базе высшего образования на факультете повышения квалификации и переподготовки кадров.

Отбор материала учитывает тот факт, что введение дискретной математики как самостоятельной дисциплины в образовательные стандарты по техническим специальностям связано с широким развитием информационных технологий. Основные дисциплины, в которых используются методы дискретной математики, так или иначе имеют отношение к разработке систем автоматического проектирования и управления, вычислительных устройств и комплексов. Поэтому помимо лекций по фундаментальным основам дискретной математики в курс включены лекции, имеющие прикладную направленность.

При использовании пособия студенты должны понимать, что содержание курса «Дискретной математики» зависит от конкретной специальности, и в зависимости от учебных программ некоторые разделы могут быть опущены. Кроме этого, в силу ограниченного объема курса, изложение материала не является полным (особенно это касается лекции по теории графов), большинство теорем и результатов приведены без доказательств. Студентам, которые хотят более глубоко изучить дисциплину, автор советует обратиться к специальной литературе. Ссылки на некоторые книги и учебники по разделам дискретной математики можно найти в конце издания.

Тем не менее, данная книга содержит весь необходимый для подготовки к экзаменам и зачетам теоретический материал для студентов-заочников всех специальностей. Автор надеется, что самостоятельное изучение и разбор решений примеров и задач, приведенных в лекциях, вместе с усердной работой на семинарских занятиях достаточны для освоения курса и выполнения итоговых контрольных работ.

ЛЕКЦИИ 1–2
МНОЖЕСТВА И ОТНОШЕНИЯ

Множество – набор, совокупность, собрание каких-либо объектов, обладающих общим для всех них характеристическим свойством. Сами объекты при этом называются ***элементами множества***.

Обозначения:

– $A, B, C, \ldots, M, \ldots$ – множества;

– $a, b, c, \ldots, x, y, \ldots$ – элементы множества;

– $x \in M$ – x принадлежит множеству;

– $x \notin M$ – x не принадлежит множеству.

Замечание. Элементы множества должны быть принципиально различимы, т. е. должна существовать процедура выделения характеристического свойства.

Множества бывают *конечными* или *бесконечными*. В компьютерных расчетах все множества конечны в силу ограниченности объема памяти ячеек.

Способы задания множеств:

– списком $M = \{a_1, a_2, ..., a_n\}$;

– характеристическим свойством (предикатом) $M = \{x \,|\, P(x)\}$;

– порождающей процедурой $M = \{x \,|\, f\}$.

Пример

Задать множество первых десяти натуральных чисел.

1) $M_{10} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ – список;

2) $M_{10} = \{n \,|\, n \in \boldsymbol{N}, n \le 10\}$ – характеристическое свойство;

3) $M_{10} = \{n \,|\, 1 \in M_{10}, \text{если } k \in M_{10}, \text{то } n = k + 1,\ n \le 10\}$ – порождающая процедура.

Важно при задании характеристического свойства иметь разрешающую процедуру.

В любом приложении теории множеств заранее понятна природа объектов, которые объединяются в множества. Все такие объекты объединяются в одно понятие – ***универсальное множество*** или ***универсум*** U.

Пример

1. Для планиметрии U – множество точек плоскости.

2. Для численных расчетов U – множество чисел ($\boldsymbol{N}$, $\boldsymbol{Z}$, $\boldsymbol{Q}$, $\boldsymbol{I}$, $\boldsymbol{R}$ или $\boldsymbol{C}$).

Определение 1. Множество, которое не содержит элементов, называется **пустым множеством** $\varnothing$.

Замечание. Понятие пустого множества $\varnothing$ вводится для удобства. Так, если не обнаружены элементы, удовлетворяющие некоторому условию, то удобнее говорить о пустом множестве, о пустых ячейках, чем о несуществовании множества.

Множества $\varnothing$ и U тесно связаны друг с другом. Без задания универсального множества U невозможно говорить о пустом множестве $\varnothing$.

Пример

Рассмотрим множество $M = \{x \mid 3x^2 - 10x + 5 = 0\}$.

Пусть $U = \boldsymbol{Z}$, тогда $M = \varnothing$.

Пусть $U = \boldsymbol{R}$, тогда $M = \left\{\frac{5-\sqrt{10}}{3};\ \frac{5+\sqrt{10}}{3}\right\}$.

Определение 2. Если каждый элемент множества A содержится в множестве B, то A называется **подмножеством *B***. При этом пишут $A \subseteq B$.

По определению пустое множество $\varnothing$ есть подмножество всякого множества: $\varnothing \subseteq M$, в том числе и пустого.

Определение 3. Два множества A и B называются равными тогда и только тогда, когда они содержат одни и те же элементы (принцип равенства множеств).

Принцип равенства всегда применим к конечным множествам. Однако для бесконечных множеств он становится формальным, так как невозможно перебрать бесконечное число элементов.

Определение 4. Если $A \subseteq B$ и $A \neq B$, то A называется **собственным подмножеством B**. При этом пишут $A \subset B$.

У любого множества есть два несобственных подмножества: пустое множество $\varnothing$ и само множество.

Множества сами по себе могут быть объектами, которые собираются в группы, т. е. в другие множества. При этом необходимо различать типы включений – включение элементов и включение подмножеств в множество.

Пример

Пусть $D = \{d_1, d_2, ..., d_{11}\}$ – футбольная команда «Динамо».

Пусть $L = \{A, B, C, D, E, F, G, H\}$ – множество команд высшей лиги.

Тогда $D \in L$ – верно; $D \subset L$ – не верно; $\{D\} \subset L$ – верно.

Теорема 1. Справедливы следующие свойства включения подмножеств:

1) $\varnothing \subseteq A \subseteq U$;

2) $A \subseteq A$;

3) $A \subseteq B$, $B \subseteq C \Rightarrow A \subseteq C$;

4) $A \subseteq B$, $B \subseteq A \Rightarrow A = B$.

Докажем, например, 4.

Доказательство (от противного)

Пусть $A \neq B$. Тогда всегда найдется элемент x такой, что он принадлежит A, но не принадлежит B или наоборот. Но если $x \in A$, $x \notin B$, то нарушается включение $A \subseteq B$. Если $x \notin A$, $x \in B$, то нарушается другое включение $B \subseteq A$. Таким образом, наша гипотеза противоречит начальным условиям. Следовательно, $A = B$.

Что и требовалось доказать.

Четвертое утверждение позволяет устанавливать равенство множеств путем проверки прямого и обратного включений. Это основной метод доказательства теоретико-множественных соотношений.

Определение 5. Пусть A – некоторое множество. Совокупность всех подмножеств множества A называется его **булеаном** $B(A)$.

Пример

Пусть $A = \{x, y, z\}$. Тогда его булеан содержит 8 элементов:

$$B(A) = \{\varnothing, \{x\}, \{y\}, \{z\}, \{x, y\}, \{x, z\}, \{y, z\}, A\}.$$

Теорема 2. Пусть A – некоторое множество, содержащее n элементов. Тогда булеан $B(A)$ содержит 2^n элементов.

Доказательство

Занумеруем элементы множества $A = \{a_1, a_2, ..., a_n\}$. Тогда каждому подмножеству A можно поставить в соответствие единственным образом набор двоичных чисел:

$$(\alpha_1, \alpha_2, ..., \alpha_n), \text{ где } \alpha_i = 0 \text{ или } 1.$$

Если элемент a_i входит в подмножество, то $\alpha_i = 1$, если нет, то $\alpha_i = 0$. В частности:

$$(0, 0, ..., 0) \Rightarrow \varnothing; \quad (1, 1, ..., 1) \Rightarrow A \text{ и т. д.}$$

Для каждой позиции имеется всего две возможности – 0 или 1. Поэтому число всех таких наборов длины n равно

$$N = \underbrace{2 \cdot 2 \cdot ... \cdot 2}_{n \text{ раз}} = 2^n.$$

Что и требовалось доказать.

Определение 6. Число элементов конечного множества A называется его **мощностью** или **порядком** и обозначается как $|A|$.

Таким образом, согласно теореме 2 справедлива формула

$$|B(A)| = 2^{|A|}. \qquad (1)$$

Определение 7. Над множествами вводятся следующие операции:

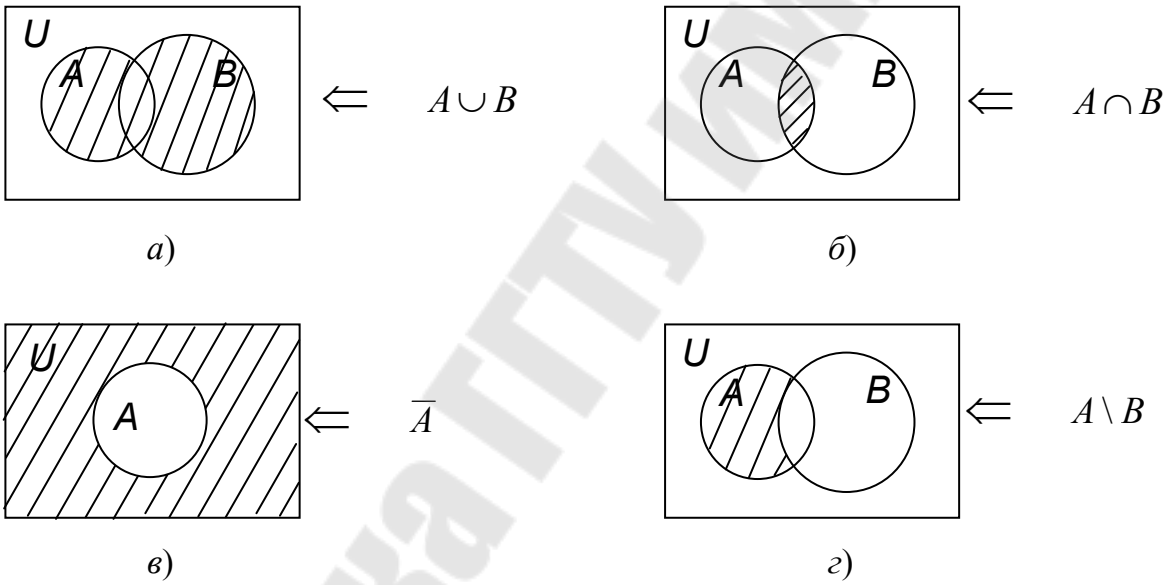
– объединение – $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$;

– пересечение – $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$;

– разность – $A \setminus B = \{x \mid x \in A \text{ и } x \notin B\}$;

– дополнение – $\overline{A} = U \setminus A = \{x \mid x \notin A\}$.

Для графического изображения операций удобны диаграммы Венна (рис. 1).



а) *б*) *в*) *г*)

Рис. 1

Свойства теоретико-множественных операций:

1) $A \cup A = A$; $A \cap A = A$;

2) $A \cup B = B \cup A$; $A \cap B = B \cap A$ – коммутативность;

3) $(A \cup B) \cup C = A \cup (B \cup C)$;

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

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

$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ – дистрибутивность;

5) $A \cup \varnothing = A$; $A \cap \varnothing = \varnothing$;

6) $A \cup U = U$; $A \cap U = A$;

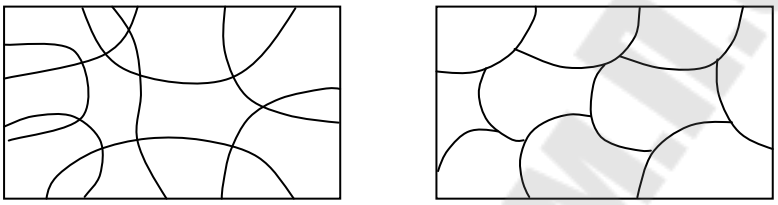
7) $A \cup \overline{A} = U$; $A \cap \overline{A} = \varnothing$;

8) $\overline{\overline{A}} = A$ – инволюция;

9) $\overline{U} = \varnothing$; $\overline{\varnothing} = U$;

10) $\overline{A \cup B} = \overline{A} \cap \overline{B}$; $\overline{A \cap B} = \overline{A} \cup \overline{B}$ – правила де Моргана.

Определение 8. Пусть $\varepsilon = \{E_1, E_2, ..., E_N\}$ – некоторое семейство подмножеств множества M. Тогда, если $\bigcup_{k=1}^{N} E_k = M$, то семейство ε называется **покрытием** M (рис. 2, *а*). Если к тому же $E_i \cap E_j = \varnothing$, то покрытие называется **разбиением** множества M (рис. 2, *б*).



а) *б*)

Рис. 2

Рассмотрим еще один способ построения нового множества из двух заданных.

Определение 9. **Декартовым (прямым) произведением** двух *непустых* множеств A и B называется множество (совокупность) *всех* упорядоченных пар (x, y), где $x \in A$, а $y \in B$.

Декартово произведение множеств, среди которых имеется хотя бы одно пустое, по определению есть пустое множество.

Обозначения декартова произведения:

$$A \times B = \{(x, y) \mid x \in A, y \in B\}.$$

По определению имеем

$$A \times \varnothing = \varnothing \times B = \varnothing \times \varnothing = \varnothing.$$

Пример

Для двух двухэлементных множеств находим:

$$\begin{matrix} A = \{a_1, a_2\} \\ B = \{b_1, b_2\} \end{matrix} \Rightarrow A \times B = \{(a_1, b_1), (a_2, b_1), (a_1, b_2), (a_2, b_2)\}.$$

Теорема 3. Для конечных множеств мощность декартового произведения равна произведению мощностей.

$$|A \times B| = |A| \times |B|. \qquad (2)$$

Безусловно, декартово произведение можно образовать и из одного множества. В этом случае оно называется *степенью множества*:

$$A \times A \equiv A^2 = \{(x, y) \mid x \in A, y \in A\}.$$

Возможно и обобщение вида:

$$A^k = A \times A^{k-1} = \{(x_1, x_2, ..., x_n) \mid x_i \in A\}.$$

Однако в общем случае декартово произведение некоммутативно и не ассоциативно.

С помощью декартова произведения легко ввести важное понятие бинарного отношения, которое отражает связь между объектами, элементами, предметами и т.п.

Определение 10. **Бинарным отношением** R, определенном на множествах A и B, называется всякое подмножество их декартового произведения:

$$R \subseteq A \times B.$$

Если $(a,b) \in R$, то пишут aRb, т. е. a находится в отношении R к b. Такая форма записи бинарного отношения называется ***инфиксной***. В важных случаях R заменяется специальным символом, например, $<$, $\geq$, $=$, $\sim$, $\subset$ и т. п. В случае, если $A = B$, говорят, что отношение R определено на множестве A, при этом $R \subset A^2$.

Определение 11. Пусть R есть отношение между A и B. Тогда вводятся следующие отношения:

– обратное отношение

$$R^{-1} = \{(b,a) \mid (a,b) \in R\}, \ R^{-1} \subseteq B \times A;$$

– дополнение отношения

$$\overline{R} = \{(a,b) \mid (a,b) \notin R\}, \ \overline{R} \subseteq A \times B, \ R \cap \overline{R} = \varnothing, \ R \cup \overline{R} = U;$$

– тождественное отношение

$$I = \{(a,a) \mid a \in A\}, \ I \subseteq A^2;$$

– универсальное отношение

$$U = \{(a,b) \mid a \in A, b \in B\}, \ U = A \times B.$$

Удобна матричная форма задания отношения. Матрица бинарного отношения $R \subseteq A \times B$ вводится следующим образом:

$$(M_R)_{ij} = \begin{cases} 1, & \text{если } a_i R b_j; \\ 0, & \text{если } a_i \overline{R} b_j. \end{cases} \qquad (3)$$

Пример

Пусть на множествах $A = \{a, b, c\}$ и $B = \{x, y\}$ задано отношение $R = \{(a, x), (b, y), (c, x), (c, y)\}$. Построим матрицу этого отношения:

$$M_R = \begin{array}{c} \\ a \\ b \\ c \end{array} \begin{array}{c} \begin{array}{cc} x & y \end{array} \\ \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 1 \end{bmatrix} \end{array}.$$

В частности матрица $\begin{bmatrix} 0 & 1 \\ 1 & 0 \\ 0 & 0 \end{bmatrix}$ задает дополнение отношения $\overline{R} = \{(a, y), (b, x)\}$.

