

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное учреждение
высшего профессионального образования
"Казанский (Приволжский) федеральный университет"

УТВЕРЖДАЮ

Проректор по научной деятельности КФУ

Проф. Д.К. Нургалеев

" 12 " 2014 г.



Программа дисциплины

Б1.В.ДВ.1. Квантовая информатика

Направление подготовки: 09.06.01 Информатика и вычислительная техника

Направленность (профиль) подготовки: 05.13.11. Математическое и программное обеспечение вычислительных машин, комплексов и компьютерных сетей

Квалификация выпускника «Исследователь. Преподаватель-исследователь»

Казань
2014

Аннотация

1. Цели освоения дисциплины Изучение дисциплины «Квантовая информатика» преследует целью ознакомление с новейшими тенденциями в области информатики и компьютерных наук, связанными с построением и анализом различных моделей для обработки и передачи информации, функционирование которых основано на законах квантовой механики, а также изучение эффективных квантовых алгоритмов для решения задач, для которых на сегодняшний день эффективных классических алгоритмов неизвестно.

2. Место дисциплины в структуре программы аспирантуры Курс «Квантовая информатика» входит в блок дисциплин по выбору, рассчитан на 18 часов лекционных, 18 часов практических занятий и 72 часа самостоятельной работы. Дисциплина читается на 2 курсе в 4 семестре. В курсе рассматриваются история зарождения квантовой информатики, приводятся необходимые определения и понятия, опирающиеся на постулаты квантовой механики, детально рассматриваются известные квантовые алгоритмы обработки и передачи информации, демонстрирующие мощь квантовых вычислений по сравнению с классическими. По окончании курса студент должен владеть основными понятиями квантовой информатики: понятием кубита, квантовой суперпозиции, квантовой системы, квантовых преобразований и измерения квантовой системы, знать основные законы квантовых вычислений, ориентироваться в рассмотренных квантовых алгоритмах преобразования и обработки информации.

3. Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) в соответствии с ФГОС ВО программ подготовки научно-педагогических кадров в аспирантуре

Знать: историю зарождения квантовой информатики и состояние развития данной области информатики на сегодняшний день;

Уметь: объяснять с математической точки зрения такие явления квантовой механики, как телепортация, запутанность состояний, невозможность копирования квантового состояния, квантовый параллелизм, и т.д.

Владеть: основными понятиями квантовой информатики, такими, как понятие кубита, преобразования квантовой системы, измерения квантовой системы;

Демонстрировать способность и готовность: применять полученные знания на практике

В результате освоения дисциплины формируются компетенции:

Профессиональные:

- способность подготавливать научные работы для публикации в ведущих российских и международных изданиях, а также выступления на российских и международных научно-практических конференциях (ПК-2).

4. Структура и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 3 зачетные единицы 108 часов. (лекции 18 ч., практика 18 ч., самостоятельная работа 72 ч.).

№	Раздел Дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)			Форма промежуточной аттестации (по
				лекции	практика	самост.	
)	

						работа	семестрам)
1	Введение. История возникновения квантовых вычислений.	4	1	1	1	4	
2	Основные понятия квантовых вычислений	4	1	1	1	4	
3	Основные постулаты квантовой механики.	4	2	1	1	4	
4	Определение запутанных квантовых состояния, примеры. EPR-парадокс.	4	2	1	1	4	
5	Квантовая криптография.	4	3	1	1	4	
6	Квантовые гейты.	4	3	1	1	4	
7	Массивы квантовых гейтов. Квантовые схемы.	4	4	1	1	4	
8	Плотное квантовое кодирование. Телепортация.	4	5	1	1	4	
9	Простейшие квантовые алгоритмы: алгоритм Дойча, алгоритм Дойча-Джозса, алгоритм Бернштейна-Вазирани.	4	6	1	1	4	
10	Алгоритм Саймона.	4	7	1	1	4	
11	Алгоритм Гровера поиска в неупорядоченной базе данных.	4	8	1	1	4	
12	Квантовое преобразование Фурье.	4	9	1	1	4	
13	Задача факторизации числа. Классический алгоритм. Квантовый алгоритм Шора.	4	10	1	1	4	
14	Устойчивость квантовых вычислений. Квантовое исправление ошибок.	4	11	1	1	4	

