

**МИНОБРНАУКИ РОССИИ**  
**Ярославский государственный университет им. П.Г. Демидова**

Кафедра алгебры и математической логики

УТВЕРЖДАЮ

Декан математического факультета



Нестеров П.Н.

21 мая 2024 г.

**Рабочая программа дисциплины**

**Быстрые алгоритмы**

Направление подготовки (специальности)  
02.03.01 Математика и компьютерные науки

Направленность (профиль)  
«Программирование, алгоритмы и анализ данных»

Форма обучения очная

Программа рассмотрена  
на заседании кафедры  
от 12 апреля 2024 г., протокол № 8

Программа одобрена НМК  
математического факультета  
протокол № 9 от 3 мая 2024 г.

## 1. Цели освоения дисциплины

Целями освоения дисциплины "Быстрые алгоритмы" являются:

- овладение быстрыми алгоритмами цифровой обработки сигналов и математическим аппаратом, лежащим в основе разработки таких алгоритмов,
- формирование практических навыков оценки сложности алгоритмов.

## 2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к части образовательной программы, формируемой участниками образовательных отношений, и является элективной дисциплиной. Для ее успешного изучения необходимы знания и умения и навыки, приобретенные в ходе освоения таких базовых курсов, как «Алгебра» и «Теория чисел».

В основе быстрых алгоритмов лежит специальная организация массивов данных в виде конечных алгебраических структур (групп, колец, полей), что позволяет применять структурные теоремы алгебры и теории чисел. Использование алгебраических структур позволяет строить алгоритмы, обеспечивающие работу цифровых процессоров в реальном масштабе времени для решения задач, возникающих в таких приложениях, как все виды связи, радиолокация, радиоастрономия, цифровая голография, медицинская электроника и т.д.

## 3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Процесс изучения дисциплины направлен на формирование следующих элементов компетенций в соответствии с ФГОС ВО, ОП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	Индикатор достижения компетенции (код и формулировка)	Перечень планируемых результатов обучения
<b>Общепрофессиональные компетенции</b>		
<b>ПК-3</b> Способен создавать и исследовать новые математические модели в естественных науках, промышленности и бизнесе, с учетом возможностей современных информационных технологий и программирования и компьютерной техники.	<b>И-ПК-3.2</b> Умеет использовать методы проектирования и производства программного продукта, принципы построения, структуры и приемы работы с инструментальными средствами, поддерживающими создание программного продукта	<b>Знать:</b> - основные понятия и определения теории конечных полей, конечных групп; - определения основных методов обработки сигналов (линейная и циклическая свертка, дискретное преобразование Фурье и т.п.); - формулировки утверждений, методы их доказательства; - методы построения быстрых алгоритмов цифровой обработки сигналов. Эти знания необходимы при решении практических задач из разнообразных прикладных областей, таких как обработка и передача данных, создание интегральных схем и др. <b>Уметь:</b> - решать задачи на построение быстрых алгоритмов вычисления линейной и циклической сверток малых длин,

		<p>применяя алгоритмы Кука – Тома и Винограда;</p> <ul style="list-style-type: none"> <li>- решать задачи на построение быстрых алгоритмов вычисления дискретного преобразования Фурье;</li> <li>- строить и анализировать быстрые алгоритмы дискретного преобразования Фурье с использованием алгоритмов Кули – Тьюки, Рейдера – Бреннера, Гуда – Томаса, Рейдера, Винограда;</li> <li>- оценивать сложность полученного алгоритма.</li> </ul> <p><b>Владеть:</b></p> <ul style="list-style-type: none"> <li>- математическим аппаратом, лежащим в основе построения быстрых алгоритмов цифровой обработки сигналов;</li> <li>- методами построения таких алгоритмов;</li> <li>- методами оценки сложности этих алгоритмов;</li> <li>- применять быстрые алгоритмы в смежных дисциплинах.</li> </ul>
--	--	---

#### 4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет **2** зачетных единиц, **72** акад. часов.

№ п/п	Темы (разделы) дисциплины, их содержание	Семестр	Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)						Формы текущего контроля успеваемости  Форма промежуточной аттестации (по семестрам)
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
1.	Вводная лекция	8	2						
2.	Группы, кольца, поля.	8	2					5	Задания для самостоятельной работы.
3.	Циклическая свертка и дискретное преобразование Фурье.	8	2			1		5	Задания для самостоятельной работы. Контр. раб. № 1
4.	Быстрые алгоритмы вычисления линейной и циклической свертки.	8	2	6		1		5	Задания для самостоятельной работы. Контр. раб. № 2
5.	Сложность алгоритмов вычисления свертки.	8	1	2		1		5	Задания для самостоятельной работы. Контр. раб. № 3

6.	Дискретное преобразование Фурье. Алгоритмы Кули - Тьюки и Гуда - Томаса.	8	3	2			5	Задания для самостоятельной работы
7.	Вычисление преобразования Фурье с помощью свертки.	8	2	2			5	Задания для самостоятельной работы
8.	Алгоритм Рейдера для различной длины преобразования Фурье.	8	2	4		1	5	Задания для самостоятельной работы. Контр. раб. № 4
							0,3	0,7
	<b>Всего</b>		<b>16</b>	<b>16</b>		<b>4</b>	<b>0,3</b>	<b>35,7</b>
								<b>Зачет</b>

### Содержание разделов дисциплины:

#### Тема № 1: Вводная лекция

Исторический обзор развития быстрых алгоритмов цифровой обработки сигналов. Введение в быстрые алгоритмы. Матричная запись алгоритма. Матрицы предположений и постсложения. Цифровой фильтр. Задача фильтрации, Фильтры с конечным импульсным откликом (КИО-фильтры) и авторегрессионные фильтры. Определение линейной свертки и корреляции. Запись через многочлены.

#### Тема № 2: Группы, кольца, поля.

Группа. Кольцо. Поле. Кольцо целых чисел. Характеристика кольца. Кольца многочленов. Кольцо  $Z_q$ . Кольцо с простой характеристикой. Поля Галуа. Расширения, подполя. Характеристика поля. Существование примитивного элемента.

Цикличность группы  $Z'_q$ . Китайская теорема об остатках для чисел. Китайская теорема об остатках для многочленов.

#### Тема № 3: Циклическая свертка и дискретное преобразование Фурье.

Циклическая свертка и ее связь с линейной. Определение дискретного преобразования Фурье (ДПФ). Теорема о свертке. История развития быстрых алгоритмов обработки сигналов.

Вычисление циклической свертки с использованием теоремы о свертке и дискретного преобразования Фурье. Вещественное преобразование Фурье. Одновременное вычисление двух вещественных сверток.

#### Тема № 4: Быстрые алгоритмы вычисления линейной и циклической сверток

Алгоритм Кука – Тома вычисления линейной свертки. Иллюстрация на примере  $2 \times 2$  – свертки. Матричная форма записи алгоритма. Модификация алгоритма.

Алгоритмы Винограда вычисления коротких сверток. Алгоритм Винограда как обобщение метода вычисления сверток с помощью преобразования Фурье. Иллюстрация на примере  $3 \times 2$  – свертки.

Матричная запись алгоритма. Обобщение алгоритма Винограда. Построение алгоритмов коротких линейных сверток:  $3 \times 3$  – свертка. Сравнение разных алгоритмов вычисления  $3 \times 2$  – свертки.

Вещественные и комплексные свертки. Сложность.

Вычисление произведения многочленов по модулю некоторого многочлена с помощью алгоритма свертки. Сравнение сложности разных алгоритмов.

Построение алгоритмов коротких циклических сверток. Иллюстрация на примере 4 –точечной циклической свертки. Матричная запись. Вычисление над полем вещественных и над полем комплексных чисел. Алгоритм Винограда как метод разложения матриц. Теплицевы матрицы. Теорема об обмене матриц.

### **Тема № 5: Сложность алгоритмов вычисления сверток.**

Свертки в общих кольцах и полях. Сложность алгоритмов свертки. Формализация алгоритмов (к задаче вида  $s = Hd$ ). Ранг матрицы по  $H$  строкам. Теорема о ранге матрицы  $H$  по строкам. Ранг матрицы  $H$  по столбцам. Теорема о ранге по столбцам.

Оценка снизу количества умножений для вычисления линейной свертки. Теоремы об оценке числа умножений в задаче вычисления произведения двух многочленов по модулю третьего.

### **Тема № 6: Дискретное преобразование Фурье. Алгоритмы Кули - Тьюки и Гуда - Томаса.**

Алгоритм Кули – Тьюки быстрого преобразования Фурье. Оценка сложности алгоритма.

Алгоритмы Кули – Тьюки по малому основанию: БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по времени, БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по частоте. Иллюстрация на примере 8 – точечного преобразования. Оценка сложности этих алгоритмов.

Модификация БПФ Рейдера – Бреннера. БПФ – алгоритмы Кули – Тьюки по основанию четыре с прореживанием по времени и по частоте. Матричная запись и оценка сложности.

Алгоритм Гуда – Томаса быстрого преобразования Фурье. Сложность алгоритма.

### **Тема № 7: Вычисление преобразования Фурье с помощью свертки.**

Вычисление преобразования Фурье с помощью свертки. Два способа перехода от преобразования Фурье к свертке: чирп – алгоритм Блестейна и алгоритм Рейдера для простых чисел. Иллюстрация алгоритма Рейдера в поле  $GF(p)$ . Построение 5 – точечного преобразования Фурье с помощью алгоритма Рейдера.

### **Тема № 8: Алгоритм Рейдера для различной длины преобразования Фурье.**

Алгоритм Рейдера в случае, когда длина преобразования равна степени нечетного простого числа. Случай, когда длина преобразования равна степени двойки. Иллюстрация на примере 16 – точечного преобразования Фурье.

Алгоритм Винограда для быстрого преобразования Фурье малой длины. Случай, когда длина преобразования равна:

- а) простому числу;
- б) степени простого числа;
- в) степени двойки

## **5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине**

В процессе обучения используются следующие образовательные технологии:

**Вводная лекция** – дает первое целостное представление о дисциплине и ориентирует студента в системе изучения данной дисциплины. Студенты знакомятся с назначением и задачами курса, его ролью и местом в системе учебных дисциплин и в системе подготовки в целом. Дается краткий обзор курса, история развития науки и практики, достижения в этой сфере, имена известных ученых, излагаются перспективные направления исследований. На этой лекции высказываются методические и организационные особенности работы в рамках данной дисциплины, а также дается анализ рекомендуемой учебно-методической литературы.

**Академическая лекция с элементами лекции-беседы** – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Элементы лекции-беседы обеспечивают контакт преподавателя с аудиторией, что позволяет привлекать внимание студентов к наиболее важным темам дисциплины, активно

вовлекать их в учебный процесс, контролировать темп изложения учебного материала в зависимости от уровня его восприятия.

**Практическое занятие** – занятие, посвященное освоению конкретных умений и навыков по закреплению полученных на лекции знаний.

**Консультации** – вид учебных занятий, являющийся одной из форм контроля самостоятельной работы студентов. На консультациях по просьбе студентов рассматриваются наиболее сложные моменты при освоении материала дисциплины, преподаватель отвечает на вопросы студентов, которые возникают у них в процессе самостоятельной работы.

## **6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине**

В процессе осуществления образовательного процесса по дисциплине используются:

для формирования материалов для текущего контроля успеваемости и проведения промежуточной аттестации, для формирования методических материалов по дисциплине:

- программы Microsoft Office;
- издательская система LaTeX;
- Adobe Acrobat Reader.

## **7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине (при необходимости)**

В процессе осуществления образовательного процесса по дисциплине используются:

- Автоматизированная библиотечно-информационная система «БУКИ-NEXT»  
[http://www.lib.uniyar.ac.ru/opac/bk\\_cat\\_find.php](http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php)
- Электронная библиотечная система «Лань» <https://e.lanbook.com>
- Электронная библиотечная система «Юрайт» <https://urait.ru>
- Электронная библиотечная система «Консультант студента»  
<https://www.studentlibrary.ru>

## **8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины**

### **а) основная литература**

1. Яблокова С.И. Введение в быстрые алгоритмы цифровой обработки сигналов: учебное пособие. – Ярославль, ЯрГУ, 2009. <http://www.lib.uniyar.ac.ru/edocs/iuni/20090238.pdf>

### **б) дополнительная литература**

1. Берлекэмп Э. Алгебраическая теория кодирования. / Э.Берлекэмп; Под ред.С.Д.Бермана.Пер.с англ - М.: Мир, 1971. - 477с.
2. Р. Блейхут. Быстрые алгоритмы цифровой обработки сигналов. – М.: Мир, 1989.

## **9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине**

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

- учебные аудитории для проведения занятий лекционного типа;
- учебные аудитории для проведения практических занятий (семинаров);
- учебные аудитории для проведения групповых и индивидуальных консультаций;
- учебные аудитории для проведения текущего контроля и промежуточной аттестации;
- помещения для самостоятельной работы;
- помещения для хранения и профилактического обслуживания технических средств обучения.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа к электронной информационно-образовательной среде ЯрГУ.

### **Автор:**

Доцент кафедры алгебры и математической логики,  
к.ф.-м.н.

С. И. Яблокова

**Приложение № 1 к рабочей программе дисциплины  
«Быстрые алгоритмы»**

**Фонд оценочных средств  
для проведения текущего контроля успеваемости  
и промежуточной аттестации студентов  
по дисциплине**

**1. Типовые контрольные задания и иные материалы,  
используемые в процессе текущего контроля успеваемости**

**Задания для самостоятельной работы**  
*(данные задания выполняются студентом самостоятельно  
и преподавателем в обязательном порядке не проверяются)*

**Задания по темам № 1 - 6.**

Построить быстрый алгоритм вычисления  $n \times m$  - линейной свертки над полем  $K$

а) применяя алгоритм Кука -Тоома:

1.  $n = 3, m = 2, K = R$ ;
2.  $n = 3, m = 3, K = R$ ;
3.  $n = 4, m = 3, K = R$ ;
4.  $n = 4, m = 4, K = R$ ;
5.  $n = 3, m = 2, K = C$ ;
6.  $n = 3, m = 3, K = C$ ;
7.  $n = 4, m = 3, K = C$ ;
8.  $n = 4, m = 4, K = C$ .

б) применяя алгоритм Винограда:

9.  $n = 3, m = 2, K = R$ ;
10.  $n = 3, m = 3, K = R$ ;
11.  $n = 4, m = 3, K = R$ ;
12.  $n = 4, m = 4, K = R$ ;
13.  $n = 3, m = 2, K = C$ ;
14.  $n = 3, m = 3, K = C$ ;
15.  $n = 4, m = 3, K = C$ ;



16.  $n = 4, m = 4, K = C$ .

Построить быстрый алгоритм перемножения двух многочленов по модулю многочлена  $m(x)$  над полем  $K$ , пользуясь алгоритмом Винограда:

1.  $m(x) = x(x^2 - 1)(x^2 + 1)(x - 2), K = R$ ;

2.  $m(x) = x^3 + x^2 + 1, K = R$ ;

3.  $m(x) = x^3 + 2x + 1, K = C$ ;

4.  $m(x) = x^3 + x^2 - 1, K = R$ ;

5.  $m(x) = x^3 + x^2 - 1, K = C$ ;

6.  $m(x) = x^3 - x^2 + x - 1, K = R$ ;

7.  $m(x) = x^3 + x + 1, K = R$ ;

8.  $m(x) = x^4 + x^3 - x - 1, K = R$ ;

9.  $m(x) = x^3 - x^2 + x - 1, K = R$ ;

10.  $m(x) = x(x^2 - 1)(x^2 + 1), K = R$ ;

11.  $m(x) = x^4 + 4, K = C$ ;

12.  $m(x) = x^5 + 1, K = R$ ;

13.  $m(x) = x^4 + 1, K = C$ ;

14.  $m(x) = x^3 + 2x^2 + 1, K = R$ ;

15.  $m(x) = x^4 + x^3 - 1, K = R$ ;

16.  $m(x) = x^4 + x^2 + 1, K = C$ ;

17.  $m(x) = x^4 + x^3 + 1, K = R$ ;

18.  $m(x) = x^4 + x^3 + x^2 + x + 1, K = R$ ;

19.  $m(x) = x^3 + x^2 + 2, K = R$ .

### **Задания по темам № 7,8.**

Построить БПФ-алгоритм  $n$  – точечного дискретного преобразования Фурье

а) пользуясь алгоритмом Кули - Тьюки:

1.  $n = 6$ ;

2.  $n = 8$ ;

3.  $n = 10$ ;

4.  $n = 16$ ;

5.  $n = 12$ ;

6.  $n = 24$ .

б) пользуясь алгоритмом Гуда - Томаса:

7.  $n = 10$ ;

8.  $n = 15$ ;

9.  $n = 21$ ;

10.  $n = 12$ ;

11.  $n = 35$ ;

12.  $n = 33$ .

Применить алгоритм Рейдера для сведения  $n$  – точечного ДПФ к свертке:

1.  $n = 7$ ;

2.  $n = 11$ ;

3.  $n = 13$ ;

4.  $n = 17$ ;

5.  $n = 9$ ;

6.  $n = 25$ ;

7.  $n = 49$ ;

8.  $n = 8$ ;

9.  $n = 16$ ;

10.  $n = 32$ .

**Контрольная работа № 1**  
(проверка сформированности ПК-3)

1. Построить быстрый алгоритм вычисления 3 – точечной циклической свертки над полем вещественных чисел (в качестве подполя взять поле рациональных чисел). Записать алгоритм в матричной форме и оценить число умножений и сложений.

2. Построить быстрый алгоритм вычисления произведения двух многочленов по модулю многочлена  $x^3 + x + 1$  над полем вещественных чисел ( в качестве подполя взять поле рациональных чисел). Записать алгоритм в матричной форме и оценить число умножений и сложений.

### Ответы к задачам:

1.

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & -2 \\ 1 & 1 & -2 & 1 \\ 1 & -2 & 1 & 1 \end{pmatrix} \begin{pmatrix} G_0 & 0 & 0 & 0 \\ 0 & G_1 & 0 & 0 \\ 0 & 0 & G_2 & 0 \\ 0 & 0 & 0 & G_3 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & -1 \\ 1 & -1 & 0 \\ 0 & 1 & -1 \end{pmatrix} \begin{pmatrix} d_0 \\ d_1 \\ d_2 \end{pmatrix}$$

$$G_0 = \frac{1}{3}(g_0 + g_1 + g_2), \quad G_1 = \frac{1}{3}(g_0 - g_2), \quad G_2 = \frac{1}{3}(g_0 - g_1), \quad G_3 = \frac{1}{3}(g_1 - g_2)$$

Алгоритм содержит 4 умножения, 5 предположений и 11 постсложений.

2.

$$\begin{pmatrix} s_0 \\ s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & -1 & 2 \\ -2 & 3 & -1 & -2 & 3 \\ -2 & 1 & 3 & 0 & -2 \end{pmatrix} \begin{pmatrix} G_0 & 0 & 0 & 0 \\ 0 & G_1 & 0 & 0 \\ 0 & 0 & G_2 & 0 \\ 0 & 0 & 0 & G_3 \\ & & & G_4 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 1 \\ 1 & -1 & 1 \\ 1 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} d_0 \\ d_1 \\ d_2 \end{pmatrix}$$

$$G_0 = \frac{1}{3}g_0, \quad G_1 = \frac{1}{2}(g_0 + g_1 + g_2), \quad G_2 = \frac{1}{6}(g_0 - g_1 + g_2), \quad G_3 = \frac{1}{6}(g_0 + 2g_1 + 4g_2), \\ G_4 = g_2.$$

Алгоритм содержит 5 умножений и 24 сложения.

### Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены несущественные ошибки в вычислениях – 1 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 0 баллов;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 7-8 соответствует оценке «отлично», 6 баллов – оценке «хорошо», 4-5 баллов – оценке «удовлетворительно», менее 4 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

### Контрольная работа № 2

(проверка сформированности ПК-3)

1. Пользуясь алгоритмом Гуда – Томаса, построить быстрый алгоритм вычисления 6 – точечного преобразования Фурье. Оценить сложность алгоритма.
2. Применить алгоритм Рейдера к 11 – точечному преобразованию Фурье, свести его к вычислению свертки. Вычисления проводятся в поле вещественных чисел (в качестве подполя взять поле рациональных).

### Ответы к задачам:

1.  $n = 2 \cdot 3, \quad n' = 2, \quad n'' = 3.$

Сворачиваем входной вектор в матрицу

$$(v_0, v_1, v_2, v_3, v_4, v_5) \rightarrow \begin{pmatrix} v_0 & v_4 & v_2 \\ v_3 & v_1 & v_5 \end{pmatrix} = \begin{pmatrix} v_{00} & v_{01} & v_{02} \\ v_{10} & v_{11} & v_{12} \end{pmatrix}$$

Над каждой строкой полученной матрицы проводим 3-точечное преобразование Фурье

$$r_{ik} = \sum_{j=0}^2 \omega^{2jk} v_{ij} = v_{i0} + \omega^{2k} v_{i1} + \omega^{4k} v_{i2} \quad (i = 0,1; \quad k = 0,1,2)$$

$$r_{i0} = v_{i0} + v_{i1} + v_{i2} \quad (i = 0,1), \quad \begin{pmatrix} r_{i1} \\ r_{i2} \end{pmatrix} = \begin{pmatrix} v_{i0} \\ v_{i1} \end{pmatrix} + \begin{pmatrix} \omega^2 & \omega^4 \\ \omega^4 & \omega^2 \end{pmatrix} \begin{pmatrix} v_{i1} \\ v_{i2} \end{pmatrix} \quad (i = 0,1)$$

Получаем матрицу  $\begin{pmatrix} r_{00} & r_{01} & r_{02} \\ r_{10} & r_{11} & r_{12} \end{pmatrix}$ . Над каждым столбцом этой матрицы проводим 2-точечное преобразование Фурье  $V_{lk} = \sum_{j=0}^1 \omega^{3lj} r_{jk} = r_{0k} + \omega^{3l} r_{1k} \quad (l = 0,1; \quad k = 0,1,2)$ .

$$V_{0k} = r_{0k} + r_{1k}, \quad V_{1k} = r_{0k} - r_{1k} \quad (k = 0,1,2).$$

Получаем матрицу

$$\begin{pmatrix} V_{00} & V_{01} & V_{02} \\ V_{10} & V_{11} & V_{12} \end{pmatrix} = \begin{pmatrix} V_0 & V_2 & V_4 \\ V_3 & V_5 & V_1 \end{pmatrix} \rightarrow (V_0, V_1, V_2, V_3, V_4, V_5).$$

Алгоритм содержит 4 умножения (надо вычислить две 2-точечные циклические свертки).

$$2. \quad V_0 = \sum_{j=0}^{10} v_j, \quad V_k = v_0 + V_k^1 \quad (k = 1, 2, \dots, 10).$$

Вычисление  $V_k^1 \quad (k = 1, \dots, 10)$  сводится к 10-точечной циклической свертке  $d(x)g(x) \pmod{x^{10} - 1}$ ,

$$\begin{aligned} d(x) &= v_1 + v_6 x + v_3 x^2 + v_7 x^3 + v_9 x^4 + v^{10} x^5 + v_5 x^6 + v_8 x^7 + v_4 x^8 + v_2 x^9, \\ g(x) &= \omega + \omega^2 x + \omega^4 x^2 + \omega^8 x^3 + \omega^5 x^4 + \omega^{10} x^5 + \omega^9 x^6 + \omega^7 x^7 + \omega^3 x^8 + \omega^6 x^9, \\ s(x) &= V_1^1 + V_2^1 x + V_4^1 x^2 + V_8^1 x^3 + V_5^1 x^4 + V_{10}^1 x^5 + V_9^1 x^6 + V_7^1 x^7 + V_3^1 x^8 + V_6^1 x^9. \end{aligned}$$

Если факторизовать матрицу 10-точечной циклической свертки

$$\tilde{W} = \begin{pmatrix} W_1 & W_2 \\ W_2 & W_1 \end{pmatrix} = \begin{pmatrix} E_5 & E_5 \\ E_5 & -E_5 \end{pmatrix} \begin{pmatrix} \frac{1}{2}(W_1 + W_2) & O \\ O & \frac{1}{2}(W_1 - W_2) \end{pmatrix} \begin{pmatrix} E_5 & E_5 \\ E_5 & -E_5 \end{pmatrix}$$

то вычисления  $V_k^1 \quad (k = 1, \dots, 10)$  сводится к двум 5-точечным циклическим сверткам

$$s_1(x) = d_1(x)g_1(x) \pmod{x^5 - 1}, \quad d_1(x) = (v_1 + v_{10}) + (v_6 + v_5)x + (v_3 + v_8)x^2 + (v_7 + v_4)x^3 + (v_9 + v_2)x^4,$$

$$g_1(x) = \cos \vartheta + x \cos 9\vartheta + x^2 \cos 7\vartheta + x^3 \cos 3\vartheta + x^4 \cos 6\vartheta$$

и

$$s_2(x) = d_2(x)g_2(x) \pmod{x^5 - 1}, \quad d_2(x) = (v_1 - v_{10}) + (v_6 - v_5)x + (v_3 - v_8)x^2 + (v_7 - v_4)x^3 + (v_9 - v_2)x^4, \quad g_2(x) = i \sin \vartheta + x i \sin 9\vartheta + x^2 i \sin 7\vartheta + x^3 i \sin 3\vartheta + x^4 i \sin 6\vartheta.$$

$$\left( \vartheta = -\frac{2\pi}{11} \right).$$

#### Правила выставления оценки по результатам контрольной работы:

Оценка по результатам контрольной работы считается в баллах по каждому заданию по следующему принципу:

- правильно выполненное задание – 4 балла;
- при выполнении задания правильно найден оптимальный алгоритм решения, но имеются незначительные ошибки в численных расчетах – 3 балла;
- при выполнении задания не найден оптимальный алгоритм и допущены несущественные ошибки в вычислениях – 1 балла;

- при выполнении задания не найден оптимальный алгоритм и допущены существенные ошибки в вычислениях – 0 баллов;
- при выполнении задания неправильно – 0 баллов.

Набранное количество баллов 7-8 соответствует оценке «отлично», 6 баллов – оценке «хорошо», 4-5 баллов – оценке «удовлетворительно», менее 4 баллов – оценке «неудовлетворительно» (умения и навыки на данном этапе освоения дисциплины не сформированы).

## **2. Список вопросов и (или) заданий для проведения аттестации**

Аттестация по дисциплине проводится в форме зачета. Зачет проводится в форме собеседования. Для допуска к собеседованию студент в течение семестра должен удовлетворительно написать контрольные №№ 1 -- 2, т. е. в каждой контрольной работе правильно решить 75-80% предложенных задач. Если это условие не выполнено, студенту сначала предлагается решить задачи по тем темам, которые вызывали у него трудности в течение семестра. Задачи подбираются аналогичные тем, которые предлагались в контрольных работах.

### **Вопросы к зачету по курсу «Быстрые алгоритмы»:**

Цифровой фильтр. Задача фильтрации, Фильтры с конечным импульсным откликом (КИО-фильтры) и авторегрессионные фильтры. Определение линейной свертки и корреляции. Запись через многочлены. Циклическая свертка и ее связь с линейной. Определение дискретного преобразования Фурье (ДПФ). Теорема о свертке.

Группа. Кольцо. Поле. Кольцо целых чисел. Характеристика кольца. Кольца многочленов. Кольцо  $Z_q$ . Кольцо с простой характеристикой.

Поля Галуа. Расширения, подполя. Характеристика поля. Существование примитивного элемента.

Цикличность группы  $Z'_q$ . Китайская теорема об остатках для чисел. Китайская теорема об остатках для многочленов.

Вычисление циклической свертки с использованием теоремы о свертке и дискретного преобразования Фурье. Вещественное преобразование Фурье.

Одновременное вычисление двух вещественных сверток.

Алгоритм Кука – Тома вычисления линейной свертки. Иллюстрация на примере  $2 \times 2$  – свертки. Матричная форма записи алгоритма. Модификация алгоритма.

Алгоритмы Винограда вычисления коротких сверток. Алгоритм Винограда как обобщение метода вычисления сверток с помощью преобразования Фурье. Иллюстрация на примере  $3 \times 2$  – свертки. Матричная запись алгоритма.

Обобщение алгоритма Винограда. Построение алгоритмов коротких линейных сверток:  $3 \times 3$  – свертка. Сравнение разных алгоритмов вычисления  $3 \times 2$  – свертки.

Вещественные и комплексные свертки. Сложность.

Вычисление произведения многочленов по модулю некоторого многочлена с помощью алгоритма свертки. Сравнение сложности разных алгоритмов. Построение алгоритмов коротких циклических сверток. Иллюстрация на примере 4-точечной циклической свертки. Матричная запись. Вычисление над полем вещественных и над полем комплексных чисел. Алгоритм Винограда как метод разложения матриц. Теплицевы матрицы. Теорема об обмене матриц.

Свертки в общих кольцах и полях. Сложность алгоритмов свертки. Формализация алгоритмов (к задаче вида  $s = Hd$ ). Ранг матрицы по  $H$  строкам.

Теорема о ранге матрицы  $H$  по строкам. Ранг матрицы  $H$  по столбцам. Теорема о ранге по столбцам. Оценка снизу количества умножений для вычисления линейной свертки.

Теоремы об оценке числа умножений в задаче вычисления произведения двух многочленов по модулю третьего.

Алгоритм Кули – Тьюки быстрого преобразования Фурье. Оценка сложности алгоритма.

Алгоритмы Кули – Тьюки по малому основанию: БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по времени.

БПФ – алгоритм Кули – Тьюки по основанию два с прореживанием по частоте. Иллюстрация на примере 8 – точечного преобразования. Оценка сложности этих алгоритмов.

Модификация БПФ Рейдера – Бреннера. БПФ – алгоритмы Кули – Тьюки по основанию четыре с прореживанием по времени и по частоте. Матричная запись и оценка сложности. Алгоритм Гуда – Томаса быстрого преобразования Фурье. Сложность алгоритма.

Два способа перехода от преобразования Фурье к свертке: чирп – алгоритм Блестейна и алгоритм Рейдера для простых чисел. Иллюстрация алгоритма Рейдера в поле  $GF(p)$ .

Построение 5 – точечного преобразования Фурье с помощью алгоритма Рейдера.

Алгоритм Рейдера в случае, когда длина преобразования равна степени нечетного простого числа.

Случай, когда длина преобразования равна степени двойки. Иллюстрация на примере 16 – точечного преобразования Фурье.

Алгоритм Винограда для быстрого преобразования Фурье малой длины. Случай, когда длина преобразования равна:

- а) простому числу;
- б) степени простого числа;
- в) степени двойки.

### **Вопросы для самопроверки при подготовке к зачету на примере тем 2 -- 5.**

**Вопрос 1.** Если ли связь между линейной и циклической?

Варианты ответов:

- 1). да;
- 2). нет.

**Вопрос 2.** Какова оценка числа умножений при прямом вычислении линейной свертки?

Варианты ответов:

- 1). Число умножений равно  $NL$ ;
- 2). Число умножений равно  $(N-1)(L-1)$  ;
- 3). Число умножений равно  $N+L$ .

**Вопрос 3.** Какова оценка числа умножений при прямом вычислении  $n$  – точечной циклической свертки?

Варианты ответов:

- 1).  $n(n - 1)$  ;

2.  $n^2$ ;
- 3).  $(n - 1)^2$ .

**Вопрос 4.** Какова минимальная оценка числа умножений для вычисления линейной свертки с помощью быстрого алгоритма?

Варианты ответов:

- 1).  $N(L - 1)$ ;
- 2).  $N + L - 1$ ;
- 3).  $N + L + 1$ .

**Вопрос 5.** Какова минимальная оценка числа умножений для вычисления произведения двух многочленов по модулю неприводимого над данным полем многочлена 5-й степени (для поля характеристики 0)?

Варианты ответов:

- 1). 9;
- 2). 10;
- 3). 12.

**Вопрос 6.** Какова минимальная оценка числа умножений для вычисления произведения двух многочленов по модулю многочлена 5-й степени, раскладывающегося в произведение неприводимых над данным полем многочленов 2 и 3 степеней (для поля характеристики 0)?

Варианты ответов:

- 1). 9;
- 2). 8;
- 3). 10.

**Вопрос 7.** Как оценивается число умножений алгоритма Кули-Тьюки по основанию 2 с прореживанием по времени для поля вещественных чисел?

Варианты ответов:

- 1).  $n \log_2 n$  ;
- 2).  $\frac{n(n-1)}{2}$ ;
- 3).  $\frac{n}{2} \log_2 n$ .

**Вопрос 8.** Как оценивается число вещественных сложений алгоритма Кули-Тьюки по основанию 2 с прореживанием по частоте над полем комплексных чисел?

Варианты ответов:

- 1).  $\frac{3n}{2} \log_2 n$ ;
- 2).  $3n \log_2 n$ ;
- 3).  $\frac{3n(n-1)}{2}$ ;
- 4).  $2n \log_2 n$ .

**Вопрос 9.** Как можно оценить число умножений для вычисления 21-точечного преобразования Фурье при использовании алгоритма Гуда-Томаса

Варианты ответов:

- 1).  $n \leq 210$ ;
- 2).  $n = 441$ ;
- 3).  $n \leq 100$ .

### Правильные ответы

Вопрос №	Вариант ответа		Вопрос №	Вариант ответа		Вопрос №	Вариант ответа
<b>1</b>	1		<b>4</b>	2		<b>7</b>	3
<b>2</b>	1		<b>5</b>	1		<b>8</b>	2
<b>3</b>	2		<b>6</b>	2		<b>9</b>	1

Количество правильных ответов не менее 7 вместе с правильно решенными задачами по изученным темам соответствует уровню формирования в рамках данной дисциплины компетенций ОПК-2 не ниже порогового уровня. В этом случае студенту выставляется оценка "зачтено".

### **Список вопросов и (или) заданий для проведения итоговой аттестации**

Итоговая аттестация по дисциплине проводится в форме экзамена. Экзамен состоит из письменной и устной частей. Письменная часть проводится в виде контрольной работы по задачам, решавшимся во втором семестре (темы 11 -18). Задачи аналогичны приведенным в контрольных работах 5 - 6. Возможно добавление задач по теме "Быстрые алгоритмы цифровой обработки сигналов". Устная часть проводится в виде собеседования. Студент отвечает на вопросы билета и вопросы преподавателя, возникающие в процессе изложения теоретического материала.

### **Примерные задания по теме "Быстрые алгоритмы цифровой обработки сигналов" на зачете**

1. Используя алгоритм Винограда, построить оптимальный по умножению алгоритм вычисления произведения двух многочленов по модулю многочлена

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

над полем  $\mathbb{R}$ . Найти число умножений и сложений.

2. Используя алгоритм Рейдера, свести 9-точечное преобразование Фурье к свертке.



## **Приложение № 2 к рабочей программе дисциплины «Быстрые алгоритмы»**

### **Методические указания для студентов по освоению дисциплины**

Для успешного усвоения данного курса необходимо знание следующих вопросов из других математических дисциплин:

- сравнения по модулю целого числа, свойства сравнений;
- китайская теорема об остатках для чисел и для многочленов;
- функция Эйлера и ее основные свойства;
- теорема Эйлера и малая теорема Ферма;
- кольцо и поле вычетов по модулю натурального числа;
- мультипликативная группа кольца вычетов;
- строение мультипликативных групп колец вычетов по модулю простого числа, по модулю степени простого числа и по модулю степени двойки;
- интерполяционная формула Лагранжа.