Нетрудно убедиться в справедливости следующих формул для матриц, введенных выше бинарных отношений:

– $M_{R^{-1}} = M_R^T$ – транспонированная матрица;

– $M_I = E = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ – единичная матрица;

– $M_U = \begin{bmatrix} 1 & 1 & \ldots & 1 \\ 1 & 1 & \ldots & 1 \\ \ldots & \ldots & \ldots & \ldots \\ 1 & 1 & \ldots & 1 \end{bmatrix}$ – матрица, составленная из единиц;

– $M_{\overline{R}} = M_U - M_R$ – разность матриц.

Определение 12. Пусть $R_1 \subseteq A \times B$, $R_2 \subseteq B \times C$ два бинарных отношения. Тогда их **композицией** называется отношение $R = R_1 \circ R_2 \subseteq A \times C$, состоящее только из тех пар $(a, c) \in R$, для которых найдется элемент $b \in B$ такой, что aR_1b и bR_2c.

Теорема 4. Матрица композиции двух бинарных отношений равна произведению матриц бинарных отношений:

$$M_{R_1 \circ R_2} = M_{R_1} \cdot M_{R_2}. \quad (4)$$

Замечание. Произведение матриц осуществляется обычным образом, но равенство понимается с точностью до ненулевых элементов.

Рассмотрим некоторые важнейшие типы отношений.

Определение 13. Пусть $R \subseteq A^2$. Тогда отношение R называется

1) рефлексивным, если для $\forall\, a \in A \quad aRa$;

2) симметричным, если для $\forall a,b \in A \quad aRb \Rightarrow bRa$, т. е. $R^{-1} = R$;

3) антисимметричным, если для $a,b \in A \quad aRb, bRa \Rightarrow a = b$;

4) транзитивным, если для $a,b,c \in A \quad aRb, bRc \Rightarrow aRc$;

5) полным, если для $\forall\, a,b \in A \quad a = b$ или aRb или bRa.

Пример

Пусть R – отношение включения множества A в множество B, т. е. $R \equiv \subseteq$. Определим тип этого отношения.

1) $A \subseteq A$ для любого A. Следовательно, $R \equiv \subseteq$ – рефлексивно.

2) $A \subseteq B, B \subseteq C \Rightarrow A \subseteq C$. Следовательно, $R \equiv \subseteq$ – транзитивно.

3) $A \subseteq B, B \subseteq A \Rightarrow A = B$. Следовательно, $R \equiv \subseteq$ – антисимметрично.

4) В общем случае из условия $A \subseteq B$ не следует, что $B \subseteq A$. Следовательно, отношение $R \equiv \subseteq$ симметричным не является.

Установить тип отношения легко и по матрице отношения:

– R – рефлексивно $\Rightarrow$ M_R на диагонали содержит 1.

– R – симметрично $\Rightarrow$ $M_R^T = M_R$.

– R – антирефлексивно $\Rightarrow$ M_R на диагонали содержит 0.

– R – полно $\Rightarrow$ M_R состоит из единиц.

Определение 14. Пусть $R \subseteq A^2$. Тогда, если отношение R

1) рефлексивно;

2) симметрично;

3) транзитивно,

то R называется отношением **эквивалентности**.

Примеры отношений эквивалентности: быть параллельными для прямых, быть подобными для треугольников, быть равными для функций, выражений и т. п.

Общая идея введения отношения эквивалентности – объединить объекты, которые похожи чем-то друг на друга.

Определение 15. Пусть R – отношение эквивалентности, определенное на множестве A. Тогда множество всех элементов x из A, таких, что aRx для некоторого a называется **смежным классом** для a:

$$[a]_R = \{x \in A \mid aRx\}.$$

Важным является следующее свойство классов смежности.

Теорема 5. Пусть R – отношение эквивалентности на множестве A. Тогда оно определяет разбиение A, состоящее из смежных классов. Наоборот, всякое разбиение множества A задает отношение эквивалентности.

Пример

Пусть $A = \{1, 2, 3\}$. Определим отношение эквивалентности $R = \{(1,1),(1,2),(2,2),(2,1),(3,3)\}$.

Матрица отношения

$$M_R = \begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

рефлексивна, симметрична, транзитивна (для транзитивных отношений с точностью до ненулевых элементов выполняется соотношение $M_R^2 = M_R$).

Классы смежности:

$$\begin{matrix} [1]_R = \{1, 2\} \\ [2]_R = \{1, 2\} \\ [3]_R = \{3\} \end{matrix} \Rightarrow [1]_R = [2]_R.$$

Таким образом, разбиение A содержит два класса $\{[1]_R, [3]_R\}$.

Определение 16. Совокупность смежных классов множества A по эквивалентности R называется **фактор-множеством** A по R и обозначается как A/R.

Таким образом, в нашем примере $A/R = \{[1]_R, [3]_R\}$.

Определение 17. Бинарное отношение R, определенное на множестве A, которое является рефлексивным, антисимметричным, транзитивным называется отношением **частичного порядка**.

Примеры отношений частичного порядка: $\subseteq$, $\leq$, «x делит y на множестве N». Общее обозначение: $\preceq$.

Определение 18. Пусть A – частично-упорядоченное множество. Элемент a называется **наибольшим** в A, если $x \preceq a$ для любого $x \in A$, и **наименьшим**, если $a \preceq x$ для любого $x \in A$.

Определение 19. **Максимальным** элементом частично-упорядо-ченного множества A называется такой его элемент a, для которого всякий x из A либо не сравним с a, либо $x \preceq a$ (для **минимального** элемента – $a \preceq x$).

Разница между наибольшим и максимальным элементами заключается в том, что наибольший элемент либо отсутствует, либо единственный. Максимальный элемент всегда существует и их может быть несколько. Если наибольший элемент существует, то он автоматически является и максимальным элементом множества с частичным порядком. Аналогично для наименьшего и минимального элементов. Частично упорядоченное множество удобно изображать с помощью диаграмм Хассе, в которых сравнимые элементы, непосредственно следующие друг за другом, изображаются точками, соединенными отрезками.

Пример

Пусть $A = \{a_1, a_2, a_3\}$. Введем частичный порядок как отношение включения подмножеств: $\preceq \equiv \subseteq$, определенном на подмножествах множества A, т. е. на булеане $B(A)$.

Диаграмма Хассе будет иметь вид, представленный на рис. 3.

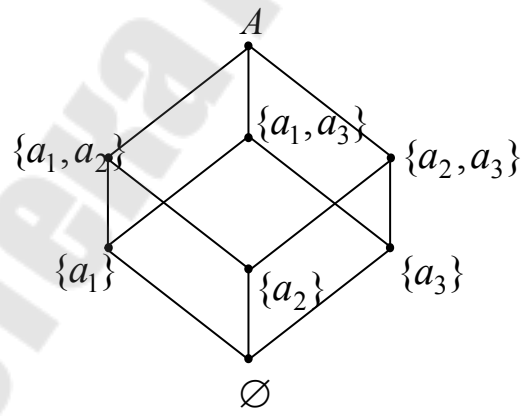


Рис. 3

Из диаграммы видно:

– наибольший элемент A;

– наименьший элемент $\varnothing$;

– подмножества $\{a_1\}$ и $\{a_2\}$ несравнимы.

ЛЕКЦИИ 2–3
ЭЛЕМЕНТЫ КОМБИНАТОРИКИ

Комбинаторика (комбинаторный анализ, комбинаторная математика) – это раздел математики, изучающий способы построения подмножеств некоторого конечного множества с заданными ограничениями.

Сами подмножества при этом называются ***комбинаторными конфигурациями*** или ***выборками***.

Предмет комбинаторики составляют следующие задачи:

– подсчет числа комбинаторных конфигураций (комбинаторные числа);

– определение системы условий существования заданных комбинаторных конфигураций;

– разработка алгоритмов построения и генерации комбинаторных конфигураций;

– решение оптимизационных задач.

Эти задачи находят самое широкое применение в теории алгоритмов, теории вероятностей, теории кодирования и т. д.

Так как в комбинаторике используются только конечные множества A, содержащие n элементов, то принято в первую очередь указывать мощность множества:

$A = \{a_1, a_2, ..., a_n\} \Rightarrow n$**-множество** A.

Определение 1. Множество C, имеющее несколько экземпляров одного и того же элемента, называется **мультимножеством**.

Пример

$$\{a, a, b, b, c\} - \text{мультимножество.}$$

Определение 2. **Выборкой** называется всякое мультимножество, элементы которого выбираются из элементов множества A. Число элементов в выборке r определяет ее объем.

Пример

$$A = \{a_1, a_2, a_3\} \Rightarrow C = \{a_1, a_2, a_1, a_1\} - 4\text{-выборка.}$$

Замечание. В лекции 1, где рассматривались элементы множеств, мультимножества не вводились, т. е. множества $\{a, a, b, c\}$, $\{a, c, b\}$, $\{a, b, b, c, c,\}$ не различались и рассматривались как одно и то же множество $\{a, b, c\}$.

Определение 3. Выборка, в которой порядок записи элементов не учитывается, называется **сочетанием**, а в которой учитывается – **перестановкой**.

Введение r-сочетаний и r-перестановок охватывает все типы выборок. При этом нет необходимости отдельно вводить понятие размещения, так как *размещение* – это r-перестановка без повторений.

Рассмотрим основные правила комбинаторики.

I. Правило суммы (закон аддитивности).

Число способов, которыми можно выбрать элементы n-множества A и элементы m-множества B при условии, что $A \cap B = \varnothing$, равно $n+m$. С использованием понятия мощности конечных множеств это правило можно записать как

$$|A \cup B| = |A| + |B|, \text{ если } A \cap B = \varnothing. \qquad (5)$$

Пример

Лекции по физике посещают 20 студентов, а лекции по теоретической механике – 30, сколько студентов посещают указанные лекции, если они происходят в одно и то же время?

Решение

Введем следующие множества:

– $A = \{\text{студенты, посещающие физику}\}$; $|A| = 20$;

– $B = \{\text{студенты, посещающие математику}\}$; $|B| = 30$.

По условию $A \cap B = \varnothing$. Тогда согласно формуле (1) находим $|A \cup B| = |A| + |B| = 20 + 30 = 50$.

II. Правило произведения (закон мультипликативности).

Число способов выбора элементов из декартового произведения двух множеств A и B объемом n и m равно произведению $n \cdot m$:

$$|A \times B| = |A| \cdot |B| = n \cdot m. \qquad (6)$$

Пример

Пусть имеется 5 различных конвертов и 6 различных марок. Сколькими способами можно отправить письмо в конверте с маркой?

Решение

Введем множества: $A = \{\text{конверты}\}$; $B = \{\text{марки}\}$; $A \times B = \{(\text{конверт, марка})\}$. Таким образом, $|A \times B| = |A| \cdot |B| = 5 \cdot 6 = 30$.

В комбинаторике основными комбинаторными числами являются:

– $U(n,r) \equiv \overline{N}(n,r)$ – число различных упорядоченных выборок с повторением из n-множества A;

– $A_n^r \equiv N(n,r)$ – число различных упорядоченных выборок без повторений из n-множества A;

– $C_n^r \equiv \binom{n}{r} \equiv C(n,r)$ – число различных неупорядоченных выборок (сочетаний) без повторений из A;

$\overline{C}_n^r \equiv \overline{C}(n,r)$ – число различных сочетаний с повторениями из n-множества A.

Теорема 1. Если выборка составляется из n-множества A, то введенные выше числа вычисляются по формулам:

$$U(n,r) = n^r; \tag{7}$$

$$A_n^r = \frac{n!}{(n-r)!}; \tag{8}$$

$$C_n^r = \frac{n!}{r!(n-r)!}; \tag{9}$$

$$\overline{C}_n^r \equiv C_{n+r-1}^r = \frac{(n+r-1)!}{r!(n-1)!}. \tag{10}$$

Доказательство

1. Если ε – множество различных упорядоченных r-выборок с повторениями, то $\varepsilon = \underbrace{A \times A \times \ldots \times A}_{r \text{ раз}} = A^r$. Поэтому

$$U(n,r) = |\varepsilon| = |A|^r = n^r.$$

2. Для упорядоченной выборки, не допускающей повторений элементов, первый элемент можно выбрать n способами, второй $(n-1)$ и т. д. Последний элемент выбирается из оставшихся $(n-r+1)$ элементов. Поэтому получаем $A_n^r = n \cdot (n-1) \cdot \ldots \cdot (n-r+1) = \frac{n!}{(n-r)!}$

(или более строго на языке множеств:

$$\varepsilon = A^{(n)} \times A^{(n-1)} \times \ldots \times A^{(n-r+1)} \Rightarrow |\varepsilon| = n \cdot (n-1) \cdot \ldots \cdot (n-r+1)).$$

3. Если имеется r-сочетание без повторений, то упорядочить его можно $r \cdot (r-1) \cdot (r-2) \cdot \ldots \cdot 1 = r!$ способами. Поэтому

$$r!C_n^r = A_n^r \Rightarrow C_n^r = \frac{A_n^r}{r!} = \frac{n!}{r!(n-r)!}.$$

4. Для подсчета числа различных r-сочетаний с повторениями удобно сопоставить пронумерованным элементам множества A ячейки, которые образованы $(n+1)$ стенкой. Тогда необходимая выборка реализуется как конфигурация размещения r неразличимых шариков в n ячеек:

$$|\mathrm{O}\ \mathrm{O}|\ |\mathrm{O}|\ldots|\mathrm{O}\ \mathrm{O}\ \mathrm{O}|\ |\ |.$$

Число шариков в конкретной ячейке указывает число экземпляров соответствующего элемента из A в выборке, а число различных выборок будет равно числу перестановок r шариков и $(n-1)$ внутренних стенок. Однако при этом в силу неразличимости шариков и стенок необходимо исключить перестановки между шариками и перестановки между стенками. Таким образом, получим

$$\overline{C}_n^r = \frac{(r+n-1)!}{r!(n-1)!} = C_{n+r-1}^r.$$

Что и требовалось доказать.

Еще один важный тип комбинаторных конфигураций составляет разбиение множества на непустые подмножества.

Вначале зафиксируем тип разбиения и решим следующую задачу. Разобьем n-множество A на семейство k подмножеств $\varepsilon = \{E_1, E_2, \ldots, E_k\}$ так, чтобы в первом подмножестве было n_1 элементов, во втором n_2 элементов и т. д., т. е. $n(E_i) = n_i$. Очевидно, что должно выполняться равенство

$$n_1 + n_2 + \ldots + n_k = n.$$

Спрашивается, сколько различных разбиений такого типа существует.

Теорема 2. Число различных разбиений n-множества A на k подмножеств с фиксированным числом элементов равно

$$C(n; n_1, n_2, \ldots n_k) = \frac{n!}{n_1! n_2! \ \ldots n_k!}. \qquad (11)$$

Доказательство

Число способов выбора элементов для первого подмножества разбиения равно $C_n^{n_1}$, для второго – $C_{n-n_1}^{n_2}$, для третьего – $C_{n-n_1-n_2}^{n_3}$ и т. д. В результате для искомого числа находим

$$C(n; n_1, n_2, ...n_k) = C_n^{n_1} \cdot C_{n-1}^{n_2} \cdot ... \cdot C_{n-n_1-...-n_{k-1}}^{n_k} =$$

$$= \frac{n!}{n_1!(n-n_1)!} \cdot \frac{(n-n_1)!}{n_2!(n-n_1-n_2)!} \cdot ... \cdot \frac{(n-n_1-..-n_{k-1})!}{n_k!(n-n_1-...-n_k)!} = \frac{n!}{n_1!n_2!...n_k!}.$$

Что и требовалось доказать.

Замечание. Формулу (7) можно также просто получить, используя модель построения разбиения с помощью системы шариков и стенок.

Теперь перейдем к более сложной задаче определения числа различных разбиений n элементного множества на k классов, когда число элементов в подмножествах не фиксировано. Единственное условие – отсутствие пустых подмножеств.

Определение 4. Пусть $n > 0$, а $1 \le k \le n$. Число различных разбиений n-множества A на k непустых классов $\varepsilon = \{E_1, E_2, ..., E_k\}$ называется **числом Стирлинга второго рода** и обозначается как $S(n,k)$.

Теорема 3. Число Стирлинга второго рода $S(n,k)$ обладает следующими свойствами:

$$S(n,1) = S(n,n) = 1; \tag{12}$$

$$S(n,k) = S(n-1, k-1) + kS(n-1,k), \text{ если } n \ge 3,\ 2 \le k \le n-1. \tag{13}$$

Доказательство

1) Понятно, что если $k = 1$, то разбиение содержит один элемент – само множество A, следовательно $S(n, 1) = 1$. Если же $k = n$, то опять имеем единственное разбиение, состоящее из одноэлементных подмножеств $\varepsilon = \{\{a_1\}, \{a_2\}, ..., \{a_k\}\}$, поэтому $S(n,n) = 1$.

2) Если $n = 2$, то все возможности исчерпываются только двумя уже рассмотренными случаями: $S(2, 1) = S(2, 2) = 1$.

Пусть $n \ge 3$, а $k \in [2, n-1]$ (случай $k = n$ рассмотрен в п. 1). Удалив из A последний элемент a_n, получим $(n-1)$ – множество $A' = A \setminus \{a_n\} = \{a_1, a_2, ..., a_{n-1}\}$. Далее рассмотрим два типа разбиений множества A:

– I тип – одноэлементное подмножество $\{a_n\}$ составляет отдельный класс разбиения;

– II тип – $\{a_n\}$ не является отдельным классом разбиения.

Тогда число разбиений множества A на k классов типа I равно числу разбиений множества $A' = A \setminus \{a_n\}$ на $k-1$ класс, т. е. $S(n-1, k-1)$. А число разбиений типа II равно числу всех различных разбиений множеств $A' = A \setminus \{a_n\}$ на k классов, причем в каждый класс разбиения последовательно добавляется элемент a_n, т. е. имеем

$$\underbrace{S(n-1, k) + \ldots + S(n-1, k)}_{k \text{ раз}} = kS(n-1, k).$$

В сумме получаем

$$S(n, k) = S(n-1, k-1) + kS(n-1, k).$$

Что и требовалось доказать.

Следствие. Число различных разбиений n-множества на 2 класса вычисляется по формуле

$$S(n, 2) = 2^{n-1} - 1 \quad \text{для} \quad n \geq 2. \tag{14}$$

Определение 5. Число всех возможных разбиений n-множества A на непустые классы называется **числом Белла**:

$$B(n) = \sum_{k=1}^{n} S(n, k). \tag{15}$$

Для удобства определяют $B(0) = 1$, хотя в разбиениях обычно пустые множества не рассматриваются.

Важнейшим понятием дискретной математики является функциональное отношение, которое есть обобщение понятия функции на произвольные множества.

Определение 6. Бинарное отношение $R \subseteq A \times B$ называется **функциональным**, если каждому элементу из A ставится в соответствие единственный элемент из B.

Определение 7. Функциональное отношение $R \subseteq A \times B$, для которого для каждого элемента из B найдется хотя бы один элемент из A такой, что, aRb называется **сюръективным**.

Замечание. Функциональные отношения часто называют отображениями. Говорят, что отображение R сюръективно, если оно отображает A на B.

Частный и чрезвычайно важный пример отображения представляют собой подстановки.

Определение 8. **Подстановкой** называется взаимно однозначное отображение множества первых n натуральных чисел на себя:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \alpha_1 & \alpha_2 & \alpha_3 & \dots & \alpha_n \end{pmatrix} \begin{matrix} A \\ \Downarrow \\ A \end{matrix}.$$

Указанная форма записи, когда элементы в верхней строке упорядочены, называется *канонической* подстановкой. При этом можно первую строку не выписывать, а указать просто набор вторых чисел $\pi(\alpha_1, \alpha_2, ..., \alpha_n)$. При этом подстановка называется *перестановкой*. Так как число различных перестановок P_n в формульном редакторе по существу равно числу различных размещений A_n^n, то согласно формуле (8) находим:

$$P_n = n! \qquad (16)$$

Более сложен другой вопрос, связанный с числом различных сюръективных отображений без взаимной однозначности.

Определение 9. Число различных сюръективных отображений из n-множества A на k-множество B называется **числом Стирлинга первого рода** и обозначается $s(n, k)$.

Если разбить n-множество A на k непустых классов, то тогда можно ввести взаимно однозначное отображение, действующее из k-множества, элементами которого являются классы разбиения, в множество B. Далее, используя определение числа Стирлинга второго рода $S(n,k)$ и формулу (16) для числа перестановок, получим следующий результат.

Теорема 4. Числа Стирлинга первого и второго родов связаны соотношением:

$$s(n,k) = k!S(n,k). \qquad (17)$$

В комбинаторном анализе существует целый ряд подходов для изучения комбинаторных объектов и чисел.

Теоретико-множественный подход

Данный подход связан с вычислением мощностей конечных множеств. Пусть $\{A_1, A_2, ..., A_n\}$ – система подмножеств конечного

множества. Спрашивается, как найти мощности множеств, образованных из множеств A_i с помощью теоретико-множественных операций. Оказывается, что для этого надо знать только мощности самих множеств $|A_i|$ и их пересечений.

Теорема 5. (принцип включения-выключения)

Пусть A и B два произвольных подмножества множества C. Тогда для мощностей множеств справедливо соотношение

$$n(C \setminus (A \cup B)) = n(C) - n(A) - n(B) + n(A \cap B). \qquad (18)$$

Следствие. Пусть A и B два конечных множества, тогда для мощности их объединения справедливо соотношение

$$n(A \cup B) = n(A) + n(B) - n(A \cap B). \qquad (19)$$

Доказательство

Из формулы (14) в случае $C = A \cup B$ находим:

$$\underbrace{n(A \cup B \setminus A \cup B)}_{=0} = n(A \cup B) - n(A) - n(B) + n(A \cap B)$$

$$\Downarrow$$

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Что и требовалось доказать.

Формула (15) допускает обобщения на случай объединения любого конечного числа множеств. В частности, для трех множеств имеем:

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) -$$
$$- n(A \cap C) - n(B \cap C) + N(A \cap B \cap C).$$

Алгебраический подход

Он основан на использовании вспомогательных комбинаторных тождеств.

Пусть имеются два семейства комбинаторных чисел $\{a(n)_k\}$ и $\{b(n)_k\}$, где $n = 0, 1, 2, \ldots$; $k = \overline{0, n}$.

Теорема 6. (теорема обращения)

Если для любого n и $k \le n$ имеет место разложение

$$a(n)_k = \sum_{l=0}^{n} \lambda(n)_k^l b(n)_l, \qquad (20)$$

причем при $k \le n$, $m \le n$ коэффициенты $\lambda(n)_k^l$ удовлетворяют соотношению

$$\sum_{l=0}^{n} \mu(n)_k^l \lambda(n)_l^m = \delta_k^m = \begin{cases} 1, & k = m; \\ 0, & k \ne m, \end{cases} \tag{21}$$

где $\mu(n)_k^l$ – определенный набор комбинаторных чисел, то при $k \le n$ справедливо разложение

$$b(n)_k = \sum_{l=0}^{n} \mu(n)_k^l a(n)_l \,. \tag{22}$$

Доказательство

Для правой части равенства (22) с использованием соотношения (21) находим

$$\sum_{l=0}^{n} \mu(n)_k^l a(n)_l \overset{\text{ф.(20)}}{=} \sum_{l=0}^{n} \mu(n)_k^l \sum_{m=0}^{n} \lambda(n)_l^m b(n)_m =$$

$$= \sum_{m=0}^{n} \underbrace{\left[\sum_{l=0}^{n} \mu(n)_k^l \lambda(n)_l^m \right]}_{\delta_k^m} b(n)_m = \sum_{m=0}^{n} \delta_k^m b(n)_m = b(n)_k \,.$$

Что и требовалось доказать.

В качестве комбинаторных чисел-коэффициентов $\lambda(n)_k^l$, как правило, выбирают биномиальные коэффициенты C_n^k, которые удовлетворяют следующим соотношениям:

1) $(a+b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}$ – разложение бинома Ньютона; (23)

2) $C_n^0 = C_n^n = 1$;

3) $C_n^k = \dfrac{n!}{k!(n-k)!} = C_n^{n-k}$ – свойство симметрии биномиальных коэффициентов;

4) $\sum_{k=0}^{n} C_n^k = 2^n$ – свойство суммы биномиальных коэффициентов. (24)

Доказательство

Из формулы (23) при $a = b = 1$ находим $2^n = \sum_{k=0}^{n} C_n^k$;

5) $\sum_{k=0}^{n} (-1)^k C_n^k = \delta_n^0 = \begin{cases} 1, & n = 0; \\ 0, & n > 0 \end{cases}$ –свойство суммы C_n^m. (25)

Доказательство

Из формулы (23) $\Rightarrow$ $a = -1$, $b = 1$, $n \neq 0 \Rightarrow$ $\sum_{k=0}^{n} (-1)^k C_n^k = 0^n = 0.$

Из формулы (23) $\Rightarrow$ $n = 0$ $\Rightarrow$ $C_0^0 a^0 b^0 = 1.$

6) $C_n^l \cdot C_l^k = C_n^k \cdot C_{n-k}^{n-l} = C_n^k \cdot C_{n-k}^{l-k}$ – мультипликативное свойство. (26)

Доказательство

Используя выражение для C_n^k через факториалы, находим:

$$C_n^l \cdot C_l^k = \frac{n!}{l!(n-l)!} \cdot \frac{l!}{k!(l-k)!} = \underbrace{\frac{n!}{k!(n-k)!}}_{=C_n^k} \cdot \underbrace{\frac{(n-k)!}{(n-l)!(l-k)!}}_{=C_{n-k}^{n-l}=C_{n-k}^{l-k}} = C_n^k \cdot C_{n-k}^{n-l},$$

Что и требовалось доказать.

7) $\sum_{l=0}^{n} \underbrace{(-1)^{l-k} C_n^l}_{\mu(n)_k^l} \underbrace{C_l^k}_{\lambda(n)_k^l} = \delta_n^k = \begin{cases} 1, & n = k; \\ 0, & n \neq k. \end{cases}$ (27)

Доказательство

Используя соотношение (26), получаем:

$$\sum_{l=0}^{n} (-1)^{l-k} C_n^l C_l^k = \sum_{l=0}^{n} (-1)^{l-k} C_n^k \cdot C_{n-k}^{l-k} = C_n^k \cdot \sum_{l=0}^{n} (-1)^{l-k} C_{n-k}^{l-k} =$$

$$= \left[\begin{matrix} \text{заметим,} \\ \text{что } l \geq k \end{matrix} \right] = C_n^k \sum_{l=k}^{n} (-1)^{l-k} C_{n-k}^{l-k} = \left[\begin{matrix} l - k = m; \\ 0 \leq m \leq n - k \end{matrix} \right] = C_n^k \sum_{m=0}^{n-k} (-1)^m C_{n-k}^m =$$

$$= C_n^k \delta_{n-k}^0 = \begin{cases} n - k = 0, & C_n^n = 1; \\ n - k \neq 0, & C_n^k \cdot 0 = 0. \end{cases}$$

Что и требовалось доказать.

Сравнивая (27) и (21), выбираем коэффициенты в виде

$$\begin{aligned} \lambda(n)_k^l &= C_k^l, \\ \mu(n)_k^l &= (-1)^{k-l} C_k^l . \end{aligned} \tag{28}$$

Доказательство

Имеем:

$$\sum_{l=0}^{n} \mu(n)_k^l \lambda(n)_l^m = \sum_{l=0}^{n} (-1)^{k-l} C_k^l C_l^m = \left[l \le k \right] = \sum_{l=0}^{k} (-1)^{k-l} C_k^l C_l^m =$$

$$= (-1)^k \sum_{l=0}^{k} (-1)^l C_k^l C_l^m = (-1)^{k-m} \underbrace{\sum_{l=0}^{k} (-1)^{l-m} C_k^l C_l^m}_{\text{ф.(27)} \; = \delta_k^m} =$$

$$= (-1)^{k-m} \cdot \delta_k^m = \delta_k^m \;\Rightarrow\; \text{ф. (21).}$$

Что и требовалось доказать.

Выбирая коэффициенты в форме (28), связь между числами $a(n)_k$ и $b(n)_k$ можно записать как

$$a(n)_k = \sum_{l=0}^{k} C_k^l b(n)_l \,;\; b(n)_k = \sum_{l=0}^{k} (-1)^{k-l} C_k^l a(n)_l \,, \tag{29}$$

где $k \le n$.

Применим этот результат для получения явных формул для чисел Стирлинга.

Рассмотрим множество всех возможных отображений из *n*-множества *A* в *k*-множество *B*. Легко описать это отображение в виде таблицы

$A \overset{\gamma}{\Rightarrow} B$

a_1	a_2	...	a_n
b_{i_1}	b_{i_2}	...	b_{i_n}

Число различных отображений такого рода равно

$$N = \underbrace{k \cdot k \cdot \ldots \cdot k}_{n \text{ раз}} = k^n .$$

С другой стороны, это же число можно найти, используя и числа Стирлинга первого рода, выбирая из множества *B* для отображений сначала 1 элемент, затем 2 элемента и т. д. Поэтому получаем равенство

$$k^n = \sum_{l=1}^{k} C_k^l s(n,l). \qquad (30)$$

С учетом доопределения $s(n,0)=0$ суммирование можно начинать с 0. Тогда, используя равенство (29), находим:

$$s(n,k) = \sum_{l=0}^{k} (-1)^{k-l} C_k^l \cdot l^n = \sum_{l=1}^{k} (-1)^{k-l} C_k^l \cdot l^n ; \qquad (31)$$

$$S(n,k) = \frac{1}{k!} s(n,k) = \frac{1}{k!} \sum_{l=1}^{k} (-1)^{k-l} C_k^l \cdot l^n . \qquad (32)$$

ЛЕКЦИЯ 4
ВВЕДЕНИЕ В ТЕОРИЮ ОБЩИХ АЛГЕБРАИЧЕСКИХ СИСТЕМ

Всякую функцию типа

$$\varphi : \underbrace{M \times M \times \ldots \times M}_{n \text{ раз}} \to M$$

будем называть *n*-арной операцией, определенной на множестве M. При этом число аргументов *n* называется **арностью** операции. В частности, при $n=2$ имеем бинарную операцию^

$$\varphi : M \times M \to M \;\Rightarrow\; w = \varphi(u,v).$$

Определение 1. Множество M вместе с заданной на нем совокупностью операций $\Omega = \{\varphi_1, \varphi_2, \ldots, \varphi_m\}$ называется **алгеброй** $A =< M, \Omega >$. При этом само множество M называется ***носителем алгебры***, а совокупность операций Ω – ***сигнатурой алгебры***.

Набор арностей операций из сигнатуры Ω $(n_1, n_2, \ldots, n_m)$ называется ***типом алгебры***.

Множество $M' \subseteq M$ называется *замкнутым* относительно некоторой операции φ, определенной на M, если значения φ на аргументах из M' сами принадлежат M', т. е.

$$\varphi(M') \in M'.$$

Если M' замкнуто относительно всех операций из сигнатуры алгебры $\Omega = \{\varphi_1, \varphi_2, ..., \varphi_m\}$, то M' называется *подалгеброй* алгебры A.

Пример

1. Для алгебры $A =< \boldsymbol{R}, \{\cdot, +\} > \Rightarrow M = \boldsymbol{R},\ \Omega = \{\cdot, +\}$.

Так как обе операции бинарные, то тип алгебры $A(2, 2)$. Такая алгебра называется *полем действительных чисел*.

Очевидно, что $A' =< \boldsymbol{Z}, \{\cdot, +\} >$ есть подалгебра A.

2. Пусть задано некоторое множество M, а $B(M)$ – его булеан. Тогда алгебра $B =< B(M); \cup, \cap, \bar{} >$ имеет сигнатуру $\Omega = \{\cup, \cap, \bar{}\}$, а ее тип $(2, 2, 1)$. Данная алгебра называется булевой алгеброй множеств или алгеброй Кантора.

Если M – конечное множество, то бинарные операции могут быть заданы таблицами.

Пример

1. Рассмотрим квадрат с вершинами в точках A_1, A_2, A_3, A_4 и повороты вокруг центра квадрата, переводящие вершины друг в друга. Зафиксируем некоторое направление поворота как положительное. Существует всего 4 различных поворота, переводящих вершины в себя, а именно, повороты на 0, $\frac{\pi}{2}$, π, $\frac{3\pi}{2}$ радиан. Таким образом, получаем алгебру с носителем $M = \{A_1, A_2, A_3, A_4\}$ и четырьмя унарными операциями-поворотами $\Omega = \{\lambda, \beta, \gamma, \delta\}$. Таблица имеет вид:

	α	β	γ	δ
A_1	A_1	A_2	A_3	A_4
A_2	A_2	A_3	A_4	A_1
A_3	A_3	A_4	A_1	A_2
A_4	A_4	A_1	A_2	A_3

Тип алгебры (1, 1, 1, 1). У этой алгебры нет подалгебр.

2. Рассмотрим множество поворотов $\Omega = \{\lambda, \beta, \gamma, \delta\}$ с бинарной операцией: $\circ$ – композицией преобразований. Тогда $A =< \Omega; \circ >$ есть алгебра поворотов с носителем Ω и сигнатурой, состоящей из одной операции $\{\circ\}$. Тип алгебры (2). Ее таблица Кэли имеет вид:

$\circ$	α	β	γ	δ
α	α	β	γ	δ
β	β	γ	δ	α
γ	γ	δ	α	β
δ	δ	α	β	γ.

Множество $\{\alpha, \gamma\}$ образует подалгебру алгебры $< \Omega; \circ >$:

$\circ$	α	γ
α	α	γ
γ	γ	α.

Далее рассмотрим различные алгебры с одной операцией.

Определение 2. Алгебра вида $< M, f_2 >$, где f_2 – некоторая бинарная операция $f_2 : M^2 \to M$ называется **группоидом**. Если f_2 – операция типа умножения, то группоид называется *мультипликативным*, а если тип сложения – *аддитивным*.

Для бинарной операции удобно ввести некоторые общие обозначения:

$$af_2b \equiv a * b .$$

Определение 3. Группоид называется **коммутативным**, если

$$a*b = b*a , \tag{33}$$

и **ассоциативным**, если

$$a*(b*c) = (a*b)*c . \tag{34}$$

Важным примером ассоциативного группоида является множество отображений с *композицией*. Примером некоммутативного группоида является множество матриц с операцией – матричное умножение. Пример не ассоциативного группоида – булеан $B(U)$ с декартовым произведением $\times$.

Определение 4. Элемент e группоида $< M; * >$ называется **единичным** для операции $*$, если выполняются равенства

$$a*e = e*a = a . \tag{35}$$

Для мультипликативных группоидов e есть 1, а для аддитивных – 0.

Замечание: Вообще-то возможно введение левого или правого единичных элементов. Однако, если в группоиде есть e_L и e_R, то они совпадают.

Определение 5. Группоид с ассоциативной операцией $*$ называется **полугруппой**. Полугруппа с единицей называется **моноидом**.

Пример

1) $< \boldsymbol{Z}; + >$ – полугруппа, так как $(a+b)+c = a+(b+c)$ для любых чисел из Z.

2) $< \boldsymbol{Z}; - >$ – группоид, но не полугруппа, так как $(a-b)-c \neq a-(b-c)$.

Рассмотрим следующий важный пример полугрупп.

Пусть имеется множество символов $S = \{s_1, s_2, ...\}$, которые назовем алфавитом. Тогда некоторая упорядоченная совокупность символов образует *слово*. Для удобства вводится в качестве отдельного символа пробел ␣. Рассмотрим множество всех символов S^*. Введем над символами следующую бинарную операцию:

$$U \circ V = UV \,. \tag{36}$$

Ее называют *конкатенацией* (другие названия – сцепление, приписывание, слияние). Очевидно, что эта операция слияния не коммутативна, но ассоциативна. Следовательно, наш группоид $< S^*, \circ >$ является полугруппой. Она называется *свободной полугруппой*. Безусловно, можно выделить не все слова, а только их часть $L \subseteq S^*$. Такое подмножество удобно называть *языком*.

Понятие языка можно ввести на любом множестве, в частности, на двухэлементном множестве $\{0,1\}$. На языке можно вводить различные грамматики типа $a^n b^m$, $b^n a b^m$ и т. п. Развитие такой алгебраической теории приводит нас к ***теории автоматов***.

Всякую полугруппу можно получить из свободных полугрупп путем задания так называемых определяющих соотношений:

$$a^2 = a, \;\; ab = ba \;\; \text{и т. п.}$$

Из любого слова, используя определяющие соотношения, можно получить эквивалентные слова.

Намного более сложной является обратная задача – установление эквивалентности двух слов. Эта задача приводит к ***теории алгоритмов***.

Определение 6. Пусть G – непустое множество с бинарной операцией $\circ$. Тогда, если выполняются следующие условия:

1) операция $\circ$ – ассоциативна;

2) в множестве G имеется единичный элемент e;

3) для $\forall g \in G \ \exists \ g^{-1}$: $g \circ g^{-1} = g^{-1} \circ g = e$;

то множество G называется **группой**.

Таким образом, группа – это обратимый моноид. Число элементов в группе называется ее порядком.

Группа, в которой операция $\circ$ – коммутативна, называется ***абелевой***. Если $\forall g \in G$ есть $g = a^k$, то группа называется ***циклической***.

Пример

1) $< \boldsymbol{Z}; + >$ – абелева группа;

2) $< \boldsymbol{Q} / \{0\}; \times >$ – абелева группа;

3) Пусть S_n – множество всех перестановок n-го порядка $\pi(\alpha_1, \alpha_2, ..., \alpha_n)$. Тогда $< S_n; \circ >$ – симметрическая группа, где $\circ$ – операция композиции перестановок.

Определение 7. Подмножество H группы G называется **подгруппой**, если H само образует группу.

Очевидно, что H должно содержать единицу e.

Определение 8. Если H есть подгруппа G и $a \in G$, то множество

$$Ha = \{h \circ a \mid h \in H\}$$

называется **левым смежным классом** для a. Обозначим его как ${}_H[a]$. Аналогично вводится и **правый смежный класс**: $aH \equiv [a]_H$.

Свойства смежных классов и подгрупп по подгруппе H:

I. Смежные классы задают разбиение группы G.

II. (теорема Лагранжа) Порядок конечной подгруппы H является делителем порядка конечной группы G.

III. Если порядок $|G|$ есть простое число, то у группы G нет нетривиальных подгрупп.

IV. Число различных смежных классов равно отношению $|G| / |H|$.

Алгебры с различными типами являются различными. Однако, если алгебры имеют один тип, то они могут быть похожи друг на друга. Степень схожести характеризуется понятием «морфизм».

Определение 9. Пусть имеются две алгебры

$$A =< K; \circ > \ \text{и} \ \ B =< M; * >.$$

Тогда отображение $\Gamma : A \to B$, удовлетворяющее условию

$$\Gamma(a \circ b) = \Gamma(a) * \Gamma(b),$$

называется **гомоморфизмом**.

Если гомоморфизм взаимно-однозначный, то он называется *изоморфизмом*. Если установлен изоморфизм алгебр, то, получив некоторые соотношения в алгебре A, можно их распространить на алгебру B.

Теорема 1. Любая подгруппа с единицей (моноид) изоморфна некоторой полугруппе преобразований носителя M.

Теорема 2. (теорема Кэли) Всякая конечная группа изоморфна группе подстановок на множестве ее элементов.

Замечание. В группе при любом количестве «умножений» не теряется информация об исходном элементе. В подгруппе это не всегда так.

Множества, на которых кроме операций заданы отношения, называются *алгебраическими системами*. Если заданы только отношения, то такие множества называются *моделями*.

Определение 10. ***Решеткой*** (структурой) называется частично упорядоченное множество с введенными операциями:

$$a \cap b = \inf\{a, b\} - \text{«меньше»},$$

$$a \cup b = \sup\{a, b\} - \text{«больше»}.$$

Пример

1. Любое линейно-упорядоченное множество – решетка.
2. Введем на множестве натуральных чисел $\boldsymbol{N}$ отношение

$$x \mid y = \{x - \text{делитель } y\}.$$

Тогда $x \cup y = H.O.K.(x, y)$, $x \cap y = H.O.D.(x, y)$. Следовательно,

$$< N; \mid; H.O.K.(x, y), H.O.D.(x, y) > - \text{решетка}.$$

3. Пусть $B(U)$ – булеан некоторого множества U, тогда

$$< B(U); \subseteq; \cup, \cap > - \text{решетка}.$$

ЛЕКЦИЯ 5
АЛГЕБРА ВЫСКАЗЫВАНИЙ И БУЛЕВЫ ФУНКЦИИ

Определение 1. **Высказывание** – это повествовательное утверждение или математическое предложение, относительно которого можно точно судить истинно оно или ложно.

Примеры

– $1 > 2$ – ложное высказывание,

– $2 + 2 = 4$ – истинное высказывание,

– $10 > 3$ и 5 – высказыванием не является.

Всякое высказывание принимает два значения – «истина» или «ложь».

Обозначения: p, q, r – высказывания;

$$\left.\begin{matrix}\{\text{И},\ \text{Л}\}\\ \{T,\ F\}\\ \{1,\ 0\}\end{matrix}\right\rangle \text{– значения высказываний.}$$

Пример

$$p = \{1 > 2\} = \text{Л} \equiv F \equiv 0\,.$$

Определение 2. **Конъюнкцией** высказываний p и q называется высказывание, которое истинно тогда и только тогда, когда истинны p и q.

Обозначение: $p \wedge q \equiv p \,\&\, q$.

Конъюнкция как операция соответствует использованию союза «и».

Определение 3. **Дизъюнкцией** двух высказываний p и q называется высказывание, которое ложно тогда и только тогда, когда ложны p и q.

Обозначение: $p \vee q$.

Дизъюнкция как операция соответствует использованию союза «или».

Определение 4. **Импликацией** p и q называется высказывание, которое ложно тогда и только тогда, когда p истинно, а q ложно.

Обозначение: $p \Rightarrow q$.

Импликация соответствует связи «если …, то …». p называется посылкой, а q – следствием.

Определение 5. **Эквиваленцией** высказываний p и q называется высказывание, которое истинно тогда и только тогда, когда p и q принимают одинаковые значения.

Обозначение: $p \sim q$.

Эквиваленция соответствует связке «p тогда и только тогда, когда q», «для p необходимо и достаточно q».

Определение 6. **Отрицанием** p является высказывание, которое принимает значение обратное p.

Обозначение: $\overline{p} \equiv \neg p$.

Отрицание есть унарная операция, которая соответствует союзу «не».

Удобной формой представления действий логических операций являются таблицы истинности:

p	$\overline{p}$
1	0
0	1

p	q	$p \vee q$	$p \wedge q$	$p \Rightarrow q$	$p \sim q$
0	0	0	0	1	1
0	1	1	0	1	0
1	0	1	0	0	0
1	1	1	1	1	1

Формулой алгебры логики называется всякое высказывание, построенное из элементарных высказываний с использованием введенных операций. При этом важным является только значение результирующего высказывания, а не его смысл. Так верными с точки зрения математической логики являются, например, такие удивительные высказывания:

«если арбуз – ягода, то снег белый».

Действительно, введем следующие высказывания: $p = \{\text{арбуз – ягода}\}$, $q = \{\text{снег – белый}\}$. Тогда имеем $p \Rightarrow q = T \Rightarrow T = T$.

Для упрощения записи сложных высказываний принят следующий порядок логических действий:

1	2	3	4	5
$\neg$	$\wedge$	$\vee$	$\Rightarrow$	$\sim$

Кроме этого порядок действий регулируется скобками.

Определение 7. Две формулы A и B называются **равносильными**, если они принимают одинаковые логические значения на любом наборе значений элементарных высказываний.

Пример

Проверить равносильность формул:

$$A = p \vee (p \wedge q), \;\; B = p.$$

Решение

p	q	$p \wedge q$	$p \vee (p \wedge q)$	p
0	0	0	0	0
0	1	0	0	0
1	0	0	1	1
1	1	1	1	1
			A	B

$\Rightarrow \; A \equiv B$, т. е. $\boxed{p \vee (p \wedge q) \equiv p}$.

Пример

Проверить равносильность высказываний:

$$A \equiv p \Rightarrow q, \;\; B = \overline{p} \vee q.$$

Решение

p	q	$p \Rightarrow q$	$\overline{p}$	$\overline{p} \vee q$
0	0	1	1	1
0	1	1	1	1
1	0	0	0	0
1	1	1	0	1

$\Rightarrow \quad \boxed{p \Rightarrow q \equiv \overline{p} \vee q}$.

Простейшие равносильности составляют таблицу законов алгебр высказываний.

1. Закон идемпотентности: $p \vee p \equiv p$, $p \wedge p \equiv p$;

2. Закон коммутативности: $p \wedge q \equiv q \wedge p$, $p \vee q \equiv q \vee p$;

3. Закон ассоциативности: $(p \vee q) \vee r \equiv p \vee (q \vee r)$, $(p \wedge q) \wedge r \equiv p \wedge (q \wedge r)$;

4. Закон дистрибутивности: $p \vee (q \wedge r) \equiv (p \vee q) \wedge (p \vee r)$, $p \wedge (q \vee r) \equiv (p \wedge q) \vee (p \wedge r)$;

5. $p \vee F \equiv p$, $p \wedge F \equiv F$;

6. $p \vee T \equiv T$, $p \wedge T \equiv p$;

7. $p \vee \overline{p} \equiv T,\ p \wedge \overline{p} \equiv F$;

8. Закон инволюции: $\overline{\overline{p}} = p$;

9. Законы де Моргана: $\overline{p \vee q} \equiv \overline{p} \wedge \overline{q}$, $\overline{p \wedge q} \equiv \overline{p} \vee \overline{q}$.

Высказывания, которые на любом наборе аргументов принимают значение T, называются **тавтологиями**, а F – **контрадикциями**.

Задача. По обвинению в ограблении перед судом предстали три лица A, B и C. Следствием достоверно было установлено:

1) если A не виновен или B виновен, то C виновен;

2) если A не виновен, то C не виновен.

Установить, виновен ли A?

Решение

Введем следующие высказывания:

$$p = \{A \text{ виновен}\},\ q = \{B \text{ виновен}\},\ r = \{C \text{ виновен}\}.$$

По условию имеем:

$$\begin{cases}(\overline{p} \vee q) \Rightarrow r \equiv T \\ \overline{p} \Rightarrow \overline{r}\end{cases} \Rightarrow \begin{cases}\overline{\overline{p} \vee q} \vee r \equiv T \\ \overline{\overline{p}} \vee \overline{r} \equiv T\end{cases} \Rightarrow \begin{cases}(\overline{\overline{p}} \wedge q) \vee r \equiv T \\ p \vee \overline{r} \equiv T\end{cases} \Rightarrow$$

$$\Rightarrow \begin{cases}(p \vee r) \wedge (q \vee r) \equiv T \\ p \vee \overline{r} \equiv T\end{cases} \Rightarrow \begin{cases}p \vee r \equiv T \\ q \vee r \equiv T \\ p \vee \overline{r} \equiv T\end{cases} \Rightarrow (p \vee r) \wedge (p \vee \overline{r}) \equiv T \Rightarrow$$

$$\Rightarrow p \vee (r \wedge \overline{r}) \equiv T \Rightarrow p \vee F \equiv T \Rightarrow p \equiv T \Rightarrow A - \text{виновен}.$$

Здесь были выполнены равносильные преобразования.

Обобщением понятия сложного высказывания является понятие булевой функции.

Рассмотрим двухэлементное множество $B = \{0, 1\}$.

Определение 8. Всякое отображение $f : \underbrace{B \times B \times \ldots \times B}_{n \text{ раз}} \to B$ называется **булевой функцией**.

Обозначение: $f(x_1, x_2, \ldots, x_n)$, где $x_i = \{0, 1\}$ и $f \in \{0, 1\}$.

Иногда булевы функции называют логическими функциями.

Набор элементов, на которых $f = 1,$ называются *единичными*.

Булевы функции можно задавать таблицей. Удобно набор элементов записывать в порядке возрастания соответствующего двоич-

ного числа. Такой порядок называется *лексикографическим*. Число различных наборов для функции n-аргументов $f(x_1, x_2, ..., x_n)$ равно

$$\underbrace{2 \cdot 2 \cdot ... \cdot 2}_{n \text{ раз}} = 2^n .$$

Таким образом, соответствующая таблица будет иметь 2^n строк. В каждой строке на позиции для значения булевой функции f имеется 2 возможности – 0 или 1. Поэтому число различных булевых функций n аргументов равно

$$\underbrace{2 \cdot 2 \cdot ... \cdot 2}_{2^n \text{ раз}} = 2^{2^n} .$$

В частности, при $n = 1$ имеем $2^2 = 4$ функций;

при $n = 2$ имеем $2^{2^2} = 2^4 = 16$ функций;

при $n = 3$ имеем $2^{2^3} = 2^8 = 256$ функций.

С ростом n резко возрастает число различных функций. Кроме того, при больших n таблицы истинности становятся громоздкими. Поэтому возникает необходимость в разработке алгебры булевых функций.

Прежде чем переходить к изучению этой алгебры, рассмотрим более подробно функции одного и двух аргументов (табл. 1, 2).

Таблица 1

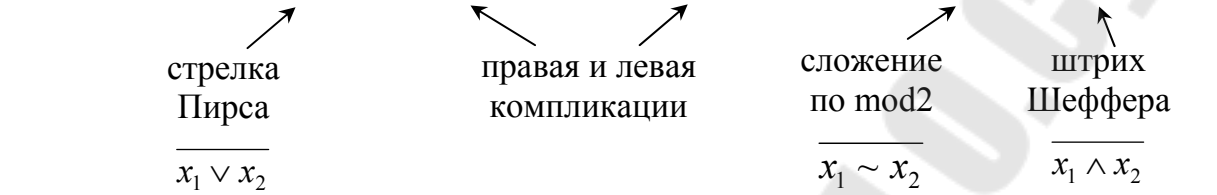
	f_1	f_2	f_3	f_4
x	0	$\bar{x}$	x	1
0	0	1	0	1
1	0	0	1	1

$\Rightarrow$ f_1 – константа 0; f_2 – отрицание x; f_3 – переменная x; f_4 – константа 1

Функцию $f_2 \equiv \bar{x}$ можно рассматривать как унарную операцию.

Таблица 2

		f_1	f_2	f_3	f_4	f_5	f_6	f_7	f_8
x_1	x_2	0	$x_1 \downarrow x_2$	$\bar{x}_1$	$\bar{x}_1$	$x_1 \leftarrow x_2$	$\bar{x}_2$	$x_1 \oplus x_2$	$x_1 \mid x_2$
0	0	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1
1	1	0	0	0	0	0	0	0	0



Продолжение табл. 2

		f_9	f_{10}	f_{11}	f_{12}	f_{13}	f_{14}	f_{15}	f_{16}
x_1	x_2	$x_1 \wedge x_2$	$x_1 \sim x_2$	x_2	$x_1 \Rightarrow x_2$	x_1	$x_1 \Leftarrow x_2$	$x_1 \vee x_2$	1
0	0	0	1	0	1	0	1	0	1
0	1	0	0	1	1	0	0	1	1
1	0	0	0	0	0	1	1	1	1
1	1	1	1	1	1	1	1	1	1

Функции $x_1 \downarrow x_2$, $x_1 \rightarrow x_2$, $x_1 \leftarrow x_2$, $x_1 \Rightarrow x_2$, $x_1 \Leftarrow x_2$, $x_1 \sim x_2$, $x_1 \wedge x_2$, $x_1 \vee x_2$, $x_1 \mid x_2$, $x_1 \oplus x_2$ можно рассматривать и как бинарные операции. А поскольку аргументы и функции f принимают значения на одном и том же множестве $B = \{0, 1\}$, то булевы функции $\{f, g, ...\}$ могут быть аргументами другой булевой функции. Тем самым мы приходим к тесной связи между композицией функций и логическими операциями.

Пусть имеется некоторое множество M булевых функций одинакового числа аргументов.

Определение 9. Множество M булевых функций называется **замкнутым классом**, если всякая суперпозиция из M снова принадлежит M.

Очевидно, что в силу конечности M любая система Σ булевых функций порождает замкнутый класс. Такой класс называется *замыканием* $[\Sigma]$.

Пример

1. Множество всех дизъюнкций есть замкнутый класс.
2. Множество всех конъюнкций есть замкнутый класс.

Чрезвычайно интересны системы функций, чьи замыкания совпадают со всем множеством булевых функций. В этом случае любая булева функция может быть представлена через композицию булевых функций из такой системы.

Определение 10. Система функций Σ называется **функционально полной**, если любая логическая функция представима в виде суперпозиций функций из системы Σ.

Важнейшей функционально полной системой является система $\Sigma_0 = \{\wedge, \vee, \neg\}$.

Очевидно, что если все функции функционально полной системы Σ представимы в виде композиции (суперпозиции) функции из системы Σ^*, то система Σ^* тоже будет функционально полной.

Пример

1. Так как $x_1 \vee x_2 = \overline{\bar{x}_1 \wedge \bar{x}_2}$, то $\{\wedge, \neg\}$ есть функционально полная система.

2. $x_1 \wedge x_2 = \overline{\bar{x}_1 \vee \bar{x}_2} \Rightarrow \{\vee, \neg\}$ – функционально полная система.

3. $\{\wedge, \oplus, 1\}$ – функционально полная система (алгебра Жегалкина).

4. $\{|\}$ и $\{\downarrow\}$ – функционально полные системы, состоящие всего лишь из одной булевой функции.

Линейная функция – это функция, представленная в виде $\alpha_1 x_1 \oplus \alpha_2 x_2 \oplus ... \oplus \alpha_n x_n \oplus \beta$, где α_i и β – константы 0 и 1 (линейный многочлен Жегалкина).

Монотонная функция – это функция, для которой из того, что $\sigma \le \tau$ следует, что $f(\sigma) \le f(\tau)$. (Порядок на двоичных наборах вводится так: $\sigma(\sigma_1,...,\sigma_n) \le \tau(\tau_1,...,\tau_n)$, если $\sigma_k \le \tau_k$ для $\forall\ k = \overline{1,n}$.)

Самодвойственная функция – это функция, для которой $f(\bar{x}_1, \bar{x}_2, ..., \bar{x}_n) = \bar{f}(x_1, x_2, ..., x_n)$.

Сохраняющая 0 функция – это функция, для которой $f(0,0,..,0) = 0$.

Сохраняющая 1 функция – это функция, для которой $f(1,1,..,1) = 1$.

Вообще имеется общий критерий функциональной полноты.

Теорема Поста. Для того, чтобы система функций Σ была функционально полной, необходимо и достаточно, чтобы она содержала хотя бы одну:

1) нелинейную;

2) немонотонную;

3) несамодвойственную;
4) не сохраняющую 0;
5) не сохраняющую 1 функции.

ЛЕКЦИЯ 6
ПРЕДСТАВЛЕНИЯ БУЛЕВЫХ ФУНКЦИЙ И ИХ УПРОЩЕНИЕ

Как следует из предыдущей лекции, всякую булеву функцию можно представить в виде композиции функций, образующих полную систему. Среди всех полных систем выделяется (в силу простоты) система

$$\Sigma_0 = \{\vee, \wedge, \neg\}.$$

Всякая формула, образованная с помощью системы Σ_0, называется ***булевой*** формулой.

Пример

Булевы формулы:

$$\overline{x \vee y} \wedge z; \overline{x \vee y \vee z} \text{ и т. п.}$$

Однако среди всех булевых формул можно выделить наиболее простые.

Определение 1. **Элементарной конъюнкцией** (одночленом) называется булева функция, составленная из символов $\{x_1, x_2, ..., x_n; \bar{x}_1, \bar{x}_2, ..., \cdots \bar{x}_n\}$ с помощью только операций конъюнкции.

Очевидно, что длина конъюнкции, т. е. число «сомножителей», не превышает n, так как в противном случае обязательно появится контрадикция $x_k \wedge x_k$.

Определение 2. Конъюнкции максимальной длины n называются **конституэнтами** 1.

Общее число конституэнт 1 равно 2^n. Название отражает тот факт, что конституэнта обращается в 1 только на одном единственном наборе аргументов.

Далее удобно ввести следующие обозначения:

$$x^{\alpha} = \begin{cases} x, & \alpha = 1, \\ \bar{x}, & \alpha = 0. \end{cases} \qquad (37)$$

Тогда произвольная конъюнкция может быть записана в виде

$$x_{i_1}^{\alpha_i} x_{i_1}^{\alpha_{i2}} \ldots x_{i_m}^{\alpha_{i_m}}, \quad m \le n,$$

а конституэнты единицы есть

$$x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}.$$

Пример

Выписать все элементарные конъюнкции, составленные для двух аргументов, отличные от констант.

Решение

$$\{x_1, x_2, \bar{x}_1, \bar{x}_2, x_1 x_2, \bar{x}_1 x_2, x_1 \bar{x}_2, \bar{x}_1 \bar{x}_2\}.$$

Всего их восемь. Последние 4 формулы являются конституэнтами 1.

Определение 3. Всякая дизъюнкция элементарных конъюнкций называется **дизъюнктивной нормальной формой** (ДНФ):

$$\bigvee_{(\alpha_{i_1} \alpha_{i_2} \ldots \alpha_{i_m})} x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} \ldots x_{i_m}^{\alpha_{i_m}}. \qquad (38)$$

Естественно, что ДНФ есть булева функция.

Интересна обратная задача сопоставления произвольной булевой функции некоторой ДНФ. Эта задача всегда имеет решение в силу полноты системы $\Sigma_0 = \{\vee, \wedge, \neg\}$. Однако возникает вопрос о количестве решений этой задачи. К сожалению, в случае произвольной постановки, т. е. без фиксирования числа аргументов, она имеет неограниченное множество решений. Другими словами, всякая булева функция может быть записана в форме ДНФ бесчисленным количеством способов. Поэтому для определенности зафиксируем число аргументов, т. е. будем рассматривать класс булевых функций n аргументов. Как было установлено нами в лекции 4, число различных функций вида $f(x_1, x_2, ..., \cdots x_n)$ равно 2^{2^n}.

Подсчитаем число различных ДНФ, которые можно составить из n аргументов. Число различных элементарных конъюнкций $x_{i_1}^{\alpha_{i_1}} x_{i_2}^{\alpha_{i_2}} \ldots x_{i_m}^{\alpha_{i_m}}$, $m = \overline{1,n}$ равно 3^n. Следовательно, число различных ДНФ будет равно 2^{3^n}. Так как $2^{2^n} < 2^{3^n}$, то очевидно, что некоторые ДНФ представляют одни и те же функции. Среди таких ДНФ выделим особый класс, в который входят только ДНФ, составленные из конституэнт единицы. Такие ДНФ называются совершенными дизъюнктивными формами (СДНФ).

Теорема 1. Всякая булева функция представляется единственным образом в виде своей СДНФ:

$$f(x_1, x_2, \ldots x_n) = \bigvee_{f(\alpha_1, \alpha_2, \ldots, \alpha_n)=1} x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n}, \qquad (39)$$

где дизъюнкция берется по единичным наборам функции f.

Из теоремы следует, что СДНФ можно построить по таблице истинности, используя единичные наборы.

Пример

$x_1 \Rightarrow x_2$:

x_1	x_2	$x_1 \Rightarrow x_2$
0	0	1
0	1	1
1	0	0
1	1	1

$\Rightarrow$ СДНФ: $x_1 \Rightarrow x_2 \equiv \bar{x}_1\bar{x}_2 \vee \bar{x}_1 x_2 \vee x_1 x_2$.

Единственность СДНФ позволяет легко установить равенство булевых функций, а именно, булевы функции, для которых СДНФ совпадают, равны.

Как уже отмечалось, при большом количестве аргументов представление булевых функций таблицами неудобно. При этом важность приобретают алгебраические способы получения ДНФ и СДНФ. Можно отметить следующие приемы и методы:

1) с помощью правил де Моргана и двойного отрицания ($\bar{\bar{x}} = x$) все отрицания преобразуются в отрицания для переменных;

2) лишние конъюнкции и повторения переменных удаляются с помощью соотношений

$$xx = x, \quad x \vee x = x, \quad x\bar{x} = 0, \quad x \vee \bar{x} = 1;$$

3) константы удаляются с помощью соотношений

$$x \wedge 0 = 0, \quad x \wedge 1 = x, \quad x \vee 0 = x, \quad x \vee 1 = 1;$$

4) упрощение ДНФ часто достигается с помощью правила поглощения $x \vee xF = x$;

5) восстановление фиктивных переменных для получения СДНФ достигается с помощью расщепления единицы: $1 = x_i \vee \bar{x}_i$.

Пример

Получить СДНФ для функции $F = \overline{x_1 \Rightarrow x_2} \vee \overline{x_3 \Rightarrow x_2}$.

Решение

Последовательно находим:

$$F = \overline{x_1 \Rightarrow x_2} \vee \overline{x_3 \Rightarrow x_2} \equiv \overline{\bar{x}_1 \vee x_2} \vee \overline{\bar{x}_3 \vee x_2} \equiv x_1\bar{x}_2 \vee x_3\bar{x}_2 \quad (\text{ДНФ}) \equiv$$

$$\equiv x_1\bar{x}_2 \cdot 1 \vee 1 \cdot \bar{x}_2 x_3 \equiv x_1\bar{x}_2x_3 \vee x_1\bar{x}_2\bar{x}_3 \vee x_1\bar{x}_2x_3 \vee \bar{x}_1\bar{x}_2x_3 \equiv$$

$$\equiv x_1\bar{x}_2x_3 \vee x_1\bar{x}_2\bar{x}_3 \vee \bar{x}_1\bar{x}_2x_3 \quad - \text{ СДНФ}.$$

Существуют и другие формы представления булевых функций, в частности, конъюнктивная нормальная форма (КНФ), совершенная конъюнктивная нормальная форма (СКНФ) и др.

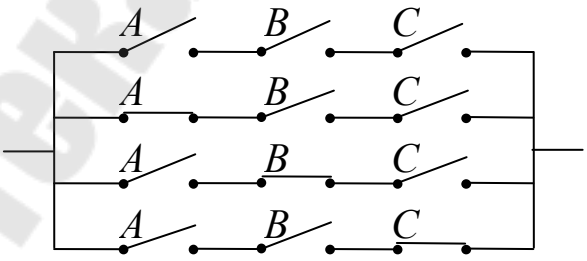
В 30-х годах прошлого века французский физик Эренфест предложил использовать аппарат булевых функций для анализа работы контактно-релейных схем (РКС). В настоящее время это направление привело к широкому проникновению алгебры булевых функций в расчет электронных схем.

Пример

Описать работу системы электронного голосования для трех голосующих.

Решение

При голосовании трех человек решение будет принято, если за него проголосуют не менее двух голосовавших. Сопоставим каждому голосующему переключатели A, B и C. Тогда, если в качестве принятия решения рассматривать положение ключей в разомкнутом виде, то схема будет иметь вид:



$$\Rightarrow F(A,B,C) = ABC \vee \bar{A}BC \vee A\bar{B}C \vee AB\bar{C}.$$

Одной из важнейших задач в алгебре булевых функций является задача минимизации формы функционального представления. Здесь на первом этапе необходимо выработать критерии минимальной формы.

Пусть имеется ДНФ булевой функции

$$f(x_1, x_2, ...x_n) = K_1 \vee K_2 \vee ... \vee K_s,$$

где K_i, $i = \overline{1,s}$ – элементарные конъюнкции. Назовем число s *длиной* ДНФ.

Определение 4. ДНФ булевой функции $f(x_1, x_2, ..., x_n)$ называется **кратчайшей**, если она содержит наименьшее число s элементарных конъюнкций по сравнению с другими ДНФ этой же функции $f(x_1, x_2, ..., x_n)$.

Рассмотрим некоторую элементарную конъюнкцию

$$K = x_1^{\alpha_1} x_2^{\alpha_2} ... x_r^{\alpha_r}.$$

Число входящих в нее символов r называют ее *рангом*. Тогда ДНФ можно характеризовать числом, равным сумме рангов конъюнкций:

$$R = r_1 + r_2 + .. + r_s. \tag{40}$$

Это число естественно назвать *рангом* ДНФ булевой функции.

Определение 5. ДНФ булевой функции $f(x_1, x_2, ..., x_n)$ называется **минимальной**, если ей соответствует наименьший суммарный ранг R по сравнению с другими ДНФ этой же функции.

Таким образом, в классе ДНФ обычно формулируют одну из следующих задач: найти кратчайшую или минимальную ДНФ заданной функции $f(x_1, x_2, ..., x_n)$. При $n > 5$ эти ДНФ могут не совпадать.

Поиск минимальной ДНФ есть достаточно сложная задача. При этом весьма полезно следующее понятие.

Определение 6. Пусть f и g две булевы функции, определенные на множестве $\{(x_1, x_2, ..., x_n)\}$. Тогда если

$$f \Rightarrow g \equiv 1, \tag{41}$$

то говорят, что функция f **имплицирует *g***.

Соотношение (5) может быть заменено эквивалентным ему соотношением

$$f \vee g \equiv g. \tag{42}$$

Из последнего легко установить, что все нулевые наборы функции f являются также нулевыми и для функции g.

Если функция g представлена в форме ДНФ, то в качестве имплицирующей функции f может выступать любая элементарная конъюнкция из ДНФ:

$$K_i \vee (K_1 \vee ... \vee K_i \vee ... K_s) \equiv K_1 \vee ... \vee K_i \vee ... K_s .$$

По этой причине элементарная конъюнкция

$$K = x_1^{\alpha_1} x_2^{\alpha_2} ... x_r^{\alpha_r}$$

называется ***импликантой***, соответствующей булевой функции. Если при удалении хотя бы одного символа из K конъюнкция перестает быть импликантой, то она называется *простой импликантой*.

Пример

$f(x_1, x_2, x_3) = x_1 x_2 \vee x_1 x_3 \Rightarrow K_1 = x_1 x_2$ и $K_2 = x_1 x_3$ – простые импликанты. Нетрудно убедиться, что $K_3 = x_1 x_2 x_3$ тоже импликанта f:

$$f \vee K_3 = x_1 x_2 \vee x_1 x_3 \vee x_1 x_2 x_3 = x_1 x_2 (\underbrace{1 \vee x_3}_{\equiv 1}) \vee x_1 x_3 = f .$$

Но K_3 не является простой импликантой.

Понятно, что чем меньше символов содержит импликанта, тем проще ДНФ.

Теорема 2. Всякая булева функция может быть представлена в виде ДНФ простых импликант.

Определение 7. Дизъюнкция всех простых импликант функции $f(x_1, x_2, ..., x_n)$ называется ее **сокращенной** ДНФ.

Вообще сокращенную ДНФ можно получить из СДНФ, просматривая каждую конституэнту единицы. Но, во-первых, эта задача очень громоздкая, а во-вторых, она зависит от порядка просмотра. Было установлено, что сокращенная ДНФ может содержать $l_c(n) \le \frac{3^n}{\sqrt{n}}$ простых импликант, что больше, чем конституэнт единицы! (Сокращенная ДНФ может иметь длину большую, чем СДНФ).

Определение 8. ДНФ, из которой нельзя удалить ни одного импликанта, называется **тупиковой**.

Пример

$f(x, y, z) = xz \vee y\bar{z} \vee xy$ – сокращенная ДНФ. Преобразуем ее:

$$f(x,y,z) = xz \vee y\bar{z} \vee xy \cdot \underbrace{1}_{=z\vee\bar{z}} = xz \vee y\bar{z} \vee xyz \vee xy\bar{z} =$$

$$= z(\underbrace{x \vee xy}_{=x}) \vee \bar{z}(\underbrace{y \vee xy}_{=y}) = xz \vee y\bar{z} \text{ – другая сокращенная ДНФ.}$$

Видно, что из первой ДНФ можно удалить одну импликанту, следовательно, она может быть упрощена. Вторая ДНФ является тупиковой ДНФ.

Для поиска тупиковых ДНФ полезен метод, основанный на построении *таблицы покрытия единицы*. Множество единичных наборов функции f называется ее *единичным интервалом*. Понятно, что совокупность единичных интервалов элементарных конъюнкций, входящих в какую-нибудь сокращенную ДНФ f покрывает единичный интервал f. Если удаление конъюнкции не меняет покрытия, то мы приходим к более простой ДНФ.

Пример

Построить таблицу покрытия единицы для функции

$$f(x,y,z) = xz \vee y\bar{z} \vee xy .$$

Решение

Таблица имеет вид:

	1 1 0	1 1 1	1 0 1	1 0 0
xy	1	1		
xz		1	1	
$x\bar{z}$	1			1
$x\bar{z}$	1			1

$\Rightarrow M_f = \{(110),(111),(101),(100)\}$ – единичный интервал для функции f. Удаление xy не меняет множества M_f, следовательно, $f = xz \vee y\bar{z} \vee xy \equiv xz \vee y\bar{z}$ – тупиковая ДНФ.

Общая схема минимизации:

– построение сокращенной ДНФ;

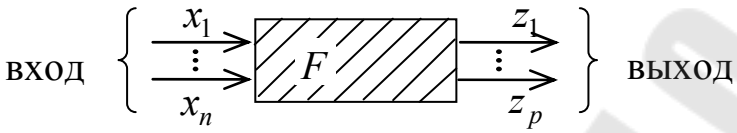
– нахождение тупиковых ДНФ;

– нахождение минимальной ДНФ.

В общем случае для реализации этой схемы используется целый ряд приемов и методов кроме рассмотренных выше: геометрический метод, метод Квайна-Мак-Класки, метод Блейка, метод Петрика, метод таблиц Вейча и др.

ЛЕКЦИЯ 7
СИНТЕЗ СХЕМ ИЗ ФУНКЦИОНАЛЬНЫХ ЭЛЕМЕНТОВ

В современной электронике, т. е. в технике управляющих и вычислительных устройств, важное место занимают дискретные преобразователи:



Устройство F осуществляет преобразование входных сигналов $\{x_1, x_2, ..., x_n\}$ в выходные $\{z_1, z_2, ..., x_p\}$. Важным подклассом дискретных преобразователей является класс устройств, в которых временем преобразования можно пренебречь по сравнению с длительностью сигналов.

Математической моделью таких устройств являются так называемые ***схемы из функциональных элементов*** (СФЭ).

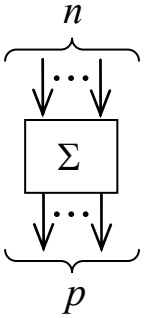
Понятие СФЭ довольно сложное и в нем можно выделить две части:

1) *структурную*, которая включает в себя описание способов соединения конструкционных элементов;

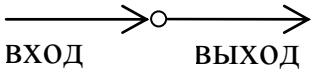
2) *функциональную*, которая, по существу, и ответственна за работу всей СФЭ.

Конструкционные особенности схемы можно описать, предварительно проклассифицировав способы соединения элементов. Введем основные способы соединения.

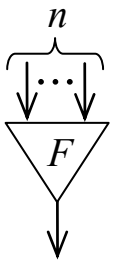
Определение 1. Устройство, имеющее n входов и p выходов назовем **логической сетью** Σ:



Сеть, у которой имеется только одна вершина и при этом вход и выход совпадают, естественно назвать ***тривиальной логической сетью***:

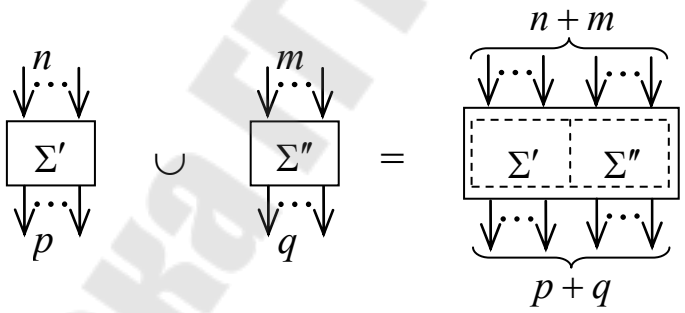


Определение 2. Логическую сеть с одним выходом назовем **элементом** F:

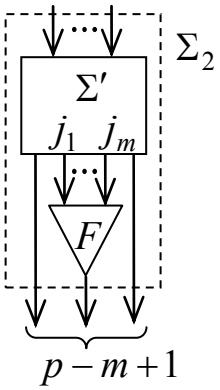


Далее введем операции над элементной базой.

Определение 3. **Объединением** двух непересекающихся сетей Σ' и Σ'', имеющих n и m входов и p и q выходов, соответственно, называется логическая сеть, имеющая $n+m$ входов и $p+q$ выходов.

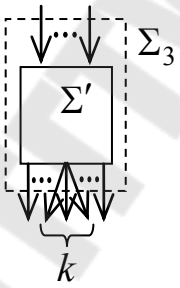


Определение 4. Пусть в заданной логической сети Σ' выделено m выходов с номерами $j_1, j_2, ..., j_m$. Подключим к Σ' элемент F, входами которого будут выделенные выходы $\{j_1, ..., j_m\}$. Такая операция называется **присоединением элемента** F к логической сети Σ'.



В результате присоединения F к Σ' получается сеть Σ_2, входы которой совпадают с входами Σ', а число выходов равно $(p-m+1)$, где p – число выходов Σ'. Очевидно, что эта операция определена только если $m \le p$.

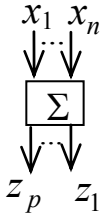
Определение 5. Операция, в результате которой выход j сети Σ' заменяется несколькими выходами $j_1, ..., j_k$, называется **операцией расщепления** выхода:



Сопоставим входам переменные $\{x_1, x_2, ..., x_n\}$, а выходам – $\{z_1, z_2, ..., z_p\}$. Тогда удобно логическую сеть обозначить как

$$\Sigma(x_1, x_2, ..., x_n;\quad z_1, z_2, ..., z_p).$$

Функционирование СФЭ описывается системой функций алгебры логики:



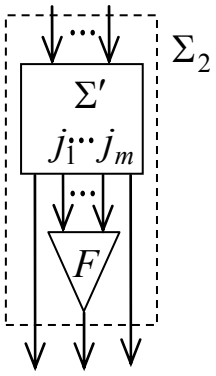
$$\Rightarrow \quad \begin{cases} z_1 = f_1(x_1, ..., x_n); \\ \ldots; \\ z_p = f_p(x_1, ..., x_n). \end{cases}$$

Если на вход подаются сигналы в виде двоичных кодов, а с выхода также снимаются показания в виде двоичных наборов, то функ-

ции f_i есть булевы функции. В дальнейшем будем рассматривать только этот случай.

Пример

Описать работу следующей схемы



Решение

Введем входной набор $\{x_1, x_2, ..., x_n\}$ и выходной набор $\{z_1, ..., z_p\}'$, где вместо символов $\{z_{j_1}, ..., z_{j_m}\}$ добавляется символ z_{p+1}, соответствующий выходу элемента F. Получим следующую систему, которая описывает работу заданной схемы:

$$\begin{cases} z_1 = f_1(x_1, ..., x_n); \\ \quad \cdots; \\ z_{j_1-1} = f_{j-1}(x_1, ..., x_n); \\ z_{j_1+1} = f_{j_1+1}(x_1, ..., x_n); \\ \quad \cdots; \\ z_{j_m-1} = f_{j_m-1}(x_1, ..., x_n); \\ z_{j_m+1} = f_{j_m+1}(x_1, ..., x_n); \\ \quad \cdots; \\ z_p = f_p(x_1, ..., x_n); \\ z_{p+1} = F(\underbrace{f_{j_1}(x_1, ..., x_n)}_{=z_{j1}}, ..., \underbrace{f_{j_n}(x_1, ..., x_n)}_{=z_{j_m}}). \end{cases}$$

Проблема синтеза СФЭ состоит в следующем. Задан базис $\{F\}$ функциональных элементов и взята произвольная система булевых уравнений:

$$\begin{cases} z_1 = f_1(x_1, ..., x_n); \\ \ldots; \\ z_p = f_p(x_1, ..., x_n). \end{cases} \qquad (43)$$

Требуется сконструировать систему $\Sigma(x_1, ..., x_n;\ z_1, ..., z_p)$ из имеющихся функциональных элементов $\{F\}$, реализующих эту систему уравнений. Понятно, что решение существует, если система $\{F\}$ полна. Но так как имеется в общем случае много решений, то из всех решений необходимо выбрать оптимальное. Для оценки меры оптимальности вводится число $L(\Sigma)$, которое называется *сложностью схемы*.

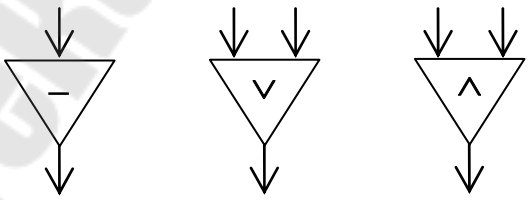
Вообще можно доказать, что существует алгоритм, который для каждой системы булевых уравнений строит минимальную схему Σ. При этом в качестве параметра $L(\Sigma)$ выбирается число элементов в схеме.

Простейший алгоритм – это алгоритм перебора. Однако он не имеет практического значения в силу его трудоемкости и больших временных затрат на реализацию.

В качестве примера рассмотрим задачу построения СФЭ, реализующую только одну булеву функцию

$$z = f(x_1, ..., x_n). \qquad (44)$$

Естественно, что схема $\Sigma(x_1, ..., x_n;\ z)$ имеет один вход. Обозначим сложность этой схемы как $L(f)$. В качестве элементарной базы возьмем базис F, состоящий из инвертора, дизъюнктора и конъюнктора:



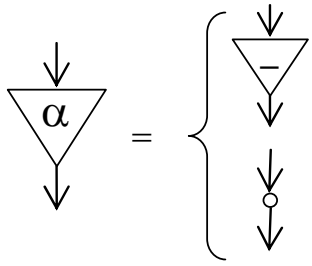
I. *Метод синтеза, основанный на СДНФ*

Представим функцию f в виде СДНФ:

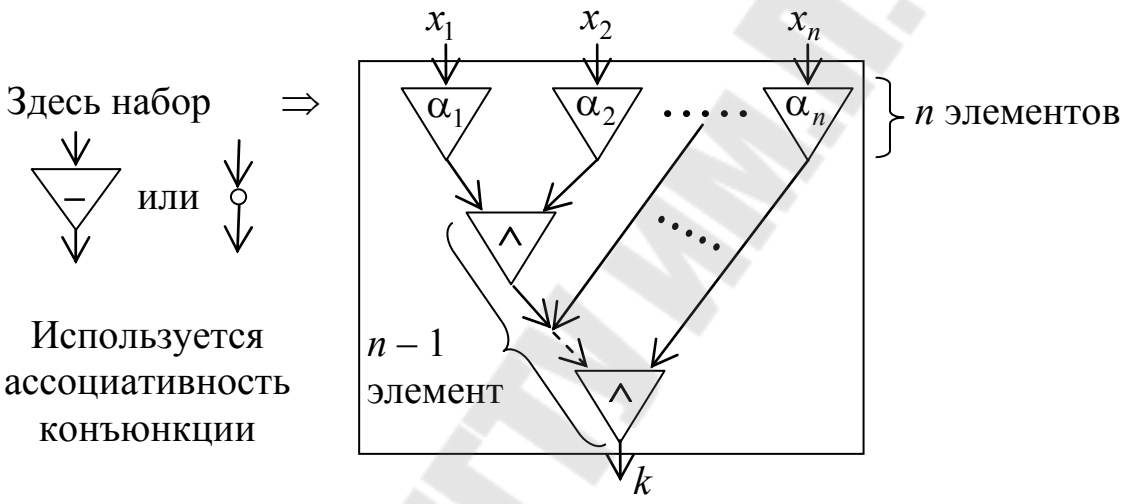
$$z = f(x_1, x_2, ..., x_n) = \bigvee_{i=1}^{s} k_i,$$

где $k_{(i)} = x_1^{\alpha_1} x_2^{\alpha_2} ... x_n^{\alpha_n}$ – конституэнты единицы.

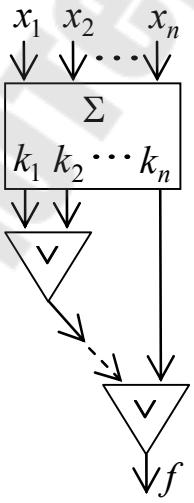
Введем вспомогательный элемент:



Тогда схема Σ'_k, соответствующая конъюнкции k, реализуется следующим образом:



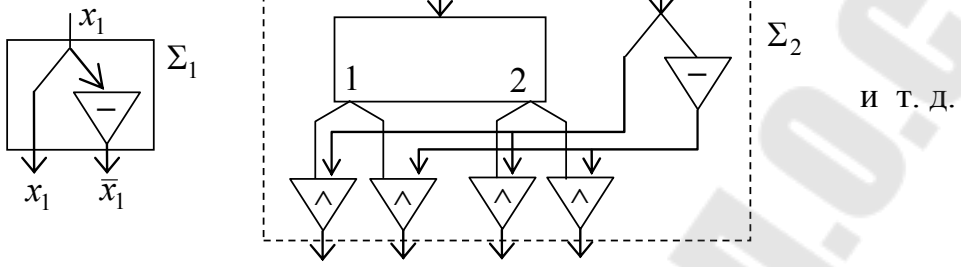
Очевидно, что $L[\Sigma_k] \le n + (n-1)$. Далее, объединяя схемы Σ_{k_1}, Σ_{k_2}, …, Σ_{k_s}, получим схему с выходами $k_1, k_2, ..., k_s$. Подключая дизъюнкторы, окончательно получаем:

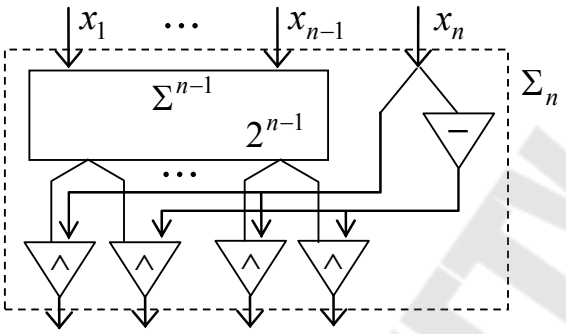


Сложность этого алгоритма $L_{A_1}(n) \le n2^n$.

II. *Метод синтеза, основанный на реализации ДНФ*

Рассмотрим последовательное конструирование многополюсника Σ_n, который реализует множество всех конъюнкций $\{x_1^{\alpha_1} ... x_p^{\alpha_p}\}$:





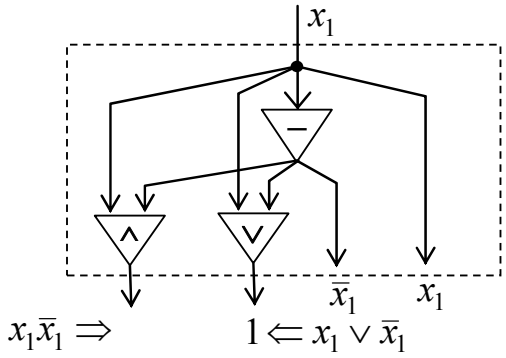
Для этого алгоритма
$L_{A_2}(n) \le 3 \cdot 2^n + n - 5$

Для построения схемы, реализующей конкретную функцию $f(x_1, ..., x_n)$, необходимо в многополюснике Σ^n отобрать выходы, соответствующие членам СДНФ $k_1, ..., k_s$ функции f, и подключить их к схеме из дизъюнкторов, осуществляющей логическое сложение. При этом можно удалить лишние элементы.

Существуют и другие схемы реализации f. Следует отметить, что алгоритмы со сложностью $L(n) \to L_{\min}$ становятся более конструкционно сложными.

Пример

Универсальный многополюсник, реализующий *все функции одной переменной*.



Его можно рассматривать как основной блок для реализации метода Шеннона. При этом

$$L[U_n] \le 2 \cdot 2^{2^n}.$$

В методе Шеннона

$$L_{A_n} \le 8\frac{2^n}{n}.$$

Общая теория синтеза СФЭ приводит к важному выводу о том, что большинство булевых функций при больших n имеют сложные минимальные схемы. Это означает, что практическую ценность представляет очень узкий класс булевых функций. Поэтому наряду с универсальными методами синтеза необходимо иметь методы синтеза, приспособленные к отдельным классам булевых функций, полнее учитывающие свойства этих функций.

В качестве примера рассмотрим синтез сумматора.

Синтез сумматора. Рассмотрим построение многополюсной схемы, реализующей сложение двух чисел, заданных в двоичной системе счисления. Известен алгоритм сложения «столбиком»:

$$\begin{array}{r} (q_{n+1}q_n \ldots q_1) \\ x_n \ldots x_1 \\ + \\ y_n \ldots y_1 \\ \hline z_{n+1}z_n \ldots z_1 \end{array}$$

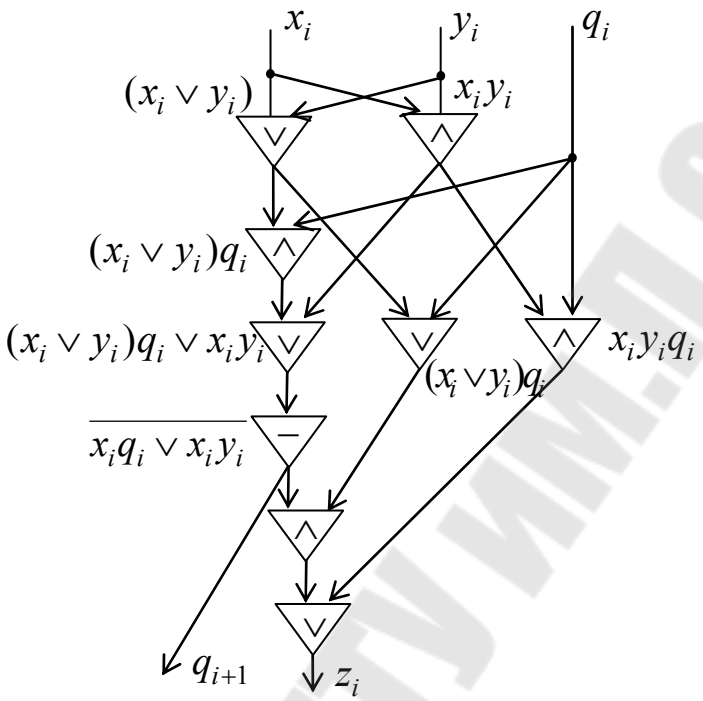
Здесь числа $q_{n+1}, ..., q$ означают результаты переносов из предыдущих разрядов ($q_1 = 0$). Очевидно,

$$z_i = x_i + y_i + q_i \pmod 2.$$

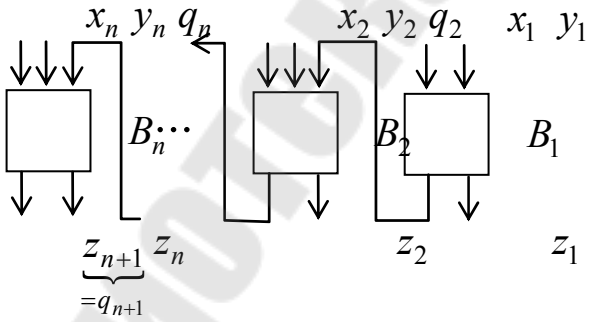
Справедливо тождество

$$z_i = x_i + y_i + q_i = \overline{x_i y_i \vee x_i q_i \vee y_i q_i} \wedge (x_i \vee y_i \vee q_i) \vee x_i y_i q_i .$$

Тогда ее реализация имеет вид:



Обозначим этот блок как $B_i (1 < i < \varepsilon_n)$. Тогда сумматор для двух n разрядных двоичных чисел получается путем последовательного соединения блоков B_i.



$$L[\Sigma_n] \le q_n - 5$$

ЛЕКЦИЯ 8
ЭЛЕМЕНТЫ ТЕОРИИ ГРАФОВ

Начало теории графов можно отнести к 1736 году, когда Л. Эйлер решил популярную в то время задачу о кенигсбергских мостах. Этот результат более ста лет был единственным результатом в теории графов. И лишь в конце 19 века инженер-электрик Г. Кирхгофф применил теорию деревьев к анализу электрических цепей. Затем математик Кэли решил перечислительную задачу соединения углеводородов опять же с помощью теории деревьев. К этому периоду относится и задача о четырех красках.

В настоящее время теория графов является неотъемлемой частью инженерного образования. Достаточно отметить в связи с этим проектирование систем управления, исследование автоматов, логических цепей, блок-схем программ, теории расписаний и т. п.

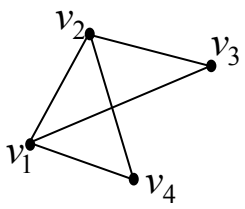
Сам термин «граф» впервые ввел в 1936 году венгерский математик Кениг. Для универсального введения понятия графа используется язык теории множеств.

Определение 1. Пусть V – непустое конечное множество, а $V^{(2)}$ – множество всех его двух элементарных подмножеств. Если $E \subseteq V^{(2)}$, то пара $G(V,E)$ называется **конечным неориентированным графом**. При этом элементы V называются *вершинами*, а E – *ребрами* графа G.

Число вершин естественно называть *порядком* графа:

$$|V_G| = n.$$

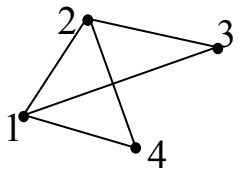
Наглядно граф изображается на плоскости в виде точек, соединенных отрезками-ребрами.



Если отрезок $[u,v] \subseteq E$, то вершины u и v называются *смежными*. Смежными также называются и ребра, имеющие общий конец. Если вершина v является концом ребра e, то v и e называются *инцидентными*.

Определение 2. Множество всех вершин, смежных с вершиной v, называются ***окрестностью*** N_v вершины v.

Пример

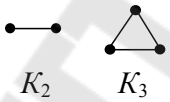


Окрестность вершины v_4: $N_4 = \{1,2\}$; вершины v_3 и v_4 несмежны; ребра $(2, 3)$ и $(1, 4)$ несмежны.

Определение 3. Если $E = \varnothing$, т. е. нет ребер, то граф G называется **пустым**.

Обозначение: $O_n \Rightarrow$  …

Определение 4. Граф, у которого все вершины смежны, называется *полным*.

Обозначение: $K_n \Rightarrow$  …

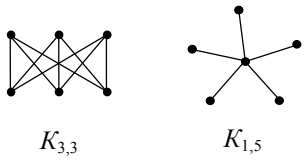
Задача. Найти число ребер графа K_n.

Решение

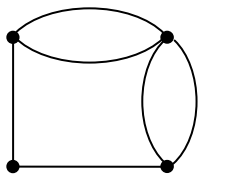
Так как ребро определяется выбором двух вершин, то число ребер для полного неориентированного графа равно числу сочетаний двух элементов из n: $| E |= C_n^2 = \dfrac{n(n-1)}{2}$.

Ответ: $\dfrac{1}{2}n(n-1)$.

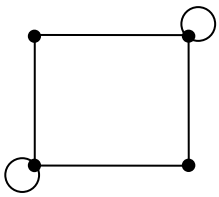
Определение 5. Если множество вершин графа VG можно разбить на 2 подмножества V_1G и V_2G так, что в каждом подмножестве нет смежных вершин, а любые две вершины $u \in V_1G$ и $w \in V_2G$ смежны, то граф называется **полным двудольным**.

Обозначение: $K_{m,n} \Rightarrow$ 

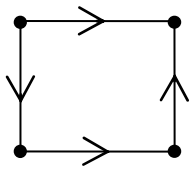
Кроме простых неориентированных графов вводятся также следующие типы графов:



– мультиграф: граф, допускающий кратные ребра;



– псевдограф: граф, допускающий петли;



– орграф (ориентированный граф).

Язык теории множеств очень удобен как для выделения частей графов, так и для ввода операций над ними.

Определение 6. Граф H называется **подграфом графа** G, если $VH \subseteq VG$ и $EH \subseteq EG$.

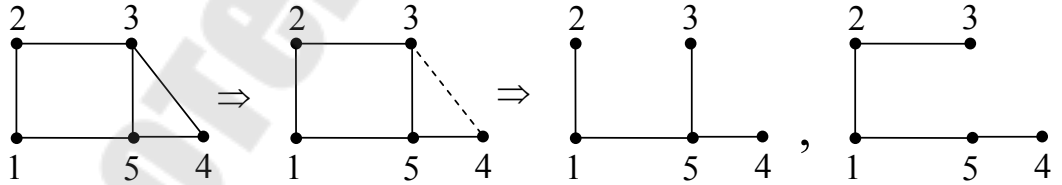
Важными случаями подграфа являются

– остовный подграф: $VH = VG$, $EH \subseteq EG$;

– порожденный подграф: $VH \subseteq VG$ и в подграфе присутствуют все ребра, которые имелись в графе G;

– дерево графа: $VH = VG$, при этом остается минимальное число ребер, сохраняющих связанность.

Пример



Граф G Остов Дерево Дерево

Основные операции над графами

1. Объединение $G_1 \cup G_2$: $VG = VG_1 \cup VG_2$, $EG = EG_1 \cup EG_2$.

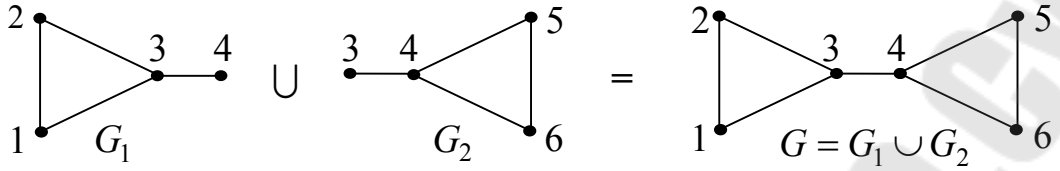
2. Дополнение $\overline{G}$: $V\overline{G} = VG$, $E\overline{G} = V_G^{(2)} \setminus EG$.

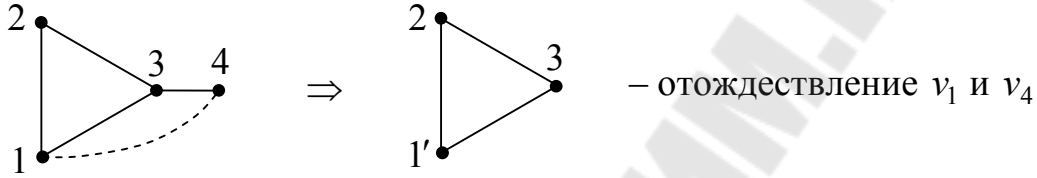
3. Отождествление вершин: $u \equiv v \Rightarrow N_\omega = N_u \cup EG$.

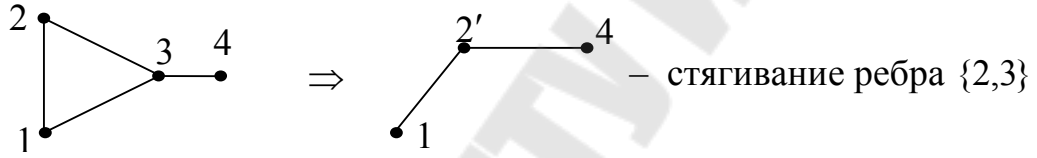
4. Стягивание ребра (отождествление его концов).

Стягивание ребра, по существу, есть отождествление смежных вершин.

Пример







Определение 7. Чередующаяся последовательность вершин и ребер

$$\{v_1, e_1, v_2, e_2, ..., v_k, e_{k+1}\},$$

такая, что $e_i = \{v_i v_{i+1}\}$ называется **маршрутом**.

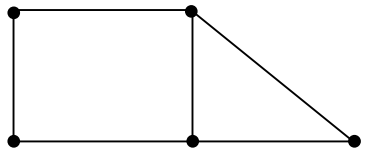
Естественно число ребер отождествить с длиной маршрута l. Если в маршруте нет совпадающих ребер, то он называется ***цепью***, а если различны как ребра, так и вершины, то ***простой цепью***:

цепь, но не простая простая цепь

Важным типом маршрутов является **циклические маршруты**, у которых $v_1 = v_{k+1}$. В частности, циклическая цепь называется **циклом**, а простая циклическая цепь – **простым циклом**.

Определение 8. Минимальная длина циклов графа называется его **обхватом**.

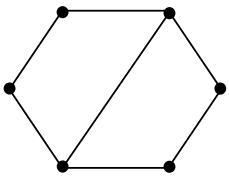
Задача. Найти обхват графа



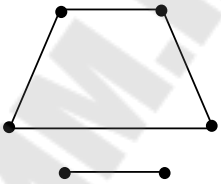
Ответ: 3.

Определение 9. Граф называется **связным**, если любые две его вершины могут быть соединены маршрутом.

Пример



связный граф



двусвязный граф

Понятно, что каждый граф может быть представлен в виде дизъюнктивного объединения своих связных компонент.

Интересна следующая задача: сколько ребер может иметь k-связный граф (т. е. граф, имеющий k-связных компонент) порядка n?

Теорема 1. Если $k(G) = k$, то для n-вершинного графа G число ребер m удовлетворяет неравенству

$$n - k \le m(G) \le \frac{(n-k)(n-k+1)}{2}.$$

Определение 10. **Степенью вершины** $\deg v$ называется число ребер с ней инцидентных.

Лемма «о рукопожатиях»

Сумма степеней всех вершин графа G равна удвоенному числу ребер:

$$\sum_{v \in V_G} \deg v = 2m_G.$$

Следствие. Во всяком графе число вершин нечетных степеней четно.

Определение 11. Графы, у которых все вершины имеют одинаковые степени, называются **регулярными**.

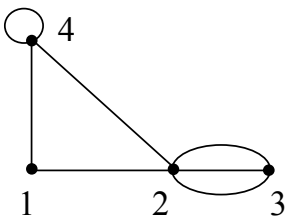
Относительно регулярных графов можно сказать, что не существует регулярных графов нечетного порядка с нечетной степенью $\deg G$.

Интересным с точки зрения компьютерной реализации является матричный способ задания графов. Введем в рассмотрение так называемые булевы матрицы, элементы которых есть целые неотрицательные числа.

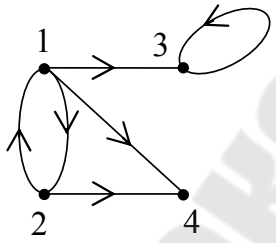
Определение 12. Матрица A, элементы которой равны 1, если вершины i и j смежны, и 0, если несмежны, называется **матрицей смежности** графа G.

Ясно, что матрица смежности симметрична, а число единиц в i-ой строке равно степени вершины i. Безусловно, матрицу смежности можно ввести и для более общих типов графов.

Пример



$$\Rightarrow \begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 3 & 1 \\ 0 & 3 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$



$$\Rightarrow \begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Матрицы смежности полезны для установления изоморфизма графов, т. е. графов, которые совпадают с точностью до переобозначения вершин. Так у изоморфных графов матрицы смежности имеют одинаковые ранги:

$$G \cong U \Rightarrow \operatorname{rang} G = \operatorname{rang} U .$$

Другой тип задач, который легко решается с помощью матрицы смежности, связан с определением числа маршрутов, которыми можно соединить вершины v_i и v_j.

Теорема 2. Пусть $G = (V, E)$ – граф, а A – его матрица смежности. Тогда $(A^m)_{ij}$ есть число маршрутов длины m, которыми можно соединить вершины v_i и v_j.

Следствие: Граф G порядка n связен тогда и только тогда, когда матрица $B = A + A^2 + ... + A^{n-1}$, где n – порядок графа, не имеющий нулевых элементов.

При разработке теории графов было сформулировано много интересных задач, в которых решение находилось в классах специальных графов. Следует отметить проблему планарности, существование эйлеровых и гамильтоновых циклов, задачу о четырех красках и т. п.

Интересны также и алгоритмы решения задач, например, алгоритм Краскала для двудольности. Ценность алгоритмов заключается в том, что они позволяют при решении задач со сложными графами использовать вычислительную технику.

Рассмотрим следующий алгоритм.

Алгоритм поиска в ширину

Начиная с произвольной вершины, приписываем ей номер 0. Каждой из вершин ее окрестности приписываем номер 1. Теперь рассматриваем поочередно окрестности вершины с номером 1 и каждой непомеченной вершине присваиваем номер 2. Продолжаем данный процесс, пока не останется непомеченных вершин. Если граф G связный, то *поиск в ширину* занумерует все вершины графа.

Далее разобьем множество VG на две части – A и B, отнеся к A все вершины с четными номерами, а к B – с нечетными, и рассмотрим порожденные подграфы $G(A)$ и $G(B)$. Если оба графа пусты, т. е. не содержат смежных вершин, то граф $G = (A, B, E)$ – двудольный граф. В противном случае граф G двудольным не является.

Простых способов распознавания k-дольного графа при $k > 2$ не существует.

Очевидно, что данный алгоритм поиска в ширину позволяет решить следующие задачи:

1) разбить множество вершин графа на области связности;

2) для несовпадающих вершин u и v найти кратчайшую цепь, их соединяющую;

3) в орграфе найти множество всех вершин, достижимых из вершины v.

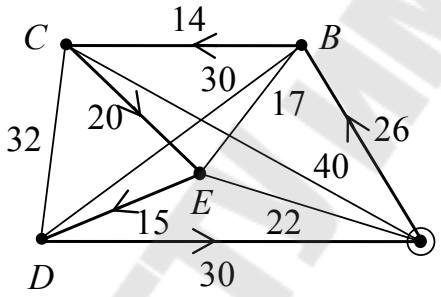
В последнее время важным является направление в теории графов, связанное с понятием сети. Сеть – это, по существу, взвешенный орграф

(т. е. орграф, каждому ребру которого поставлено в соответствие некоторое число). Такие графы позволяют моделировать графики выполнения технологических процессов, оптимизировать пропускную способность сети, оптимизировать процессы строительства и т. п.

Рассмотрим следующую задачу.

Задача о коммивояжере

Предположим, что Вы – коммивояжер (анг. – traveling salesman, и Вам требуется посетить, например, 5 городов *A*, *B*, *C*, *D*, *E*. На карте отмечены города, которые вязаны друг с другом дорогами. Числа для каждого участка соответствуют расстоянию или длине дороги. Стартуя из пункта *A*, Вы должны решить, какой порядок посещения городов выбрать так, чтобы пройденное расстояние после посещения всех городов и возвращения в начальный пункт *A* было бы *минимальным*.



Имеется множество алгоритмов решения этой задачи, но ни один из них не является универсальным. Чтобы это осознать, рассмотрим простейший *алгоритм перебора*:

1) выписать все возможные маршруты;

2) подсчитать длины маршрутов;

3) выбрать оптимальный маршрут, т. е. $l = l_{\min}$.

Результаты анализа представим в следующем виде:

1.	*ABCDEA*	109	9.	*ACDBEA*	141	17.	*ADEBCA*	116
2.	*ABCEDA*	105	10.	*ACDEBA*	130	18.	*ADECBA*	105
3.	*ABDECA*	131	11.	*ACEBDA*	137	19.	*AEBCDA*	115
4.	*ABDCEA*	130	12.	*ACEDBA*	131	20.	*AEBDCA*	141
5.	*ABEDCA*	130	13.	*ADBCEA*	116	21.	*AECBDA*	116
6.	*ABECDA*	125	14.	*ADBECA*	137	22.	*AECDBA*	130
7.	*ACBDEA*	121	15.	*ADCBEA*	115	23.	*AEDBCA*	121
8.	*ACBEDA*	116	16.	*ADCEBA*	125	24.	*AEDCBA*	109

Из таблицы следует, что оптимальными маршрутами с наикратчайшей длиной являются

ABCEDA и ADECBA.

Фактически оба маршрута совпадают, но противоположны по направлению. Для нашего примера алгоритм перебора дает решение достаточно быстро. Однако имеется одна очень серьезная проблема, связанная с тем, что с увеличением числа пунктов резко возрастает число возможных маршрутов. Закон роста – факториальный. По этой причине алгоритм перебора относится к классу тривиальных алгоритмов и для решения прикладных задач практически не применятся.

Разработка оптимальных алгоритмов является одной из важнейших задач так называемой *теории алгоритмов.*

ЛИТЕРАТУРА

1. Новиков, Ф. А. Дискретная математика для программистов / Ф. А. Новиков. – Санкт-Петербург : Питер, 2007.

2. Просветов, Г. И. Дискретная математика / Г. И. Просветов. – БИНОМ, 2008.

3. Плотников, А. Д. Дискретная математика / А. Д. Плотников. – Москва : Новое изд-во, 2006.

4. Кузнецов, О. П. Дискретная математика для инженеров / О. П. Кузнецов, Г. М. Адельсон-Вельский. – Москва : Энергия, 1980.

5. Яблонский, С. В. Введение в дискретную математику / С. В. Яблонский. – Москва : Высш. шк., 2001.

6. Вольвачев, Р. Т. Элементы математической логики и теории множеств / Р. Т. Вольвачев. – Минск : Университетское, 1986.

7. Горбатов, В. А. Фундаментальные основы дискретной математики / В. А. Горбатов. – Москва : Наука-физматлит, 1999.

8. Палий, И. А. Дискретная математика: курс лекций / И. А. Палий. – Москва : ЭКСМО, 2008.

9. Емеличев, В. А. Лекции по теории графов / В. А. Емеличев. – Москва : Наука, 1990.

10. Оре, О. Графы и их применение / О. Оре. – Москва : Мир, 1965.

Содержание

Учебное электронное издание комбинированного распространения

Учебное издание

Бабич Александр Антонович

ДИСКРЕТНАЯ МАТЕМАТИКА

Курс лекций по одноименной дисциплине для студентов инженерно-технических специальностей заочной формы обучения

Электронный аналог печатного издания

Редактор *В. В. Вороник*
Компьютерная верстка *Н. Б. Козловская*

Подписано в печать 20.09.10.
Формат 60x84/16. Бумага офсетная. Гарнитура «Таймс».
Ризография. Усл. печ. л. 3,95. Уч.-изд. л. 3,86.
Изд. № 252.
E-mail: ic@gstu.by
http://www.gstu.by

Издатель и полиграфическое исполнение:
Издательский центр учреждения образования
«Гомельский государственный технический университет
имени П. О. Сухого».
ЛИ № 02330/0549424 от 08.04.2009 г.
246746, г. Гомель, пр. Октября, 48.