15	Квантовые и классические классы сложности.	4	12	1	1	4	
16	Определение квантового конечного автомата. Распознавание языков квантовыми конечными автоматами.	4	13	1	1	4	
17	Определение квантовой бинарной программы. Вычислений функций квантовыми ветвящимися программами.	4	14	1	1	4	
18	Сравнение квантовых и классических ветвящихся программ	4	15	1	1	4	
	Итого:			18	18	72	зачет

4.2 Содержание дисциплины

Тема 1. Математические основы квантовой информатики. Гильбертово пространство, линейные преобразования, унитарные оператор и его свойства, оператор проекции и его свойства. Выполнение упражнений на отработку правильного понимания и умения манипулировать основными понятиями линейной алгебры, используемые в квантовой информатике.

Тема 2. Основные понятия: квантовый бит, квантовый регистр, квантовая суперпозиция, квантовая система, проективное измерение. Основные постулаты квантовой механики. Квантовые преобразования, унитарные матрицы, теорема о неклонировании, запутанные состояния. Выполнение упражнений, контролирующих правильность понимания основных понятиями квантовой информатики (кубит, квантовое состояние, квантовое преобразование, измерение и т.д.) и умение манипулировать данными понятиями. Например, проверить унитарность матрицы, построить унитарную матрицу, проверить квантовое состояние на запутанность, и т.д.

Тема 4. Квантовые преобразования, квантовые гейты, квантовые схемы. Выполнение упражнений на построение и манипуляцию простейших квантовых схем.

Тема 5. Квантовая криптография. Проверка домашнего задания, примерные вопросы: Провести анализ квантовых протоколов распределения ключа.

Тема 6. Плотное квантовое кодирование. Телепортация. Проверка домашнего задания, примерные вопросы: Провести анализ квантовых алгоритмов, использующих запутанные состояния.

Тема 7. Квантовое и классическое преобразование Фурье. Проверка домашнего задания, примерные вопросы: Классическое преобразование Фурье, быстрое преобразование Фурье, квантовое преобразование Фурье. Провести их сравнительный анализ.

Тема 8. Квантовые алгоритмы: алгоритм Гровера, алгоритм Саймона, алгоритм Вазирани, телепортация, плотное кодирование. Проверка домашнего задания. Примерные варианты заданий, построить квантовый алгоритм, использующий идеи изученных квантовых алгоритмов: алгоритма Гровера, алгоритма Саймона, алгоритма

Вазирани, телепортации, плотного кодирования.

Тема 9. Алгоритм Шора факторизации чисел. Проверка домашнего задания, примерные вопросы: Факторизация числа. Классические и квантовый алгоритмы. Провести их сравнительный анализ.

Тема 10. Квантовые конечные автоматы. Распознавание языков. Построение эффективных квантовых автоматов. Проверка домашнего задания. Примерный вариант задания: построить квантовый автомат для конкретного языка. Оценить его сложность. Оценить вероятность ошибки.

Тема 11. Квантовые ветвящиеся программы. Построение эффективных квантовых ветвящихся программ.

5. Образовательные технологии

Обучение происходит в форме практических занятий, а также самостоятельной работы аспирантов. Рекомендуется предлагать к выполнению упражнения по теме занятия для самостоятельного выполнения с целью более глубокого закрепления и понимания материала. Если упражнения предлагаются для самостоятельного выполнения дома, то необходимо в начале следующего занятия уделить время для разбора упражнения и проверки правильности его выполнения. Целесообразно в ходе обсуждения решения задачи задавать выступающим и аудитории дополнительные и уточняющие вопросы с целью выяснения уровня усвоения теоретических аспектов обсуждаемых проблем. Следует поощрять выступления с места в виде кратких дополнений и вопросов к выступающим и преподавателю. Рекомендуется привлекать аспирантов к активному участию в проведении занятия, предлагая к самостоятельному доказательству несложные утверждения и давая подсказку в случае затруднения. Также рекомендуется отмечать посещаемость занятий.

Проводить групповые и индивидуальные консультации аспирантов по вопросам, возникающим у них в ходе их подготовки к аттестации по учебной дисциплине, рекомендовать в помощь учебные и другие материалы, а также справочную литературу. Кроме того, рекомендуется предлагать для самостоятельного доказательства некоторые частные утверждения, способствующие более глубокому пониманию изучаемой темы и развитию абстрактного мышления.

6. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине.

САМОСТОЯТЕЛЬНАЯ РАБОТА АСПИРАНТОВ (СРА) включает следующие виды работ:

Проработку лекционного материала, выполнение домашних заданий, изучение дополнительной литературы.

7. Фонд оценочных средств.

7.1. Регламент дисциплины

Оценочные средства текущего контроля – устные вопросы, решение задач, собеседование, тесты

«**Зачтено**» - Сформированные систематические представления об основных проблемах и методах решений и специфике нормативно-правовых актов, регламентирующих научную деятельность

«**Не зачтено**» - Фрагментарные представления об основных проблемах и методах решений. Фрагментарные представления о специфике нормативно-правовых актов, регламентирующих научную деятельность.

7.2. Оценочные средства текущего контроля

Формами промежуточного контроля являются:

- регулярная проверка выполнения заданий на практических занятиях;
- проверка хода работ по выполнению лабораторного задания на компьютере.

7.3 Вопросы к зачёту:

1. Понятие квантового бита. Основные свойства квантового бита. Его отличие от классического. Геометрическая интерпретация. Понятие стандартного (вычислительного) базиса. Квантовый регистр. Квантовое состояние. Информационное содержание квантового и классического битов.

2. Квантовый регистр и его состояние. Сравнение с классическим регистром. Пространство состояний квантового и классического регистров. Тензорное и декартово произведение пространств.

3. Квантовая система, квантовое состояние, преобразования квантовой системы, квантовое измерение как способ извлечения информации.

4. Понятие унитарного оператора и его основные свойства.

5. Квантовые гейты. Их сравнение с классическими гейтами. Примеры однокубитных и двухкубитных квантовых гейтов.

6. Понятие универсального квантового гейта. Квантовые схемы.

7. Преобразование Адамара. преобразование Уолша-Адамара. Примеры алгоритмов, использующих данные преобразования.

8. Вычисление функций на квантовом компьютере. В чем состоит мощь и ограниченность квантового вычисления функций. Понятие квантового параллелизма.

9. Теорема о неклонировании. Использование гейта CNOT для создания запутанных состояний. Объяснение данного явления в свете Теоремы о неклонировании.

10. Запутанность как один из феноменов квантовой механики. Два различных определения запутанных квантовых состояний. Примеры использования.

11. Алгоритм плотного кодирования.

12. Телепортация (алгоритм передачи квантового состояния).

13. Алгоритм Дойча. Квантовая сложность алгоритма в сравнении с классической.

14. Алгоритм Дойча-Джозса. Квантовая сложность алгоритма в сравнении с классической.

15. Алгоритм Гровера. Квантовая сложность алгоритма в сравнении с классической.

16. Алгоритм Саймона. Квантовая сложность алгоритма в сравнении с классической.

17. Сведение задачи факторизации к задаче нахождения периода функции. Алгоритм Шора факторизации числа (без изложения алгоритма нахождения периода).

18. Преобразование Фурье (детерминированное, быстрое, квантовое). Классическая и квантовая сложность преобразования Фурье. Роль квантового преобразования Фурье в алгоритме Шора.

19. Алгоритм Шора нахождения периода функции.

20. Алгоритм Шора факторизации числа.

21. RSA-алгоритм шифрования. Почему использование квантового компьютера поможет взломать системы, основанные на методе RSA-шифрования с открытым ключом.

22. Определение квантового конечного автомата с одним измерением. Сравнение с детерминированным, вероятностным конечным автоматом.

23. Свойство: квантовые конечные автоматы распознают собственное подмножество регулярных языков.

24. Сравнительная сложность квантовых, детерминированных и вероятностных конечных автоматов на примере булевой функции MODp.

7.4. Таблица соответствия компетенций, критериев оценки их освоения и

оценочных средств

Индекс компетенции	Расшифровка компетенции	Показатель формирования компетенции для данной дисциплины	Оценочное средство
ПК-2	способность подготавливать научные работы для публикации в ведущих российских и международных изданиях, а также выступления на российских и международных научно-практических конференциях	Аспирант способен подготавливать научные работы для публикации в ведущих российских и международных изданиях, а также выступления на российских и международных научно-практических конференциях.	Решение задач на практических занятиях. Программа эмулирующая квантовый алгоритм.

8. Методические указания для обучающихся при освоении дисциплины

В курсе дисциплины «Квантовые информатика» описывается история зарождения квантовых вычислений;

- приводятся определения и понятия, используемые в квантовой информатике и опирающиеся на постулаты квантовой механики;
- обсуждаются основные законы квантовых вычислений;
- детально рассматриваются известные квантовые алгоритмы обработки и передачи информации, демонстрирующие мощь квантовых вычислительных моделей по сравнению с классическими.

По окончании курса аспирант должен владеть основными понятиями квантовой информатики, такими, как понятие кубита, квантового регистра, квантовых преобразований и измерения квантовой системы, знать основные законы квантовых вычислений, ориентироваться в рассмотренных квантовых алгоритмах.

На практических занятиях аспиранты выполняют задания, закрепляющие пройденный на лекциях теоретический материал.

Последние два практических занятия (а также часы самостоятельной работы) отведены под лабораторную работу. Целью лабораторной работы является написание и отладка программы, эмулирующей квантовый алгоритм на классическом компьютере. Выбор квантового алгоритма производится на усмотрение преподавателя из рассмотренных на лекциях квантовых алгоритмов. При создании программы-эмулятора квантового алгоритма необходимо

- произвести выбор структуры данных для представления кубита, квантового регистра;
- последовательность шагов в реализации алгоритма должна в точности соответствовать последовательности шагов алгоритма в его квантовой интерпретации;
- программа, реализующая алгоритм, должна быть протестирована на разных входных данных.

Выбор языка программирования – на усмотрение программиста.

Форма контроля – зачет. Для допуска к сдаче зачета

- должны быть выполнены все задания, предлагаемые на практических занятиях,
- аспирант должен представить работающую программу-эмулятор и объяснить ее;
- должен быть представлен отчет по программе-эмулятору в электронном и бумажном виде.

Зачет производится в устной форме. Билеты, предлагаемые на зачете, содержат

1. Один теоретический вопрос по курсу прочитанных лекций
2. Одну задачу, подобную тем, что рассматривались на практических занятиях.

9. Учебно-методическое и информационное обеспечение дисциплины (модуля)

9.1 Основная литература:

1. Аблаев Ф. М., Васильев А. В. Классические и квантовые ветвящиеся программы. Казанский (Приволжский) федеральный университет: Институт вычислительной математики и информационных технологий, Кафедра теоретической кибернетики, 2010. http://libweb.ksu.ru/ebooks/09-IVMIT/09_62_2010_000088.pdf

2. Р. Перри Элементарное введение в квантовые вычисления : [учебное пособие] / Р. Перри ; пер. с англ. А. Д. Калашникова .— Долгопрудный : Интеллект, 2015 .— 203 с. : ил., портр. ; 21 .— Загл. и авт. ориг.: Quantum Computing from the Ground Up / Riley Tipton Perry .— Библиогр.: 201-203 (40 назв.).

9.2 Дополнительная литература:

1. Классические и квантовые вычисления / А. Китаев, А. