



Министерство образования и науки Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новгородский государственный университет имени Ярослава Мудрого»
**МНОГОПРОФИЛЬНЫЙ КОЛЛЕДЖ
ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ**
Учебно-методическая документация

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ПРАКТИЧЕСКИМ ЗАНЯТИЯМ

ОП.08 ДИСКРЕТНАЯ МАТЕМАТИКА

Специальность:

09. 02. 01 Компьютерные системы и комплексы

Квалификация выпускника:

Техник по компьютерным системам
(базовая подготовка)

Разработчик:

Алексеева Ю.В, преподаватель ПТК НовГУ

Методические рекомендации по учебной дисциплине «Дискретная математика» приняты на заседании предметной (цикловой) комиссии дисциплин профессионального цикла колледжа, протокол №_1_от 05. 09. 2016 г.

Председатель предметной (цикловой) комиссии  / Л.Н. Цымбалюк

Оглавление

Пояснительная записка	4
Тематический план и содержание учебной дисциплины «Дискретная математика».....	6
Содержание практических занятий	9
Тема 1.1.Элементы математической логики.....	9
Практическая работа № 1. Упрощение формул алгебры высказываний.	9
Практическая работа №2. Нахождение СКНФ и СДНФ формул алгебры высказываний...	11
Тема 1.2.Основные классы функций	14
Практическая работа № 3. Нахождение полинома Жегалкина.....	14
Практическая работа № 4. Свойства булевых функций.	16
Тема 2.1. Основы теории множеств.....	20
Практическая работа № 5. Операции над множествами	20
Тема 3.1. Основные понятия алгебры предикатов	25
Практическая работа № 6. Операции над предикатами	25
Тема 4.1. Основы теории графов.....	30
Практическая работа № 7. Нахождение метрических характеристик графов.....	30
Тема 5.1.Основы комбинаторики.....	34
Практическая работа № 8 Основные комбинаторные принципы.....	34
Тема 5.2.Принцип математической индукции.....	37
Практическая работа № 9 Решение задач методом математической индукции	37
Тема 6.1.Элементы теории кодирования.....	41
Практическая работа № 10. Применение простейших криптографических шифров для шифрования текстов.....	41
ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ.....	46

Пояснительная записка

Методические рекомендации по практическим занятиям, являющиеся частью учебно-методического комплекса по дисциплине «Дискретная математика», составлены в соответствии с:

1. Федеральным государственным образовательным стандартом по специальности: 09.02.01 Компьютерные системы и комплексы;
2. Рабочей программой учебной дисциплины;
3. Положением о планировании, организации и проведении лабораторных работ и практических занятий студентов, осваивающих основные профессиональные образовательные программы среднего профессионального образования в колледжах НовГУ.

Методические рекомендации включают 10 практических занятий, предусмотренных рабочей программой учебной дисциплины в объеме 20 часов.

В результате выполнения практических заданий обучающийся должен:

уметь:

- Формулировать задачи логического характера и применять средства математической логики для их решения;
- Применять законы алгебры логики;
- Определять типы графов и давать их характеристики;
- Строить простейшие автоматы.

знать:

- Основные понятия и приемы дискретной математики;
- Логические операции, формулы логики, законы алгебры логики;
- Основные классы функций, полноту множества функций, теорему Поста;
- Основные понятия теории множеств, теоретико-множественные операции и их связь с логическими операциями;
- Логику предикатов, бинарные отношения и их виды;
- Элементы теории отображений и алгебры подстановок;
- Метод математической индукции, алгоритмическое перечисление основных комбинаторных объектов;
- Основные понятия теории графов, характеристики и виды графов;
- Элементы теории автоматов.

В практических работах предлагаемые задания носят репродуктивный, частично-поисковый характер и поисковый характер.

Основные теоретические положения даются студентам на лекциях. Перед проведением практического занятия проводится инструктаж, выдаются задания для самостоятельного выполнения. Во время проведения практической работы решение индивидуального задания проверяется, корректируется, проводится анализ решения, подводятся итоги.

Степень овладения студентами запланированных умений оценивается во время защиты практической работы. Критерием оценки практических работ является качество выполненных заданий, правильность ответов во время защиты.

Оценка «5» ставится в случае, когда результатом работы является полностью выполненная работа, даны ответы на поставленные контрольные вопросы.

Оценка «4» ставится, когда итогом работы является правильно выполненная практическая работа, но могут быть небольшие неточности при выполнении.

Оценка «3» - не выполнено до конца одно из заданий, даны ответы не на все контрольные вопросы.

Оценка «2» ставится в случае неподготовленности студента к защите практической работы.

Тематический план и содержание учебной дисциплины «Дискретная математика»

Наименование разделов и тем	Содержание учебного материала, лабораторные и практические работы, самостоятельная работа обучающихся	Объем часов	Уровень освоения
1	2	3	4
Раздел 1 Элементы математической логики			
Тема 1.1. Элементы математической логики	Содержание учебного материала		
	Предмет и задачи дискретной математики. Основные понятия математической логики. Составные высказывания. Простейшие связки. Другие связки. Логические отношения. Варианты импликации	4	1,2
	Практические занятия:		
	Практическая работа № 1. Упрощение формул алгебры высказываний. Практическая работа №2. Нахождение СКНФ и СДНФ формул алгебры высказываний.	4	
	Самостоятельная работа №1 Работа с конспектом. Решение задач.	2	
Тема 2.2. Основные классы функций	Булевы функции. Свойства элементарных булевых функций. Полнота множества булевых функций. Теорема Поста.	2	2
	Практические занятия:		
	Практическая работа № 3. Нахождение полинома Жегалкина. Практическая работа № 4. Определение полноты системы булевых функций.	4	
	Контрольная работа №1. Основы теории множеств. Элементы математической логики.	2	
	Самостоятельная работа №2 Работа с конспектом. Решение задач.	2	
Раздел 2. Основы теории множеств			

Тема 2.1. Основы теории множеств	Содержание учебного материала		2
	Основные понятия теории множеств. Способы задания множеств. Операции над множествами. Диаграммы Эйлера-Венна.	4	
	Практические занятия:		
	Практическая работа № 5. Операции над множествами.	2	
	Самостоятельная работа №3 Работа с конспектом. Решение задач.	2	
Раздел 3. Основы алгебры предикатов			
Тема 3.1. Основные понятия алгебры предикатов	Содержание учебного материала	4	2
	Основы языка и алгебры предикатов. Применение предикатов в алгебре. Булева алгебра предикатов. Кванторы. Формулы логики предикатов.		
	Практические занятия:		
	Практическая работа № 6. Операции над предикатами.	2	
	Самостоятельная работа №4. Работа с конспектом. Решение задач.	2	
Раздел 4. Основы теории графов и теории автоматов			
Тема 4.1. Основы теории графов	Содержание учебного материала		2
	Основные понятия теории графов: Степень вершины. Маршруты, цепи, циклы. Связность графа. Ориентированные графы. Изоморфизм графов. Плоские графы.	6	
	Практические занятия:		
	Практическая работа № 7. Нахождение метрических характеристик графов.	2	
	Самостоятельная работа №5 Работа с конспектом. Решение задач.	2	
Тема 4.2. Основы теории автоматов	Определение конечного автомата. Способы задания конечного автомата. Примеры конечно автомата. Канонические уравнения автоматов.	2	2
	Самостоятельная работа №6	4	
Раздел 5. Элементы комбинаторного анализа			
Тема 5.1. Основы комбинаторики	Содержание учебного материала	2	1
	Основные понятия и формулы комбинаторики.		

	Самостоятельная работа №7 Работа с конспектом. Подготовка сообщений.	2	
Тема 5.2. Принцип математической индукции.	Содержание учебного материала		2
	Принцип математической индукции. Обобщение метода математической индукции.	4	
	Практические занятия:		
	Практическая работа № 8. Решение задач методом математической индукции.	2	
	Контрольная работа №2 Основы теории графов. Принцип математической индукции	2	
	Самостоятельная работа № 8. Работа с конспектом. Решение задач.	2	
Раздел 6. Элементы теории кодирования			
Тема 6.1. Элементы теории кодирования	Содержание учебного материала	4	2
	Основы криптографии и алгебры вычетов.		
	Практические занятия:		
	Практическая работа № 9. Выполнение операций в алгебре вычетов. Практическая работа № 10. Применение простейших криптографических шифров для шифрования текстов.	4	
	Самостоятельная работа №9 Работа с конспектом. Подготовка сообщений, докладов, презентаций по теме.	2	
Всего часов		76	

Содержание практических занятий

Раздел 1 Элементы математической логики

Тема 1.1. Элементы математической логики

Практическая работа № 1. Упрощение формул алгебры высказываний.

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться упрощать формулы алгебры высказываний на основе законов алгебры логики.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Равносильное преобразование формулы - замена формулы другой, ей равносильной.

Упрощение формулы - такое равносильное преобразование, приводящее к формуле, которая не содержит знаков $\rightarrow$ и $\leftrightarrow$, не содержит отрицаний неэлементарных формул (в частности, двойных отрицаний) или содержит в совокупности меньшее число знаков $\wedge$ и $\vee$, чем исходная.

Принцип двойственности.

Две формулы, не содержащие знаков $\rightarrow$ и $\leftrightarrow$, называются **двойственными**, если каждую из них можно получить из другой заменой $\wedge, \vee, \neg, \leftrightarrow$ соответственно на $\vee, \wedge, \neg, \leftrightarrow$.

Принцип двойственности утверждает следующее: если две формулы (не содержащие знаков $\rightarrow$ и $\leftrightarrow$) равносильны, то двойственные им формулы тоже равносильны.

1. $A \wedge (\neg A \vee \neg B)$
2. $\neg(\neg A \vee B) \wedge B$
3. $(A \vee (B \rightarrow C)) \rightarrow A \equiv (A \vee (\neg B) \vee C) \rightarrow A \equiv \neg(A \vee (\neg B) \vee C) \vee A \equiv (\neg A) \wedge B \wedge (\neg C) \vee A \equiv A \vee B \wedge (\neg C)$
4. $(A \vee B) \rightarrow (\neg A \rightarrow C) \equiv \neg(A \vee B) \vee A \vee C \equiv \neg A \wedge \neg B \vee A \vee C \equiv A \vee (\neg B) \vee C$
5. $(\neg A \vee \neg B) \vee \neg((B \wedge \neg C) \vee (\neg B \wedge \neg C)) = \neg A \vee \neg B \vee \neg C$
6. $(B \wedge C) \vee A \vee (A \wedge B) = A \vee B \wedge C$
7. $A \wedge (B \vee \neg B) \vee (\neg A \vee B) = A \vee B$

Равносильности формул логики высказываний часто называют **законами логики**.

- | | |
|--|---|
| 1. $A \equiv A$ - закон тождества | 7. $(A \wedge B) \wedge C \equiv A \wedge (B \wedge C)$ - закон ассоциативности (сочетательности) |
| 2. $A \wedge (\neg A) \equiv \text{Л}$ - закон противоречия | $(A \vee B) \vee C \equiv A \vee (B \vee C)$ |
| 3. $A \vee (\neg A) \equiv \text{И}$ - закон исключенного третьего | 8. $A \wedge (B \vee C) \equiv (A \wedge B) \vee (A \wedge C)$ - закон дистрибутивности |
| 4. $\neg(\neg A) \equiv A$ - закон двойного отрицания | (распределительности) |
| 5. $A \wedge A \equiv A$ - закон идемпотентности | $A \vee (B \wedge C) \equiv (A \vee B) \wedge (A \vee C)$ |
| $A \vee A \equiv A$ | 9. $\neg(A \wedge B) \equiv \neg A \vee (\neg B)$ - закон де Моргана |
| 6. $A \wedge B \equiv B \wedge A$ - закон коммутативности (переместительности) | $\neg(A \vee B) \equiv \neg A \wedge (\neg B)$ |
| $A \vee B \equiv B \vee A$ | 10. $A \wedge \text{И} \equiv A$ |
| | $A \vee \text{Л} \equiv A$ |

11. $A \wedge I \equiv I$
 $A \vee I \equiv I$
12. $A \wedge (A \vee B) \equiv A$ - закон поглощения
 $A \vee (A \wedge B) \equiv A$
13. $(A \vee B) \wedge (\neg A \vee B) \equiv B$ - закон склеивания
 $(A \wedge B) \vee (\neg A \wedge B) \equiv B$
14. $A \rightarrow B \equiv \neg A \vee B$ - выражение импликации
 через дизъюнкцию и отрицание
 $A \rightarrow B \equiv \neg(A \wedge (\neg B))$ - выражение
 импликации через конъюнкцию и
 отрицание
15. $A \leftrightarrow B \equiv ((\neg A) \vee B) \wedge (A \vee (\neg B))$ - выражение
 эквиваленции через конъюнкцию,
 дизъюнкцию и отрицание
 $A \leftrightarrow B \equiv \neg(A \wedge (\neg B)) \wedge ((\neg A) \wedge B)$ - выражение
 эквиваленции через конъюнкцию и
 отрицание
16. $A \rightarrow B \equiv (\neg B) \rightarrow (\neg A)$ - закон
 контрапозиции

4. Содержание заданий

Используя законы алгебры логики, упростить следующие формулы:

Варианты заданий:

1. $A \wedge (\neg A \vee \neg B)$
2. $\neg (\neg A \vee B) \wedge B$
3. $(A \vee (B \rightarrow C)) \rightarrow A$
4. $(A \vee B) \rightarrow (\neg A \rightarrow C)$
5. $A \wedge (B \vee \neg B) \vee (\neg A \vee B)$
6. $(\neg A \vee \neg B) \vee \neg((B \wedge \neg C) \vee (\neg B \wedge \neg C))$
7. $(B \wedge C) \vee A \vee (A \wedge B)$

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Что значит упростить формулу?
- 6.2. Закон распределительный, сочетательный?
- 6.3. Закон де Моргана?
- 6.4. Таблицы истинности основных логических операций.

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Практическая работа №2. Нахождение СКНФ и СДНФ формул алгебры высказываний

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться находить СКНФ и СДНФ формул алгебры высказываний.

2. Перечень необходимых средств обучения (оборудование, материалы):

- технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Нормальная форма логической формулы - это формула, которая не содержит знаков импликации, эквиваленции и отрицания неэлементарных формул.

Существует два вида нормальных форм: конъюнктивная нормальная форма, т. е. конъюнкция нескольких дизъюнкций (КНФ) и дизъюнктивная нормальная форма, т. е. дизъюнкция нескольких конъюнкций (ДНФ).

КНФ: $(X \vee Y)(\neg X \vee Z)(X \vee \neg Y)$

ДНФ: $(\neg X Y) \vee (X Z) \vee (\neg Y \neg Z) \vee (X \neg Z)$

Совершенная конъюнктивная нормальная форма (СКНФ) – такая конъюнкция дизъюнкций, в которой:

- 1) Различны все члены дизъюнкции ("слагаемые");

- 2) Различны все члены каждой конъюнкции ("множители");
 - 3) В каждой конъюнкции нет одновременно переменной и ее отрицания;
 - 4) Каждая конъюнкция содержит все переменные, входящие в данную формулу или их отрицания.
- СКНФ:** $(X \vee Y \vee Z)(\neg X \vee \neg Y \vee Z)(X \vee \neg Y \vee Z)$

Совершенная дизъюнктивная нормальная форма (СДНФ) – такая дизъюнкция конъюнкций, в которой:

- 1) Различны все члены конъюнкции ("множители");
 - 2) Различны все члены каждой дизъюнкции ("слагаемые");
 - 3) В каждой дизъюнкции нет одновременно переменной и ее отрицания;
 - 4) Каждая дизъюнкция содержит все переменные, входящие в данную формулу или их отрицания.
- СДНФ:** $(\neg X \vee Y \vee Z) \vee (X \neg Y \vee Z) \vee (\neg X \vee Y \neg Z) \vee (X \vee Y \neg Z)$

Приведение формулы к СДНФ с помощью равносильных преобразований:

- 1) Привести формулу к нормальному виду (т.е. избавиться от импликации, эквиваленции и отрицания неэлементарных формул).
- 2) Из всех одинаковых членов дизъюнкции ("слагаемых") оставить только один.
- 3) Если в каком-то члене дизъюнкции ("слагаемом") не хватает переменной X_i , то "домножаем" его с на $(X_i \vee \neg X_i)$, т.е. на 1.
- 4) Раскрыть скобки и из всех одинаковых членов дизъюнкции ("слагаемых") оставить только один.

Приведение формулы к СКНФ с помощью равносильных преобразований:

- 1) Привести формулу к нормальному виду (т.е. избавиться от импликации, эквиваленции и отрицания неэлементарных формул).
- 2) Из всех одинаковых членов конъюнкции ("множителей") оставить только один.
- 3) Если в каком-то члене конъюнкции ("множителе") не хватает переменной X_i , то "прибавить" к нему $(X_i \wedge \neg X_i)$, т.е. 0.
- 4) Раскрыть скобки и из всех одинаковых членов конъюнкции ("множителей") оставить только один.

Пример:

$$\begin{aligned}
 &(\neg(XY) \rightarrow \neg X) \wedge \neg((XY \rightarrow (\neg Y))) \equiv (XY \vee (\neg X)) \wedge \neg(\neg X \vee (\neg Y)) \equiv (\neg X \vee Y)XY - \text{нормальная форма} \\
 &(\neg X \vee Y)XY \equiv (\neg X \vee Y)(X \vee Y - Y)(Y \vee X - X) \equiv (\neg X \vee Y)(X \vee Y)(X \vee Y)(\neg X \vee Y) \equiv (\neg X \vee Y)(X \vee Y)(X \vee Y) \\
 &- \text{СКНФ} \\
 &(\neg X \vee Y)XY \equiv XY - \text{СДНФ}
 \end{aligned}$$

Построение СДНФ и СКНФ по таблице истинности:

СДНФ:

- 1) Выбрать из таблицы истинности те строки, в которых значение формулы - "Истина".
- 2) Для каждой выбранной строки составить конъюнкцию переменных или их отрицаний так, чтобы эта конъюнкция была истинной (для этого переменные, которые в соответствующей строке имеют значение "Ложь" нужно взять с отрицанием, а переменные, имеющие значение "Истина" - без отрицания).
- 3) Составить дизъюнкцию полученных конъюнкций.

СКНФ:

- 1) Выбрать из таблицы истинности те строки, в которых значение формулы - "Ложь".
- 2) Для каждой выбранной строки составить дизъюнкцию переменных или их отрицаний так, чтобы эта дизъюнкция была ложной (для этого переменные, которые в соответствующей строке имеют значение "Истина" нужно взять с отрицанием, а переменные, имеющие значение "Ложь" - без отрицания).
- 3) Составить конъюнкцию полученных дизъюнкций.

Пример:

X	Y	Z	F	СДНФ	СКНФ
0	0	0	1	$\neg X \neg Y \neg Z$	
0	0	1	1	$\neg X \neg Y Z$	
0	1	0	0		$X \vee \neg Y \vee Z$
0	1	1	0		$X \vee \neg Y \vee \neg Z$
1	0	0	0		$\neg X \vee Y \vee Z$
1	0	1	1	$X \neg Y Z$	
1	1	0	0		$\neg X \vee \neg Y \vee Z$
1	1	1	0		$\neg X \vee \neg Y \vee \neg Z$

СДНФ: $(\neg X \neg Y \neg Z) \vee (\neg X \neg Y Z) \vee (X \neg Y Z)$

СКНФ: $(X \vee \neg Y \vee Z)(X \vee \neg Y \vee \neg Z)(\neg X \vee Y \vee Z)(\neg X \vee Y \vee \neg Z)(\neg X \vee \neg Y \vee \neg Z)$

Нетрудно заметить, что для того, чтобы построить формулу по таблице истинности достаточно получить СКНФ или СДНФ и затем упростить полученную формулу.

4. Содержание заданий

Следующие формулы представить в СКНФ и СДНФ:

1. $A \& B \rightarrow (A \vee C)$
2. $A \& (B \rightarrow C)$
3. $A \rightarrow B \rightarrow (C \& A)$
4. $A \& B \rightarrow (C \rightarrow B)$
5. $A \rightarrow (C \& B \rightarrow A)$
6. $C \rightarrow A \rightarrow (B \& C)$
7. $(A \& B \& C) \rightarrow C$
8. $(B \& C) \rightarrow (A \rightarrow B)$
9. $A \wedge B \wedge C \rightarrow A$
10. $A \vee B \vee C \rightarrow B$

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Что значит упростить формулу?
- 6.2. Что такое СКНФ, СДНФ?
- 6.3. Способы приведения формул к СКНФ и СДНФ?

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Тема 1.2. Основные классы функций

Практическая работа № 3. Нахождение полинома Жегалкина.

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться строить полином Жегалкина для функций.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Определение. Полиномом Жегалкина (полиномом по модулю 2) от переменных $x_1, \dots, x_n$ называется выражение вида

$$\bigoplus_{\substack{\{i_1, \dots, i_j\} \\ 0 \leq i_1 < \dots < i_j \leq n}} a_{i_1 \dots i_j} x_{i_1} \dots x_{i_j} = a_0 \oplus a_1 x_1 \oplus \dots \oplus a_n x_n \oplus a_{12} x_1 x_2 \oplus \dots \oplus \\ \oplus a_{n-1n} x_{n-1} x_n \oplus \dots \oplus a_{1\dots n} x_1 \dots x_n,$$

где $a_{i_1 \dots i_j} \in \{0, 1\}$.

Наибольший из рангов элементарных конъюнкций входящих в полином, называется **степенью** этого полинома. Степень полинома 0 принимается равной $-\infty$. Число слагаемых в формуле полинома называется **длиной** полинома.

Теорема. Каждая функция представляется в виде полинома Жегалкина и это представление единственно.

Следствие. Из доказанной теоремы вытекает единственность представления булевых функций посредством полинома Жегалкина.

Приведем основные методы построения полиномов Жегалкина от заданной функции.

1. **Метод неопределенных коэффициентов.** Пусть $P(\tilde{x}^n)$ – искомый полином Жегалкина, реализующий заданную функцию $f(\tilde{x}^n)$.

Запишем его в виде

$$P(\tilde{x}^n) = \beta_0 \oplus \beta_1 x_1 \oplus \dots \oplus \beta_n x_n \oplus \dots \oplus \beta_{2^n-1} x_1 \dots x_n.$$

Вектор длины 2^n назовем **вектором коэффициентов полинома** $P(\tilde{x}^n)$. Найдем его компоненты. Для этого заметим, что если переменным $x_1, \dots, x_n$ придать значения $\sigma_1, \dots, \sigma_n$ из i -ой строки таблицы, то значение $P(\tilde{x}^n)$ будет равно сумме β_0 с компонентами вектора $\tilde{\beta}$, соответствующими ненулевым конъюнкциям $\sigma_{i_1} \dots \sigma_{i_j}$ ($1 \leq i_1 < \dots < i_j \leq n$). В итоге получим систему из 2^n уравнений с 2^n неизвестными, имеющую единственное решение. Решив ее, находим коэффициенты полинома $P(\tilde{x}^n)$.

Пример. Построить полином Жегалкина функции $f(x_1, x_2) = x_1 \rightarrow x_2$.

Решение. 1. (метод неопределенных коэффициентов). Запишем искомым полином в виде $P(x_1, x_2) = \beta_0 \oplus \beta_1 x_1 \oplus \beta_2 x_2 \oplus \beta_3 x_1 x_2$.

Табл. 1.11

x_1	x_2	$x_1 \rightarrow x_2$
0	0	1
0	1	1
1	0	0
1	1	1

Тогда

$$f(1, 0) = \beta_0 \oplus \beta_1 \cdot 1 \oplus \beta_2 \cdot 0 \oplus \beta_3 \cdot 0 = 0,$$

$$f(1, 1) = \beta_0 \oplus \beta_1 \cdot 1 \oplus \beta_2 \cdot 1 \oplus \beta_3 \cdot 1 = 1.$$

$$\text{Или } \begin{cases} \beta_0 = 1, \\ \beta_0 \oplus \beta_2 = 1, \\ \beta_0 \oplus \beta_1 = 0, \\ \beta_0 \oplus \beta_1 \oplus \beta_2 \oplus \beta_3 = 1. \end{cases}$$

Из системы уравнений находим $\beta_0 = 1, \beta_1 = 1, \beta_2 = 0, \beta_3 = 1$. Следовательно, $x_1 \rightarrow x_2 = 1 \oplus x_1 \oplus x_1 x_2$.

2. **Метод, основанный на преобразовании формул над множеством связок** $\{\&, \neg\}$. Строят некоторую формулу Φ над множеством связок $\{\&, \neg\}$, реализующую данную функцию $f(\vec{x}^n)$. Затем заменяют всюду подформулы вида $\bar{A}$ на $A \oplus 1$, раскрывают скобки, пользуясь дистрибутивным законом $A \cdot (B \oplus C) = A \cdot B \oplus A \cdot C$, и применяют эквивалентности $A \cdot A = A, A \cdot 1 = A, A \oplus A = 0, A \oplus 0 = A$.

2. (Метод преобразования формул). Имеем

$$x_1 \rightarrow x_2 = \overline{x_1} \vee x_2 = \overline{x_1 \cdot \overline{x_2}} = (x_1 \cdot (x_2 \oplus 1)) \oplus 1 = 1 \oplus x_1 \oplus x_1 x_2.$$

4. Содержание заданий

1. Дана функций:

- $f(x, y, z) = (z \rightarrow y') \cdot (x' + z)$;
- $f(x, y, z) = (x + y) \rightarrow (z' \oplus x')$;
- $f(x, y, z) = (x \cdot y') \rightarrow (y' + z)$;
- $f(x, y, z) = (x + y')' \rightarrow (z \oplus x')$

Требуется:

- а. Вычислить значение функции на наборах (1,0,0) и (0,1,0)
- б. Найти СДНФ, СКНФ с помощью равносильных преобразований.
- с. Представить функцию в виде полинома Жегалкина.

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Определение полинома Жегалкина?
- 6.2. Построение полинома Жегалкина методом неопределенных коэффициентов?
- 6.3. Построение полинома Жегалкина методом преобразования формул?

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Практическая работа № 4. Свойства булевых функций.

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться упрощать булевы функции, применяя законы логики.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Булевыми (переключательными) функциями $f(x_1, x_2, \dots, x_n)$ называют такие функции, у которых все аргументы, как и сами функции, могут принимать лишь два значения. Эти значения, называемые булевыми, представляют двумя системами обозначений: {ложь, истина}, {0, 1}. Последнюю систему удобно использовать при разработке дискретных элементов преобразователей информации с двумя устойчивыми состояниями, например “высокое или низкое напряжение”. Булеву функцию $f(x_1, x_2, \dots, x_n)$ называют **n-местной с областью значений из множества {0, 1}** и со значениями аргументов из этого же множества. Область определения n-местной булевой функции может состоять максимум из 2^n различных наборов значений n ее аргументов (кортежи (последовательности) из 0 и 1).

Алгеброй булевых функций будем называть множество всех конечно-местных булевых функций, рассматриваемое вместе с заданными на нем бинарными операциями конъюнкции ($\bullet$) и дизъюнкции ($+$) и отрицания'. Для всех x, y и z должны выполняться следующие аксиомы:

а) Законы коммутативности

$$x \cdot y = y \cdot x$$

$$x + y = y + x$$

б) Законы ассоциативности

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

$$x + (y + z) = (x + y) + z$$

в) Законы дистрибутивности

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

$$x + (y \cdot z) = (x + y) \cdot (x + z)$$

г) Законы тождества

$$x + 0 = x$$

$$x \cdot 1 = x$$

д) **Законы дополнения**

$$x + x' = 1$$

$$x \cdot x' = 0$$

Элемент 1 называется **единичным** элементом, или единицей, элемент 0 называется **нулевым** элементом, или нулем; а x' называется дополнением x . Знак бинарной операции $\cdot$ часто опускается, и $x \cdot y$ записывается просто как xy .

Используя приведенные выше аксиомы, легко доказать ряд теорем о булевых алгебрах, в частности, справедливы приведенные ниже теоремы.

ДОКАЗАТЕЛЬСТВО. В каждом случае доказано только первое из утверждений теоремы. Доказательство второго утверждения предоставляется читателю.

а) $x + x = (x + x) \cdot 1 =$	свойство констант
$= (x + x) \cdot (x + x') =$	закон дополнения
$= x + (x \cdot x') =$	закон дистрибутивности
$= x + 0 =$	закон дополнения
$= x;$	закон тождества
б) $x + 1 = (x + 1) \cdot 1 =$	закон тождества
$= (x + 1) \cdot (x + x') =$	закон дополнения
$= x + (1 \cdot x') =$	закон дистрибутивности
$= x + (x' \cdot 1) =$	закон коммутативности
$= x + x' =$	закон тождества
$= 1;$	закон дополнения
в) $x + (x \cdot y) = (x \cdot 1) + (x \cdot y) =$	закон тождества
$= x \cdot (1 + y) =$	закон дистрибутивности
$= x \cdot (y + 1) =$	закон коммутативности
$= x \cdot 1 =$	свойство констант
$= x.$	закон тождества

ТЕОРЕМА. Для всех элементов x и y булевой алгебры выполняются такие соотношения:

а) Законы идемпотентности

$$x + x = x;$$

$$x \cdot x = x.$$

б) Свойства констант

$$x + 1 = 1$$

$$x \cdot 0 = 0.$$

ТЕОРЕМА (Закон единственности дополнения) Дополнение произвольного элемента x булевой алгебры единственным образом определяется его свойствами: если $x + x' = 1$, $x \cdot x' = 0$, $x + x'' = 1$, а $x \cdot x'' = 0$, то $x' = x''$.

ТЕОРЕМА Для всех элементов x и y булевой алгебры имеют место такие соотношения:

а) Закон инволюции

$$(x')' = x.$$

б) Дополнение законов тождества

$$0' = 1;$$

$$1' = 0.$$

в) Законы де Моргана

$$(x + y)' = x' \cdot y';$$

$$(x \cdot y)' = x' + y'$$

4. Содержание заданий

1. Докажите:

a. $x \cdot x = x$.

b. $x \cdot 0 = 0$.

c. $x \cdot (x + y) = x$.

2. Упростите выражения:

a. $(x \cdot y + 1) \cdot (0 + x) \cdot z$

b. $x + x \cdot y' + x \cdot z' + y \cdot x'$

c. $(x + y') \cdot (z' + y)'$

d. $(1 + x) \cdot y \cdot z + x \cdot y' \cdot z$

e. $(x \rightarrow y') + (y \oplus z)'$

f. $(x + y + z) \rightarrow ((x + y)(x + z))$

g. $((x \rightarrow y) + ((x \rightarrow z)y))'$

5. Содержание отчёта:

- постановка задачи;

- запись решения в рабочей тетради.

6. Контрольные вопросы

6.1. Булева функция?

6.2. Алгебра булевых функций?

6.3. Аксиомы алгебры булевых функций?

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.

7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.

7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Раздел 2. Основы теории множеств

Тема 2.1. Основы теории множеств

Практическая работа № 5. Операции над множествами

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться определять принадлежность элементов множеству, изображать множества с помощью диаграмм Эйлера-Венна.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

1. Понятие множества

Создателем теории множеств был Георг Кантор. Георг Кантор (Cantor) (1845—1918) — немецкий математик.

Определение (по Кантору) Множество S есть любое собрание определенных и различных между собой объектов нашей интуиции или интеллекта, мыслимое как единое целое. Эти объекты называются элементами множества.

Существенным пунктом канторовского понимания множества является то, что собрание объектов «мыслится как единое целое», т.е. само рассматривается как один предмет.

Под множеством понимается некоторая, вполне определенная совокупность объектов или элементов.

В дальнейшем будем использовать стандартные обозначения числовых множеств:

- ✓ N — множество натуральных чисел;
- ✓ Z — множество целых чисел;
- ✓ Q — множество рациональных чисел;
- ✓ R — множество вещественных чисел;
- ✓ C — множество комплексных чисел.

2. Принадлежность элемента множеству

Если a есть один из объектов множества A , мы говорим, что a есть элемент A , или a принадлежит A . Принадлежность элемента a множеству A записывается как $a \in A$. Если a не является элементом A , это записывается как $a \notin A$.

Об элементах говорят, что они принадлежат множеству, и записывают это так: $x \in A$ (читается: « x принадлежит множеству A »), или « x является элементом множества A »). Допускается запись: $x_1, x_2, \dots, x_n \in A$, если все эти элементы принадлежат множеству A . Запись $x \notin A$ означает, что x не принадлежит множеству A .

Однозначно определенное множество X , элементами которого являются предметы $x_1, x_2, \dots, x_n$, будем обозначать $X = \{x_1, x_2, \dots, x_n\}$.

Если множество X конечное, то количество элементов в множестве обозначается $|X|$.

Например, если $X = \{a, b, c\}$, то $|X| = 3$.

Порядок следования элементов в множестве не имеет значения. Например, $\{a, b, c\}$ и $\{c, a, b\}$ — это одно и то же множество.

Элементы какого-либо множества сами могут быть множествами. Например, множество $A = \{\{1, 3\}, \{2, 4\}, \{5, 6\}\}$ есть множество из трех элементов ($|A| = 3$), а именно: $\{1, 3\}$, $\{2, 4\}$ и $\{5, 6\}$. Множества $B = \{\{1, 2\}, \{2, 3\}\}$ и $C = \{1, 2, 3\}$ — различные множества, так как элементами первого являются $\{1, 2\}$, $\{2, 3\}$, и $|B| = 2$, а элементами второго — $1, 2$ и 3 , $|C| = 3$.

Множества $D = \{\{1, 2\}\}$ и $G = \{1, 2\}$ также различны, так как первое — одноэлементное множество, имеющее единственным своим элементом $\{1, 2\}$, а второе имеет своими элементами 1 и 2 .

3. Свойства множеств.

- а. **Равенство множеств.** Два множества равны тогда и только тогда, когда они состоят из одних и тех же элементов. Равенство множеств обозначается: $A = B$, неравенство — $A \neq B$.

б. Интуитивный принцип абстракции

Под **одноместным предикатом** (формой) от x — $P(x)$ понимается конечная последовательность, состоящую из слов и символа x , такую, что если каждое вхождение x в эту последовательность заменить одним и тем же именем некоторого предмета соответствующего рода, то в результате получится высказывание.

Например, каждое из следующих выражений есть предикат от x :

- ✓ 5 делит x ; $x^2 + x + 1 > 0$;
- ✓ x любит Джона; $x^2 = 2$; $0 < x$.

Теперь можно сформулировать **интуитивный принцип абстракции**. Любой одноместный предикат $P(x)$ определяет некоторое множество A таким образом, что элементами множества A являются те и только те предметы a , для которых $P(a)$ есть истинное высказывание.

Множество, обозначаемое в математике через $\{x \mid P(x)\}$, читается так: «множество всех таких x , что $P(x)$ ». Таким образом, $a \in \{x \mid P(x)\}$ в том и только том случае, если $P(a)$ — истинное высказывание.

с. Отношение включения

Если A и B есть множества, то говорят, что A **включено** в B , если каждый элемент множества A является также элементом множества B (символическая запись: $A \subseteq B$ или $B \supseteq A$). В этом случае говорят также, что множество A есть **подмножество** множества B . Множество A строго включено в B , или B строго включает A , или A есть собственное подмножество B , если $A \subseteq B$ и $A \neq B$ (символически: $A \subset B$). Например, множество четных чисел строго включено в множество Z целых чисел, а множество Q рациональных чисел строго включает Z .

Основные свойства отношения включения:

- ✓ $X \subseteq X$ — рефлексивность
- ✓ $X \subseteq Y$ и $Y \subseteq Z$ влечет $X \subseteq Z$ — транзитивность
- ✓ $X \subseteq Y$ и $Y \subseteq X$ влечет $X = Y$ — антисимметричность

- d. **Пустое множество**, обозначаемое $\emptyset$ или $\{\}$, — это множество, не имеющее элементов. Обозначают его символом $\emptyset$. Пустое множество есть подмножество любого множества.

Каждое множество $A \neq \emptyset$ имеет, по крайней мере, два различных подмножества: само A и $\emptyset$, т.е. $A \subseteq A$ и $\emptyset \subseteq A$.

- e. **Универсальное множество** U есть множество, обладающее таким свойством, что все рассматриваемые множества являются его подмножествами.

Если все рассматриваемые в ходе какого-либо рассуждения множества являются подмножествами некоторого множества U , то это множество U называют **универсальным множеством** (для этого рассуждения). Например, для элементарной арифметики универсальным множеством служит Z , а для аналитической геометрии плоскости — множество всех упорядоченных пар действительных чисел.

- f. Множество всех подмножеств множества A называется **множеством-степенью** множества A и обозначается 2^A . Например, если $A = \{1, 2, 3\}$, то $2^A = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

4. Операции над множествами

- a. **Объединение** множеств A и B (обозначается через $A \cup B$ и читается как «объединение A и B ») есть множество всех предметов, которые являются элементами множества A или B , т.е. $A \cup B = \{x \mid x \in A \text{ или } x \in B\}$. Здесь подразумевается не исключающий смысл слова «или». Таким образом, по определению, $x \in A \cup B$ тогда и только тогда, когда x есть элемент хотя бы одного из множеств A и B . Например: $\{1, 2, 3\} \cup \{1, 3, 4\} = \{1, 2, 3, 4\}$.

- b. **Пересечение** множеств A и B (обозначается через $A \cap B$ и читается как «пересечение A и B ») есть множество всех предметов, которые являются элементами обоих множеств A и B , т.е. $A \cap B = \{x \mid x \in A \text{ и } x \in B\}$. Таким образом, по определению, $x \in A \cap B$ тогда и только тогда, когда x является одновременно элементом множества A и элементом множества B . Например: $\{1, 2, 3\} \cap \{1, 3, 4\} = \{1, 3\}$. Для всякой пары множеств A и B имеют место следующие включения: $A \cap B \subseteq A \subseteq A \cup B$.

Два множества A и B называются **непересекающимися** (или **дизъюнктными**), если $A \cap B = \emptyset$, и пересекающимися, если $A \cap B \neq \emptyset$. Система множеств называется **расчлененной**, если любая пара ее различных элементов является непересекающейся.

Разбиением множества X будем называть такую расчлененную систему U непустых и различных подмножеств множества X , где каждый элемент множества X является в то же время элементом некоторого (следовательно, в точности одного) элемента системы U . Например, $\{\{1, 2\}, \{3\}, \{4, 5\}\}$ есть разбиение множества $\{1, 2, 3, 4, 5\}$.

Абсолютное дополнение множества A (обозначается через A' или $\neg A$) — это множество всех элементов, не являющихся элементами множества A : $\{x \mid x \notin A\}$.

Относительное дополнение множества B до множества A — это множество $A \cap B'$; оно обычно обозначается через $A \setminus B$ (иногда $A - B$), что читается как « A минус B ». Таким образом $A \setminus B = A \cap B'$ есть сокращение для $\{x \in A \mid x \notin B\}$, т.е. это множество тех элементов множества A , которые не являются элементами множества B .

с. Симметрическая разность множеств A и B , обозначаемая через $A \triangle B$ (иногда используются обозначения $A \oplus B$ или $A + B$), определяется следующим образом: $x \in A \triangle B$ тогда и только тогда, когда x принадлежит ровно одному из множеств A и B : $A \triangle B = \{x \mid (x \in A \text{ и } x \notin B) \text{ или } (x \notin A \text{ и } x \in B)\}$. Из определения следует, что $A \triangle B = (A \setminus B) \cup (B \setminus A)$. Нетрудно показать, что эта операция коммутативна: $A \triangle B = B \triangle A$, ассоциативна: $(A \triangle B) \triangle C = A \triangle (B \triangle C)$ и дистрибутивна относительно пересечения: $(A \triangle B) \cap C = (A \cap C) \triangle (B \cap C)$. Кроме того, $A \triangle A =$ и $A \triangle \emptyset = A$.

Диаграммы Венна

Для графической иллюстрации отношений, которые могут иметь место между подмножествами какого-либо универсального множества U , часто используют так называемые диаграммы Венна — по имени английского священника Джона Венна (1834—1923) 1, применявшего их в своих исследованиях по логике. Диаграмма Венна представляет собой схематическое изображение множеств в виде точечных множеств: универсальное множество U изображается множеством точек некоторого прямоугольника, а его подмножество A — в виде круга или какой-нибудь другой простой области внутри этого прямоугольника. Правильнее, однако, было бы назвать их диаграммами Эйлера, поскольку задолго до Венна их употреблял знаменитый швейцарский математик Леонард Эйлер (1707—1783) показаны основные операции над множествами.

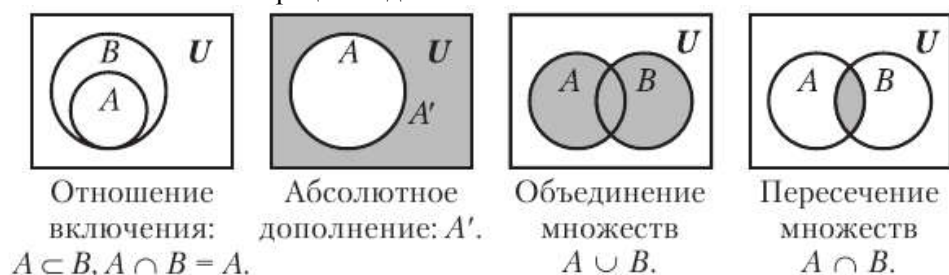


Рис. 1.1. Диаграммы Венна и круги Эйлера.

4. Содержание заданий

1. Пусть $A = \{1, 2, 3, 4, 5, 6, 7\}$, $B = \{4, 5, 6, 7, 8, 9, 10\}$, $C = \{2, 4, 6, 8, 10\}$, а $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Определите следующие множества:

а) $A \cup C$;	б) $A \cap B$;
в) $A \cap (B \cup C)$;	г) $(A \cap B) \cup C$;
д) $(A \cap B)'$;	е) $A' \cap B'$;
ж) $A \triangle B$;	з) $A - B$.
 2. Пусть $A = \{1, 2, 3, 4, 5, 6, 7\}$, $B = \{4, 5, 6, 7, 8, 9, 10\}$, $C = \{2, 4, 6, 8, 10\}$, а $U = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Определите следующие множества:

а) $A - C$;	б) $(A - B) \cup (B - A)$;
в) $A \cap (B \cap C')$;	г) $(A \cup C) - B'$;
д) $(A - \emptyset) \cup (A - A)$;	е) $B \triangle C$;
ж) $C - A$.	
 3. Пусть $A = \{1, 2, 3\}$, а $B = \{a, b\}$. Определите

а) $A \times B$;	б) $B \times B$;	в) $A \times \emptyset$.
-------------------	-------------------	---------------------------
 4. Пусть $A = \{1, 2, 3\}$, а $B = \{a, b\}$. Определите

а) $A \times A$;	б) $B \times A$;	в) $A \triangle B$.
-------------------	-------------------	----------------------
 5. Определите $\mathcal{P}(A)$, если $A = \emptyset$.
 6. Определите $\mathcal{P}(A)$, если $A = \{\emptyset, \{\emptyset\}\}$.
 7. Определите $\mathcal{P}(\mathcal{P}(A))$, если $A = \emptyset$.
 8. Определите, какие из следующих утверждений истинны, а какие ложны:

а) $A \cap \emptyset = A$;	б) $A \triangle A = \emptyset$;
в) если $A \subseteq B$, то $A \cap B = A$;	г) если $A \cap B = A$, то $B \subseteq A$;
д) $A - A = A$;	е) $(A \times B)' = A' \times B'$.
-

Раздел 3. Основы алгебры предикатов

Тема 3.1. Основные понятия алгебры предикатов

Практическая работа № 6. Операции над предикатами

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться определять истинность утверждения с кванторами на основе диаграмм Эйлера-Венна.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Многие утверждения, имеющие форму высказываний, на самом деле таковыми не являются, так как содержат переменные, конкретные значения которых не указаны. Поскольку такое утверждение при одних значениях переменных может быть истинным, а при других — ложным, ему не может быть предписано истинностное значение. Такие утверждения, примерами которых являются:

$$\begin{aligned}P(x) : 3 + x &= 5; \\Q(x, y, z) : x^2 + y^2 &\geq z^2; \\R(x, y) : x^2 + y^2 &\geq 0; \\S(x) : -1 &\leq \sin(x) \leq 1,\end{aligned}$$

называются предикатами. Предикат с одной переменной называется одноместным предикатом. Предикат, имеющий две переменные, называется двуместным предикатом, а предикат, содержащий p переменных, называется p -местным предикатом. Предикат $P\{x\}$ — одноместный, поскольку имеет одну переменную. Предикат $Q(x, y, z)$ является трехместным предикатом. Предикаты становятся высказываниями, когда их переменным присваивается значение.

Например, $P(2) : 3 + 2 = 5$ - является высказыванием, и это высказывание истинно.

$P(7) : 3 + 7 = 5$ тоже является высказыванием, и это высказывание ложно.

Говорят, что набор значений переменных удовлетворяет предикату, если на этом наборе предикат принимает значение "истина", т.е. становится истинным высказыванием.

Некоторые предикаты истинны для каждого возможного набора значений переменных, взятых из данного множества.

Квантор всеобщности

Среди примеров, приведенных выше, $S(x)$ — предикат $-1 < \sin(x) < 1$, где x принадлежит множеству действительных чисел. Тот факт, что для любого значения x $-1 < \sin(x) < 1$, дает основание сказать, что для любого x истинно $S(x)$, что символически изображается как $\forall x S(x)$

или

$$\forall x (-1 < \sin(x) < 1).$$

Символ $\forall x$ называется универсальным квантором, или квантором всеобщности, и читается "для любого x " или "для всех x ". Множество значений, которое может принимать x , называется универсом, или предметной областью. В частности, предметной областью может являться множество действительных чисел, множество целых чисел или другие подобные множества. Вообще говоря, истинность утверждения с квантором всеобщности зависит от предметной области.

Например, высказывание $\forall x (x^2 > 5)$

не истинно, если универсом (предметной областью) является множество целых чисел; однако, оно было бы истинным, если в качестве предметной области взять

множество целых чисел, больших чем 2. Точно так же высказывание $\forall x (x^2 > 0)$ истинно, если предметная область — множество действительных чисел, но ложно, если предметная область содержит комплексное число i , т.к. $i^2 = -1$.

Предикат $\forall x \forall y R(x, y)$ читается как "для каждого x , для каждого y имеет место $R(x, y)$ " или "для каждого x и для каждого y имеет место $R(x, y)$ ". Предикат $\forall x \forall y R(x, y)$ истинный только тогда, когда для любого набора значений x и y из соответствующей предметной области $x^2 + y^2 > 0$ истинно. Если предметной областью для x и для y является множество действительных чисел, то $\forall x \forall y R(x, y)$.

Квантор существования $\exists x P(x)$

Высказывание $\exists x (x^2 = 4)$ истинно, если предметной областью есть множество действительных чисел, т.к. $x^2 = 4$ истинно для $x = 2$. Высказывание $\exists x (x^2 = 5)$ также истинно, если предметной областью есть множество действительных чисел; однако, оно не является истинным, если предметная область есть множество целых чисел, так как не существует целого числа, квадрат которого равен 5.

Поскольку для предиката $Q(x, y, z)$ высказывания $Q(1, 2, 0)$ и $Q(-3, 4, 5)$ истинны, то высказывание $\exists x \exists y \exists z Q(x, y, z)$ истинно.

Чтобы предикат был высказыванием, все его переменные должны иметь конкретные значения или быть связаны соответствующим квантором. Например, $(\exists x)(\forall z)Q(x, y, z)$ не является высказыванием, т.к. переменная y не связана никаким квантором.

Если $D\{x\}$ — предикат, то высказывание $\forall x D(x)$ истинно только тогда, когда высказывание $D(x)$ истинно для любого x . Когда же высказывание $\forall x D(x)$ будет ложным? Отрицание может быть записано как $\neg \forall x D(x)$

Тождества:

$$\neg \forall x (D(x)) = \exists x (\neg D(x))$$

$$\neg \exists x (G(x)) = \forall x (\neg G(x))$$

Для образования отрицания с навешенным квантором всеобщности нужно заменить $\forall x$ на $\exists x$ и взять отрицание предиката, следующего за квантором. А для формирования отрицания предиката с навешенным квантором существования нужно заменить $\exists x$ на $\forall x$ и взять отрицание предиката, следующего за квантором.

Отрицание высказывания, содержащего более одного квантора, осуществляется путем последовательного рассмотрения каждого квантора, начиная с первого.

Например:

$$\begin{aligned} \sim (\forall x)(\forall y) R(x, y) &\equiv \exists x \sim (\forall y) R(x, y) \equiv \\ &\equiv (\exists x)(\exists y) \sim R(x, y). \end{aligned}$$

Аналогично:

$$\begin{aligned} \sim (\exists x)(\forall y)(\exists z) Q(x, y, z) &\equiv (\forall x) \sim (\forall y)(\exists z) Q(x, y, z) \equiv \\ &\equiv (\forall x)(\exists y) \sim (\exists z) Q(x, y, z) \equiv \\ &\equiv (\forall x)(\exists y)(\forall z) \sim Q(x, y, z). \end{aligned}$$

Следовательно, для отрицания высказывания, содержащего кванторы, $\exists$ заменяется на $\forall$ и наоборот, после чего берется отрицание предиката, связанного с этой последовательностью кванторов.

Определения:

- 1) **Универсальная конкретизация** Из истинности $\forall x P(x)$ следует истинность $P(a)$ для произвольного a из универса.
- 2) **Универсальное обобщение** Если произвольное a из универса обеспечивает истинность $P\{a\}$, делаем вывод, что $\forall x (P(x))$ истинно.
- 3) **Экзистенциальная конкретизация** Из истинности $\exists x P(x)$ следует, что существует конкретное b такое, что $P(x)$ истинно.
- 4) **Экзистенциальное обобщение** Из существования конкретного c из универса, для которого $P(c)$ истинно, можно сделать вывод, что $\exists x P(x)$.

ТЕОРЕМА Для произвольных предикатов $P(x)$ и $Q(x)$, имеющих одну предметную область,

- а) $\forall x (P(x) \wedge Q(x)) = \forall x P(x) \wedge \forall x Q(x)$;
- б) $\exists x (P(x) \vee Q(x)) = \exists x P(x) \vee \exists x Q(x)$;
- в) из $\forall x P(x) \vee \forall x Q(x)$ следует, что $\forall x (P(x) \vee Q(x))$
- г) из $\exists x (P(x) \wedge Q(x))$ следует, что $\exists x P(x) \wedge \exists x Q(x)$.

Диаграммы Эйлера

Для неформальной проверки правильности умозаключений, включающих утверждения типа "для всех" и "для некоторого", используются так называемые диаграммы Эйлера, которые состоят из кругов, изображающих множества. Например, утверждению "Все p есть q " соответствует диаграмма, приведенная на рис.1 ниже, где круг, изображающий множество p , содержится в круге, изображающем множество q . Утверждение "Некоторые p есть q " представляется диаграммой на рис. 2, где мы видим, что пересечение кругов, изображающих множества p и q , не пусто. Для проверки умозаключения необходимо попытаться построить диаграмму Эйлера, в которой посылки истинны, а заключение ложно. Если такое построение осуществимо, то умозаключение неправильно, если же нет, то это доказывает правильность нашего умозаключения.

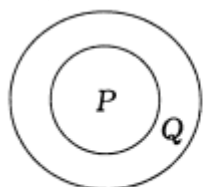


Рис. 1

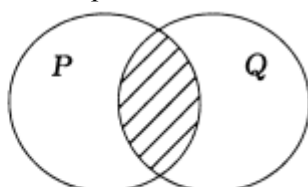


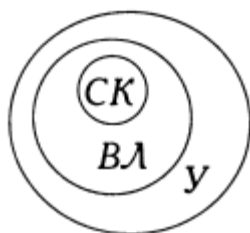
Рис. 2

ПРИМЕР 1. Рассмотрим умозаключение

Все студенты колледжа выдающиеся

Все выдающиеся люди — ученые

Все студенты колледжа — ученые



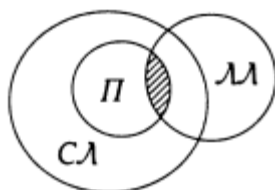
В соответствии с посылками круг, изображающий студентов колледжа (СК), должен быть внутри круга, изображающего выдающихся людей (ВЛ), который, в свою очередь, должен быть внутри круга (У), изображающего ученых. Следовательно, круг студентов колледжа должен находиться внутри круга ученых, и умозаключение является правильным.

ПРИМЕР 2. Рассмотрим умозаключение

Все поэты счастливы

Некоторые поэты ленивы

Некоторые ленивые люди счастливы



В соответствии с посылками круг, изображающий поэтов (П), должен быть внутри круга, изображающего счастливых людей (СЛ), а пересечение поэтов и ленивых людей (ЛЛ) должно быть не пусто. Но это пересечение содержится в круге, изображающем поэтов, так что пересечение ленивых и счастливых людей не пусто. Умозаключение правильно.

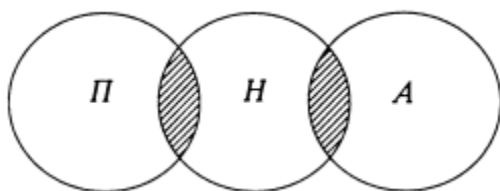
ПРИМЕР 3. Рассмотрим умозаключение

Некоторые поэты неудачники

Некоторые атлеты неудачники

Некоторые поэты являются атлетами

Соответствующая диаграмма Эйлера изображена на рис.



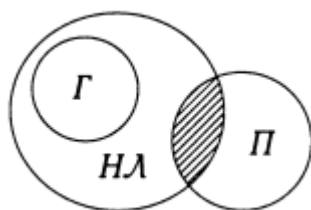
Мы видим, что возможно построить такую диаграмму Эйлера, в которой пересечение кругов поэтов (П) и неудачников (Н) непусто и пересечение кругов атлетов (А) и неудачников непусто, так что посылки истинны, но при этом круги поэтов и атлетов не пересекаются, так что следствие не является верным. Следовательно, умозаключение не является правильным.

ПРИМЕР 4. Рассмотрим умозаключение

Все гении нелогичны

Некоторые политики нелогичны

Некоторые политики гении



На рисунке слева круг для гениев (Г) содержится внутри множества нелогичных людей (НЛ), а пересечение круга политиков (П) и круга нелогичных людей непусто, но круги политиков и гениев не пересекаются. Следовательно, посылки истинны, но заключение ложно. Поэтому умозаключение не является правильным.

4. Содержание заданий

1. Заданы предикаты

$$P(x, y, z) : x^2 + y^2 \geq z^2;$$

$$Q(x, y) : y = (x - 4)/(x + 4);$$

$$R(x, r) : |x - 1| \leq r;$$

$$S(n, y) : y = n!;$$

$$T(a, b, c) : a \text{ нравится } b \text{ больше, чем } c.$$

Запишите следующие высказывания:

а) $P(3, 4, 5);$

б) $Q(8, 2);$

в) $R(3, 7);$

г) $S(4, 24);$

д) $T(\text{Джон}, \text{Сью}, \text{Мэри}).$

2. Заданы предикаты

$$P(x, y, z) : x^2 + y^2 = z^2;$$

$$Q(x, y) : \text{если } y^2 = x^2, \text{ то } x = y;$$

$$R(x) : \lfloor \lfloor x \rfloor \rfloor = \lfloor x \rfloor;$$

$$S(a, b, x) : a \leq x^2 \leq b;$$

$$T(a, b) : a \text{ играет в теннис лучше, чем } b.$$

Запишите следующие высказывания:

а) $P(3, 4, 5);$

б) $Q(-2, 2);$

в) $R(3.1416);$

г) $S(0, 4, -3);$

д) $T(\text{Джон}, \text{Фред}).$

3. Используя P, Q, R, S и T из упражнения 1, запишите высказывания:

- а) $(\exists x)(\exists y)P(x, y, 25)$; б) $(\exists x)Q(x, 7)$;
 в) $(\forall r)(\exists x)R(x, r)$; г) $(\exists n)(\forall y)S(n, y)$;
 д) $(\forall c)T(\text{Джон}, \text{Сью}, c)$.

4. Используя P, Q, R, S и T из упражнения 1, запишите высказывания:

- а) $(\forall x)(\forall y)(\exists z)P(x, y, z)$; б) $(\forall x)(\forall y)Q(x, y)$;
 в) $(\forall x)R(x)$; г) $(\forall x)(\exists a)(\exists b)S(a, b, x)$;
 д) $(\forall a)T(a, \text{Тед})$.

5. Запишите приведенные ниже утверждения в символической форме, введя предикаты. В случае необходимости укажите предметную область.

- а) На каждой улице будет праздник.
 б) Некоторые машины умнее людей.
 в) Любый играет в теннис лучше Фрэда.
 г) Для каждого действия существует равное и противоположно направленное противодействие.
 д) Каждый игрок в гольф, в конце концов, будет обыгран более сильным игроком.

6. Запишите приведенные ниже утверждения в символической форме, введя предикаты. В случае необходимости укажите предметную область.

- а) Некоторые композиторы пишут симфонии лучше, чем другие.
 б) Для каждого n существует три целых числа таких, что n -я степень одного из них равна сумме n -ых степеней двух других.
 в) Существуют лошади, которые могут обогнать некоторых людей.
 г) Он лучший атлет в мире.
 д) Не существует совершенных героев.

7. Ранее было показано, что если $Q(x, y, z) : x^2 + y^2 \geq z^2$, то утверждение

$$\forall x \forall y \forall z Q(x, y, z)$$

ложно. Если универс — множество положительных целых чисел, то что можно сказать об истинности

- а) $\forall x \forall y \exists z Q(x, y, z)$?
 б) $\forall x \exists y \exists z Q(x, y, z)$?
 в) $\exists x \forall y \exists z Q(x, y, z)$?
 г) $\exists x \exists y \exists z Q(x, y, z)$?
 д) $\exists x \exists y \forall z Q(x, y, z)$?

8. Пусть известно, что

$$\forall n (n \text{ нечетно} \rightarrow (\exists k)(n = 2k + 1)).$$

а) Какое из этих утверждений истинно?

$$\begin{aligned} 7 \text{ нечетно} &\rightarrow (\exists k)(7 = 2k + 1), \\ 6 \text{ нечетно} &\rightarrow (\exists k)(6 = 2k + 1). \end{aligned}$$

б) Какое из этих утверждений истинно и почему?

$$\begin{aligned} (\exists k)(7 = 2k + 1), \\ (\exists k)(6 = 2k + 1). \end{aligned}$$

9. Докажите, что из $\forall x P(x) \vee \forall x Q(x)$ следует, что $\forall x (P(x) \vee Q(x))$.

10. Докажите, что из $\exists x (P(x) \wedge Q(x))$ следует, что $\exists x P(x) \wedge \exists x Q(x)$.

11. Проверьте правильность умозаключений при помощи диаграмм Эйлера.
- | | |
|---------------------------------------|---|
| Все адвокаты богаты | Некоторые адвокаты богаты |
| Все богатые едят омаров | Некоторые врачи богаты |
| $\therefore$ Все адвокаты едят омаров | $\therefore$ Некоторые врачи — адвокаты |
12. Проверьте правильность умозаключений при помощи диаграмм Эйлера.
- | | |
|--|---|
| Некоторые марсиане зеленые | Все мужчины любят мясо |
| Все елки зеленые | Некоторые учителя — мужчины |
| $\therefore$ Некоторые марсиане — елки | $\therefore$ Некоторые учителя любят мясо |
13. Проверьте правильность умозаключений при помощи диаграмм Эйлера.
- | | |
|--------------------------------|--------------------------------------|
| Все врачи любят музыку | Некоторые врачи умные |
| Все поэты любят музыку | Все умные люди поэты |
| $\therefore$ Все врачи — поэты | $\therefore$ Некоторые врачи — поэты |
14. Проверьте правильность умозаключений при помощи диаграмм Эйлера.
- | | |
|------------------------------------|--|
| Все машины дорогие | Все мужчины смотрят телевизор |
| Велосипед недорогой | Некоторые слесари — мужчины |
| $\therefore$ Велосипед — не машина | $\therefore$ Некоторые слесари смотрят телевизор |
15. Проверьте правильность умозаключений при помощи диаграмм Эйлера.
- | | |
|------------------------------|--|
| Все люди смертны | Некоторые гуси — мужчины |
| Гуси — не люди | Некоторые мужчины играют в гольф |
| $\therefore$ Гуси бессмертны | $\therefore$ Некоторые гуси играют в гольф |

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Что такое предикат?
- 6.2. Кванторы существования и общности?
- 6.3. Представление кванторов с помощью диаграмм Эйлера-Венна?

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Раздел 4. Основы теории графов и теории автоматов

Тема 4.1. Основы теории графов

Практическая работа № 7. Нахождение метрических характеристик графов.

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться определять элементы графа и орграфа, строить матрицу инцидентности и смежности.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

ОПРЕДЕЛЕНИЕ *Граф* есть конечное множество V , называемое **множеством вершин**, на котором задано симметричное антирефлексивное отношение R и выделено множество E двухэлементных подмножеств V , определяемое как $\{a, b\} \in E$ тогда и только тогда, когда $(a, b) \in R$ и $a \neq b$. Множество E называется **множеством ребер**. Всякий элемент E называется **ребром**. Граф обозначается $G(V, E)$. Говорят, что элементы a и b графа V **соединены** или **связаны** ребром $\{a, b\}$, если $\{a, b\} \in E$.

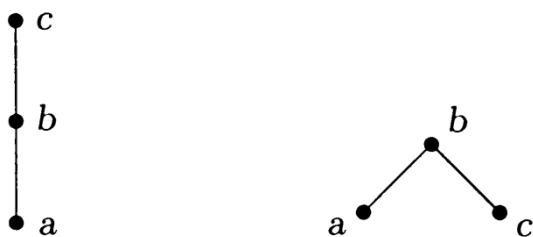
Конечный граф обычно изображается при помощи диаграммы, в которой вершины представлены **точками**, а **ребра**, соединяющие две вершины, — линиями между этими точками.

ОПРЕДЕЛЕНИЕ *Граф* есть конечное множество V , называемое **множеством вершин**, и множество E двухэлементных подмножеств множества V . Множество E называется **множеством ребер**. Элемент множества E называется **ребром**. Граф обозначается $G(V, E)$. Элементы a и b множества V называются **соединенными**, или **связанными** ребром $\{a, b\}$, если $\{a, b\} \in E$.

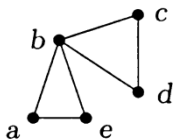
Обычно конечный граф изображают в виде диаграммы, на которой вершины обозначаются точками, а ребра, соединяющие две вершины, — линиями между этими точками.

ОПРЕДЕЛЕНИЕ Если $\{a, b\}$ — ребро, тогда вершины a и b называются **концами** ребра $\{a, b\}$. Ребро $\{a, b\}$ называют также **инцидентным** к вершинам a и b . Обратно, говорят, что вершины a и b инцидентны к ребру $\{a, b\}$. Две вершины называются **смежными**, если они являются концами ребра, или, что то же самое, если они инцидентны к одному ребру. Два ребра называются **смежными**, если они инцидентны к общей вершине.

Пример 1: Граф с множеством вершин $V = \{a, b, c\}$ и множеством ребер $E = \{\{a, b\}, \{b, c\}\}$ может быть изображен, как показано на рис. ниже:



Пример 2. Граф, у которого $V = \{a, b, c, d, e\}$ и $E = \{\{a, b\}, \{a, e\}, \{b, e\}, \{b, c\}, \{b, d\}, \{c, d\}\}$, может быть изображен диаграммой, показанной на рис. ниже



ПРИМЕР 1 Граф, в котором множество вершин $V = \{a, b, c\}$, а $E = \{\{a, b\}, \{b, c\}\}$, может иметь вид, как на рис. 1 или рис. 2



Рис. 1

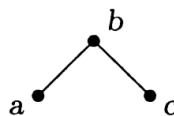


Рис. 2

$$R = \{(a, b), (b, a), (b, c), (c, b)\}.$$

□

Если линии не ориентированы, то их называют **ребрами** (u), а сам граф – **неориентированным** (рис. 1, а), а если линии **ориентированы**, то их называют **дугами** (u), а граф – **ориентированным** (рис. 1, б), или **орграфом**. Если множество вершин и ребер (или дуг) **конечно**, то граф называется **конечным**.

Говорят, что ребро (дуга) и его граничные точки **инцидентны** друг другу, иначе говоря, вершины, **инцидентные** ребру (дуге), являются его концевыми точками. Понятие **инцидентности** ребер (дуг) и их концевых вершин является фундаментальным в теории графов, которая построена с учетом именно этой особенности и не учитывает реальной природы вершин и ребер (дуг).

Степенью вершины $\delta(v)$ называется число концов ребер, **инцидентных** вершине v (т. е. петля учитывается дважды). Для изолированной вершины $\delta(v) = 0$. **Вырожденным** называется граф, у которого все вершины изолированы.

Суграфом графа G называется граф $G' = (V, U')$, где $U' \subset U$, т. е. суграф получается из исходного графа удалением некоторого числа ребер (с сохранением вершин).

Подграфом графа G называется граф $G' = (V', U')$, где $V' \subset V$, $U' = U \cap (V' \times V')$, т. е. подграф получается из исходного графа удалением некоторого числа вершин вместе со всеми ребрами, инцидентными удаленной вершине.

Разновидности графов:

Деревом называется связный граф без циклов. Граф является деревом тогда и только тогда, когда каждая пара различных вершин соединяется одной и только одной цепью.

Лесом из K деревьев называется граф без циклов, состоящий из K компонент.

Обыкновенным называется граф, который не содержит петель и параллельных ребер.

Полным называется граф, в котором любые две различные вершины являются смежными, т. е. соединяются ребром. Полный граф с n вершинами обозначается через K_n .

ПРИМЕР 6.22. На рис. 6.17 показаны, соответственно, графы K_2 , K_3 , K_4 и K_5 .

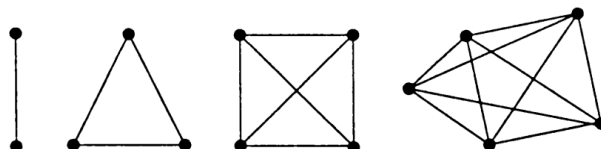


Рис. 6.17

[

4. Содержание заданий

1 Постройте граф для каждого из приведенных ниже отношений на A .

а) $A = \{a, b, c, d, e\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, a), (a, c), (d, e), (e, d)\}$;

б) $A = \{a, b, c, d, e\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (c, a), (a, c)\}$;

в) $A = \{a, b, c, d, e\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d), (b, e), (e, b), (b, d), (d, b)\}$;

г) $A = \{a, b, c, d\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, a), (a, d), (b, d), (d, b), (a, c), (c, a)\}$.

2 Постройте граф для каждого из приведенных ниже отношений на A .

а) $A = \{a, b, c, d, e\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, a), (a, d)\}$;

б) $A = \{a, b, c, d, e, f\}$;

$R = \{(a, b), (b, a), (b, c), (c, b), (c, a), (a, c), (d, e), (e, d)\}$;

в) $A = \{a, b, c, d, e\}$;

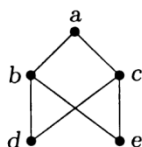
$R = \{(a, b), (b, a), (b, c), (c, b), (c, d), (d, c), (d, e), (e, d), (a, d), (d, a)\}$;

г) $A = \{a, b, c, d, e, f\}$;

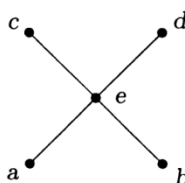
$R = \{(a, b), (b, a), (b, c), (c, b), (c, a), (a, c), (a, e), (e, a), (b, e), (e, b), (b, f), (f, b), (c, d), (d, c), (c, f), (f, c), (d, f), (f, d), (e, f), (f, e)\}$.

3 Найдите множество вершин, ребер и соответствующее симметричное отношение для графов, изображенных на нижеследующих рисунках.

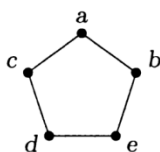
а)



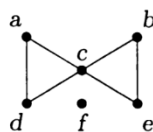
б)



в)

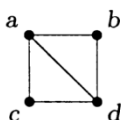


г)

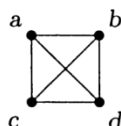


4 Найдите множество вершин, ребер и соответствующее симметричное отношение для графов, изображенных на нижеследующих рисунках.

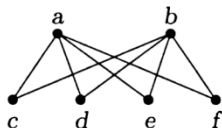
а)



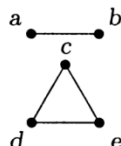
б)



в)



г)



5 Нарисуйте следующие графы:

а) K_6 ;

б) $K_{1,3}$;

в) $K_{1,4}$;

г) K_3 .

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Что такое граф? Какой граф называется ориентированным?
- 6.2. Назовите элементы графа?
- 6.3. Виды графов?

7. Список рекомендуемой литературы:

- 7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
- 7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
- 7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Раздел 5. Элементы комбинаторного анализа

Тема 5.1. Основы комбинаторики

Практическая работа № 8 Основные комбинаторные принципы

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться применять основные принципы комбинаторики при решении задач.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

ТЕОРЕМА 8.1. (Комбинаторный принцип умножения) Пусть задана последовательность событий

$$E_1, E_2, E_3, \dots, E_m$$

таких, что событие E_1 осуществляется n_1 способами, и если события $E_1, E_2, E_3, \dots, E_{k-1}$ осуществились, то событие E_k может осуществиться n_k способами. Тогда существует $n_1 \times n_2 \times n_3 \times \dots \times n_m$ способов осуществления всей последовательности событий.

ПРИМЕР 8.4. Битовая строка — это строка, состоящая из элементов, каждый из которых имеет значение 1 или 0. Сколько существует битовых строк, имеющих длину 5? Сколько существует битовых строк длины k ? Поскольку каждый символ строки может иметь значение 1 или 0, то существует два варианта выбора для каждой позиции. Следовательно, существует $2 \times 2 \times 2 \times 2 \times 2 = 2^5$ битовых строк длины 5. По аналогичным соображениям, имеется 2^k битовых строк длины k . $\square$

Предположим, что на собрании присутствуют 10 мужчин и 15 женщин, и кого-то одного нужно выбрать председателем. Существует $10 + 15 = 25$ способов выбора председателя. Предположим, что человек направляется в ресторан, в котором предлагаются 15 блюд из говядины, 8 блюд из свинины и 12 блюд из морских продуктов. Посетителю ресторана предложен выбор из $15 + 8 + 12 = 35$ различных блюд. Предположим теперь, что студент выбирает книгу на полке, где находятся 25 различных учебников по математике, 30 учебников по информатике и 15 — по химии. Существует $25 + 30 + 15 = 70$ различных вариантов выбора книги студентом. Заметим, что в каждом случае множества, из элементов которых делается выбор, не пересекаются. Эти примеры приводят к следующей теореме, которая формулируется без доказательства.

ТЕОРЕМА 8.6. (Комбинаторный принцип сложения) Пусть $S_1, S_2, S_3, \dots, S_m$ — попарно непересекающиеся множества (т.е. $S_i \cap S_j = \emptyset$ для всех $i \neq j$), и пусть для каждого i , множество S_i содержит n_i элементов. Количество вариантов выбора из S_1 или S_2 или S_3 или $\dots$ или S_m равно $n_1 + n_2 + n_3 + \dots + n_m$. На языке теории множеств утверждение теоремы имеет вид

$$|S_1 \cup S_2 \cup S_3 \cup \dots \cup S_m| = |S_1| + |S_2| + |S_3| + \dots + |S_m|,$$

где $|S|$ обозначает количество элементов множества S .

ПРИМЕР 8.7. Сколько существует целых чисел между 0 и 1000, содержащих ровно одну цифру 6? Пусть S будет множеством целых чисел между 0 и 1000, содержащих ровно одну цифру 6. Пусть S_1 — подмножество множества S , которое содержит число, состоящее из одной цифры, и эта цифра равна 6. Пусть S_2 — подмножество множества S , содержащее двузначные числа ровно с одной цифрой, равной 6. Пусть S_3 — подмножество множества S , содержащее трехзначные числа ровно с одной цифрой, равной 6. Множество S_1 содержит только один элемент — число 6. В S_2 каждый элемент, содержащий 6, имеет ее либо первой, либо второй цифрой. Если 6 — вторая цифра, то существуют 8 различных чисел, поскольку первое число не может быть 0 или 6. Если 6 — первая цифра, то таких чисел 9, поскольку вторая цифра не может быть 6. Таким образом, S_2 содержит $8 + 9 = 17$ элементов. Элемент из S_3 содержит 6 как первую, вторую или третью цифру. Если 6 — первая цифра, то существуют 9 вариантов выбора второй цифры и 9 вариантов выбора третьей цифры. Согласно комбинаторному принципу умножения, S_3 содержит $9 \times 9 = 81$ чисел с 6 как первой цифрой. Если 6 — вторая цифра, то имеются 9 вариантов выбора третьей цифры и 8 вариантов выбора первой цифры, поскольку первая цифра не может быть нулем. Следовательно, S_3 содержит $9 \times 8 = 72$ чисел, у которых 6 — вторая цифра. Аналогично, S_3 содержит 72 числа, у которых 6 — третья цифра. Следовательно, всего S_3 содержит $81 + 72 + 72 = 225$ элементов. Поскольку $S = S_1 \cup S_2 \cup S_3$, то S содержит $1 + 17 + 225 = 243$ элементов. $\square$

ПРИМЕР 8.8. Сколько существует целых чисел между 0 и 1000, содержащих хотя бы одну цифру 6? Для решения этой задачи положим S множеством целых чисел от 0 до 1000, **не** содержащих цифру 6 ни в одном из разрядов. Пусть S_1 — подмножество множества S , содержащее однозначные числа; S_2 — подмножество множества S , содержащее двузначные числа; S_3 — подмножество множества S , содержащее трехзначные числа; и S_4 — подмножество множества S , содержащее четырехзначные числа. Множество S_1 содержит девять чисел без цифры 6, поскольку только число 6 исключено. Множество S_2 содержит числа, имеющие 8 вариантов выбора первой цифры и 9 вариантов выбора второй цифры, поскольку первая цифра не может быть ни 6, ни 0, а вторая цифра не может быть 6. Поэтому S_2 содержит $8 \times 9 = 72$ элементов без цифры 6. Множество S_3 содержит числа, имеющие 8 вариантов выбора первой цифры, 9 вариантов выбора второй цифры и 9 вариантов выбора третьей цифры. Поэтому множество S_3 содержит $8 \times 9 \times 9 = 648$ элементов без цифры 6. Множество S_4 содержит только число 1000. Следовательно, S содержит $9 + 72 + 648 + 1 = 730$ элементов. Пусть T — множество всех чисел между 0 и 1000. Тогда $T - S$ — множество всех целых чисел между 0 и 1000, содержащих хотя бы одну цифру 6. Более того, S и $T - S$ — непересекающиеся множества. Следовательно, $|S| + |T - S| = |T|$, так что $730 + |T - S| = 1001$. Значит, $|T - S| = 271$, поэтому между 1 и 1000 существует 271 целое число, содержащее хотя бы одну цифру 6. □

4. Содержание заданий

УПРАЖНЕНИЯ

1. Сколько положительных целых чисел, меньших 700, делятся на 5? Сколько таких чисел делятся на 3? А сколько таких чисел делятся и на 5, и на 3?
2. Если авиакомпания осуществляет 15 рейсов из Сан-Франциско в Чикаго и 20 рейсов из Чикаго в Нью-Йорк, то сколько всего рейсов из Сан-Франциско в Нью-Йорк проходит транзитом через Чикаго?
3. Сколько существует способов избрания президента, вице-президента, секретаря и казначея среди членов клуба, включающего 8 студентов последнего курса, 10 студентов предпоследнего курса, 15 второкурсников и 20 первокурсников, если
 - а) отсутствуют какие-либо ограничения?
 - б) президентом должен быть студент последнего курса?
 - в) студент последнего курса не может быть вице-президентом?
 - г) первокурсники могут быть избраны только на должность секретаря?
4. В ресторане из напитков предлагают кофе, чай, молоко или колу. Предлагают на выбор суп или салат. Имеются 10 различных бифштексов и 5 разнообразных куриных блюд. На гарнир можно выбрать картофель фри, печеный картофель, макароны с сыром или рис. На десерт подают сладкий пирог, мороженое или то и другое вместе.
 - а) Сколько можно составить различных меню?
 - б) Сколько можно составить различных меню, включающих бифштекс?
 - в) Сколько можно составить различных меню, если клиент выбирает бифштекс и картофель или не выбирает ни то, ни другое?

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Комбинаторный принцип сложения?
- 6.2. Комбинаторный принцип умножения?
- 6.3. Что такое сочетание, распределение?

7. Список рекомендуемой литературы:

7. 1 Игошин В.И. Задачи и упражнения по математической логике и теории алгоритмов. М.: АCADEMA, 2009.
7. 2 Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.

Тема 5.2. Принцип математической индукции

Практическая работа № 9 Решение задач методом математической индукции

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться применять метод математической индукции при доказательстве утверждений.

2. Перечень необходимых средств обучения (оборудование, материалы):

– технические средства обучения: проектор, учебная доска.

3. Основные теоретические положения

Принцип математической индукции Пусть $P(n)$ есть такое утверждение, что

а) $P(1)$ истинно, и

б) для каждого k , если $P(k)$ истинно, то $P(k + 1)$ истинно.

Тогда $P(n)$ истинно для любого целого положительного числа n .

В символической записи принцип математической индукции имеет вид

$(P(1) \wedge ((\forall k) P(k) \rightarrow P(k + 1))) - (\forall n) P(n)$.

Математическую индукцию можно сравнить с бесконечным рядом костяшек домино. Свойство выстроенных в ряд домино состоит в том, что если опрокинуть одну костяшку, падает следующая. Пусть утверждение $P(n)$ состоит в том, что падает n -я костяшка. Опрокидывание первой костяшки домино обозначим PA), т.е. истинность PA) состоит в том, что первая костяшка падает. Поскольку каждая костяшка опрокидывает следующую, то из истинности $P(k)$ следует истинность $P(k + 1)$. Поскольку падают все костяшки, $P(n)$ истинно для каждого положительного целого числа n . В дальнейшем, проводя доказательство при помощи описанного выше принципа математической индукции, мы будем просто говорить, что доказываем утверждение по индукции.

ПРИМЕР 1 Допустим, необходимо найти формулу для вычисления суммы первых n положительных целых чисел, $1 + 2 + 3 + \dots + n$. Такая формула была бы полезна, если надо было бы, например, найти сумму первых 100000 положительных целых чисел, не выполняя для этого 99 999 операций сложения. Предположим, у нас имеются основания полагать, что сумма первых n положительных чисел равна $\frac{n(n+1)}{2}$. Докажем это утверждение по индукции.

Пусть S_n есть утверждение

$$1 + 2 + 3 + \dots + n = \frac{n(n+1)}{2}. \quad (1)$$

Сначала покажем, что S_1 истинно. При $n = 1$ левая часть равенства $1+2+3+\dots+n$ равна 1. Справа получаем

$$\frac{n(n+1)}{2} = \frac{1(1+1)}{2} = 1,$$

так что S_1 истинно. Затем предполагаем, что для любого положительного числа k S_k истинно, т.е. равенство (1) истинно для $n = k$. Это означает, что

$$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2}.$$

Теперь необходимо доказать, что S_{k+1} истинно, т.е. равенство S_n истинно для $n = k + 1$. Другими словами, требуется доказать, что

$$1 + 2 + 3 + \dots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2}.$$

Используя предположение

$$1 + 2 + 3 + \dots + k = \frac{k(k+1)}{2}$$

и сравнивая это равенство с предыдущим, мы замечаем, что, добавив $k + 1$ к обеим частям последнего равенства, получим левую часть искомого равенства:

$$\begin{aligned} 1 + 2 + 3 + \dots + k &= \frac{k(k+1)}{2}; \\ 1 + 2 + 3 + \dots + k + (k+1) &= \frac{k(k+1)}{2} + (k+1) = \\ &= (k+1)\left(\frac{k}{2} + 1\right) = \\ &= \frac{(k+1)((k+1)+1)}{2}. \end{aligned}$$

Итак, доказано равенство

$$1 + 2 + 3 + \dots + k + (k+1) = \frac{(k+1)((k+1)+1)}{2},$$

которое означает, что соотношение (1) справедливо для $n = k + 1$. Этот результат обеспечивает истинность S_{k+1} . Следовательно, в силу аксиомы N4, S_n истинно для любого положительного целого числа n . $\square$

Пример 2. Требуется доказать, что $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Пусть S_n обозначает утверждение, что равенство в уравнении (2) выполняется. Сначала покажем, что утверждение S_n истинно для $n = 1$. Подставляя 1 в обе части равенства, получаем

$$1^2 = \frac{1(1+1)(2 \cdot 1 + 1)}{6},$$

что дает нам $1 = 1$ и обеспечивает истинность утверждения S_n при $n = 1$.

Затем мы предполагаем, что равенство S_n истинно для $n = k$. То есть,

$$1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

Теперь требуется доказать, что равенство S_n истинно для $n = k+1$. Иначе говоря, требуется доказать, что

$$\begin{aligned} 1 + 2 + 3 + \dots + k^2 + (k+1)^2 &= \frac{(k+1)((k+1)+1)(2(k+1)+1)}{6} = \\ &= \frac{(k+1)(k+2)(2k+3)}{6}. \end{aligned}$$

Используя предположение

$$1 + 2 + 3 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6},$$

замечаем, что, прибавив к обеим частям последнего равенства $(k+1)^2$, мы получим левую часть искомого равенства. Таким образом,

$$\begin{aligned} 1 + 2 + 3 + \dots + k^2 &= \frac{k(k+1)(2k+1)}{6}; \\ 1 + 2 + 3 + \dots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \\ &= \frac{k(k+1)(2k+1)}{6} + \frac{6(k+1)^2}{6} = \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \\ &= \frac{(k+1)[k(2k+1) + 6(k+1)]}{6} = \\ &= \frac{(k+1)(2k^2 + 7k + 6)}{6} = \\ &= \frac{(k+1)(2k+3)(k+2)}{6}. \end{aligned}$$

4. Содержание заданий

УПРАЖНЕНИЯ

1. Докажите, что $1 + 4 + 7 + 10 + \dots + (3n - 2) = \frac{n(3n - 1)}{2}$.
 2. Докажите, что $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \frac{1}{7 \cdot 9} + \dots + \frac{1}{(2n - 1)(2n + 1)} = \frac{n}{2n + 1}$.
 3. Докажите, что $1 + 2 + 2^2 + 2^3 + \dots + 2^{n-1} = 2^n - 1$.
 4. Докажите, что $1 + r + r^2 + r^3 + \dots + r^{n-1} = \frac{1 - r^n}{1 - r}$.
 5. Докажите, что $1 + 3 + 5 + 7 + \dots + (2n - 1) = n^2$.
 6. Докажите, что $\sum_{i=1}^n i^3 = \frac{n^2(n + 1)^2}{4}$.
 7. Докажите, что $\sum_{i=1}^n i(i + 1) = \frac{n(n + 1)(n + 2)}{3}$.
 8. Для положительного целого числа n определим a^n как $a^1 = a$ и $a^{k+1} = a^k \cdot a$.
Докажите, что $a^{m+n} = a^m a^n$.
 9. Используя математическую индукцию, докажите, что $(ab)^k = a^k b^k$.
-

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Идея принципа математической индукции?
- 6.2. Пример доказательства с помощью ПМИ?

7. Список рекомендуемой литературы:

7. 1Новиков Ф.А., Дискретная математика, ЗАО издательский дом «Питер», 2009.
7. 2Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3Просветов Г.И., Дискретная математика. Задачи и решения. БИНОМ, Лаборатория знаний, 2008.
7. 4 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.
7. 5Яблонский С.В., Введение в дискретную математику, М.: Высшая школа, 2008

Раздел 6. Элементы теории кодирования

Тема 6.1.Элементы теории кодирования

Практическая работа № 10. Применение простейших криптографических шифров для шифрования текстов

Время, отводимое на выполнение практической работы - 2 часа.

1. Цель занятия:

- научиться выполнять шифрование и дешифрование сообщений с помощью простых криптографических шифров.

2. Перечень необходимых средств обучения (оборудование, материалы):

- технические средства обучения: проектор, учебная доска.

3.Основные теоретические положения

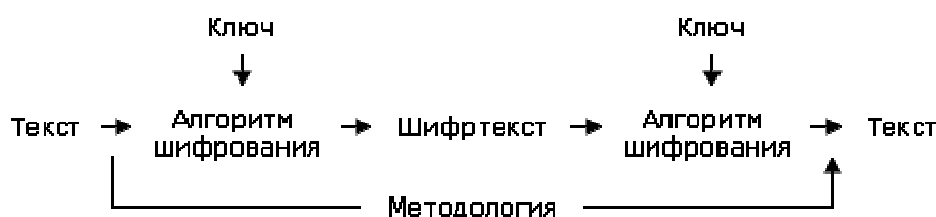
Криптография – это наука об обеспечении безопасности данных, обеспечивающая решение четырех важных проблем безопасности: конфиденциальности, аутентификации, целостности и контроля участников взаимодействия.

Шифрование – это преобразование данных в нечитаемую форму, используя ключи шифрования-расшифровки. Шифрование позволяет обеспечить конфиденциальность, сохраняя информацию в тайне от того, кому она не предназначена.

Самый надежный технический метод защиты информации основан на использовании криптосистем. Криптосистема включает:

- алгоритм шифрования;
- набор ключей (последовательность двоичных чисел), используемых для шифрования;
- систему управления ключами

Общая схема работы криптосистемы



Криптосистемы решают такие проблемы информационной безопасности как обеспечение **конфиденциальности, целостности данных**, а также **аутентификацию данных и их источников**.

Рассмотрим основные понятия методологии криптографии.

Алфавит — конечное множество используемых для кодирования информации знаков.

В качестве примеров алфавитов, используемых в современных НС, можно привести следующие:

алфавит Z_{33} — 32 буквы русского алфавита и пробел;

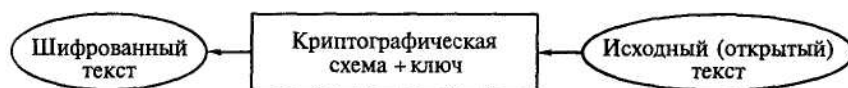
алфавит Z_{256} — символы, входящие в стандартные коды ASCII и КОИ-8;

бинарный алфавит — $Z_2 = \{0,1\}$;

восьмеричный или шестнадцатеричный алфавит.

Текст — упорядоченный набор из элементов алфавита.

Шифрование — преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом



Дешифрование — процесс, обратный шифрованию. На основе ключа шифрованный текст преобразуется в исходный.

Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

Под шифрованием {дешифрованием} понимается такой вид криптографического закрытия (раскрытия), при котором преобразованию подвергается каждый символ защищаемого сообщения. Методы шифрования и дешифрования подразделяют на два класса: с симметричным ключом и системы с открытыми ключами. Все известные способы шифрования с симметричными ключами можно разбить на пять групп: подстановка (замена), перестановка, аналитическое преобразование, гаммирование и комбинированное шифрование (дешифрование).

Шифры перестановки

Являются самыми простыми и самыми древними.

1. шифрующие таблицы

С начала эпохи возрождения начала возрождаться криптография. В разработках шифров перестановки того времени применяются шифрующие таблицы. В качестве ключа используют:

- 1) размер таблицы
- 2) слово или фразу задающие перестановку
- 3) особенности структуры таблицы

Одним из самых примитивных табличных шифров является простая перестановка, для которой ключом служит размер таблицы.

Пример:

Сообщение *ТЕРМИНАТОР ПРИБЫВАЕТ СЕДЬМОГО В ПОЛНОЧЬ*

Записывается в таблицу поочередно по столбцам:

<i>Т</i>	<i>Н</i>	<i>П</i>	<i>В</i>	<i>Е</i>	<i>Г</i>	<i>Л</i>
<i>Е</i>	<i>А</i>	<i>Р</i>	<i>А</i>	<i>Д</i>	<i>О</i>	<i>Н</i>
<i>Р</i>	<i>Т</i>	<i>И</i>	<i>Е</i>	<i>Ь</i>	<i>В</i>	<i>О</i>
<i>М</i>	<i>О</i>	<i>Б</i>	<i>Т</i>	<i>М</i>	<i>П</i>	<i>Ч</i>
<i>И</i>	<i>Р</i>	<i>Ы</i>	<i>С</i>	<i>О</i>	<i>О</i>	<i>Ь</i>

После заполнения таблицы текстом сообщения по столбцам для формирования шифротекста считывают содержимое таблицы по строкам. Если шифротекст записывать группами по пять букв, получается: *ТНПВЕ ГЛЕАР АДОНР ТИЕЬВ ОМОБТ МПЧИР ЫСООЬ*

Отправитель и получатель должны условиться об общем ключе в виде размера таблицы.

Несколько большей стойкостью к раскрытию обладает метод шифрования, называемый одиночной перестановкой по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или наборе чисел длиной в строку таблицы. Применим в качестве ключа слово *ПЕЛИКАН*, текст сообщения возьмем из предыдущего примера (заранее была произведена нумерация букв ключевого слова по возрастанию, если бы в ключе встретились две одинаковые буквы, они были бы пронумерованы слева направо):

<i>П</i>	<i>Е</i>	<i>Л</i>	<i>И</i>	<i>К</i>	<i>А</i>	<i>Н</i>
<i>7</i>	<i>2</i>	<i>5</i>	<i>3</i>	<i>4</i>	<i>1</i>	<i>6</i>
<i>Т</i>	<i>Н</i>	<i>П</i>	<i>В</i>	<i>Е</i>	<i>Г</i>	<i>Л</i>
<i>Е</i>	<i>А</i>	<i>Р</i>	<i>А</i>	<i>Д</i>	<i>О</i>	<i>Н</i>
<i>Р</i>	<i>Т</i>	<i>И</i>	<i>Е</i>	<i>Ь</i>	<i>В</i>	<i>О</i>
<i>М</i>	<i>О</i>	<i>Б</i>	<i>Т</i>	<i>М</i>	<i>П</i>	<i>Ч</i>
<i>И</i>	<i>Р</i>	<i>Ы</i>	<i>С</i>	<i>О</i>	<i>О</i>	<i>Ь</i>

<i>А</i>	<i>Е</i>	<i>И</i>	<i>К</i>	<i>Л</i>	<i>Н</i>	<i>П</i>
<i>1</i>	<i>2</i>	<i>3</i>	<i>4</i>	<i>5</i>	<i>6</i>	<i>7</i>
<i>Г</i>	<i>Н</i>	<i>В</i>	<i>Е</i>	<i>П</i>	<i>Л</i>	<i>Т</i>
<i>О</i>	<i>А</i>	<i>А</i>	<i>Д</i>	<i>Р</i>	<i>Н</i>	<i>Е</i>
<i>В</i>	<i>Т</i>	<i>Е</i>	<i>Ь</i>	<i>И</i>	<i>О</i>	<i>Р</i>
<i>П</i>	<i>О</i>	<i>Т</i>	<i>М</i>	<i>Б</i>	<i>Ч</i>	<i>М</i>
<i>О</i>	<i>Р</i>	<i>С</i>	<i>О</i>	<i>Ы</i>	<i>Ь</i>	<i>И</i>

При считывании содержимого правой таблицы по строкам и записи группами по пять букв получается: *ГНВЕП ЛТООА ДРНЕВ ТЕЬИО РПОТМ БЧМОР СОЬЫИ*

Для обеспечения дополнительной скрытности можно повторно зашифровать сообщение, которое уже прошло шифрование. Такой метод шифрования называется

двойной перестановкой. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк.

Шифры простой замены

При шифровании заменой (подстановкой) символы шифруемого текста заменяются символами того же или другого алфавита с заранее установленным правилом замены. В шифре простой замены каждый символ исходного текста заменяется символом того же алфавита одинаково на всём протяжении текста.

Шифр Цезаря

Является частным случаем шифра простой замены. Своё название получил от имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50г. до н.э.). При шифровании заменяющая буква определяется путём смещения от алфавита исходной буквы на k букв.

Аффинная система подстановок Цезаря

Данное преобразование определяется формулой $= at + b \pmod{m}$, где a и b – целые числа, $0 < a, b < m$, $\text{НОД}(a, m) = 1$, m – число букв в алфавите.

Например, $m=32, a=3, b=5 \Rightarrow \text{НОД}(3, 32)=1 \Rightarrow$

t	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
3t+5	5	8	11	14	17	20	23	26	29	0	3	6	9	12	15	18	21	24	27	30	1	4	7	10	13	16	19	22	25	28	31	2

Зашифруйте сообщение Пришёл увидел победил

Шифр Цезаря с ключевым словом

Является одноалфавитной системой подстановки. Особенностью этой системы являются использование ключевого слова для смещения и изменения порядка символов в алфавите подстановки.

Выберем некоторое число от 0 до 32 и слово или фразу. Желательно, чтобы буквы были различны. Пусть выбрано слово ДИПЛОМАТ и число = 5. Ключевое слово записывается под буквами алфавита, начиная с буквы, числовой код которой совпадает с выбранным числом. Оставшиеся буквы алфавита подстановки записываются после ключевого слова в алфавитном порядке.

4. Содержание заданий

Каждая буква имеет соответствующий код

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	К	Н	О	П
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32

Задание 1. Зашифруйте текст по заданию преподавателя шифром Цезаря

Задание 2. Расшифруйте текст, зашифрованный шифром Цезаря по вариантам:

№	Сдвиг	Шифрованный текст
1	3	тстуюжцрявфхуинскг
2	4	хцфйотлдчксйутйц
3	5	телкршйупфкчбиуруйтао
4	6	рщтцюржтулчщцжууфгшф
5	7	пшмтпфзтънхсцхлтпцсп
6	8	щуыярущцщцццкджхиаыфрэчшрунънд
7	9	сльощняофёъяояльомныйчдвоыьмчфчу
8	10	шьёкошьётмсшлэоеякчжпыщпъхш

Задание 3. Зашифруйте текст по заданию преподавателя методом Аффинная система

Задание 4. Расшифруйте текст, зашифрованный методом Аффинная система по предложенным вариантам:

№	Сдвиг	Шифрованный текст
---	-------	-------------------

п/п	a	b	
1	3	9	цуццътврэжъящшзуюй
2	3	8	ыюшчжтэибъпчхтчю
3	5	7	изеаюжынцтабуцннюныоф
4	5	6	шевеюшжвзяыацжззмчам
5	6	5	хлгзхуезчйщбящэзхяхх
6	7	4	ысьеьсжыиыжсжтицядмйшьчнфьсззвви
7	7	3	ысъжуяэжрзьбжсъжшягебатжбишерей
8	9	2	адтвжаыдкфбалнжхявчюпыйптеа

5. Содержание отчёта:

- постановка задачи;
- запись решения в рабочей тетради.

6. Контрольные вопросы

- 6.1. Что такое криптография, шифрование?
- 6.2. Криптосистема – это...?
- 6.3. Вопросы, которые решает криптосистема?
- 6.4. Примеры шифров перестановки, замены?

7. Список рекомендуемой литературы:

7. 1Новиков Ф.А., Дискретная математика, ЗАО издательский дом «Питер», 2009.
7. 2Никольская И.Л., Математическая логика, М.: АCADEMA, 2009.
7. 3Просветов Г.И., Дискретная математика. Задачи и решения. БИНОМ, Лаборатория знаний, 2008.
7. 4 Спирина М.С. Дискретная математика. М.: Издательский центр «Академия», 2015. – 368с.
7. 5Яблонский С.В., Введение в дискретную математику, М.: Высшая школа, 2008

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изме- нения	Обозначение документа	Номер листа				Всего листов в документе	Подпись ответственного за внесение изменения	Дата внесения изменения	Дата введения изменения
		измененного	замененного	нового	изъятого				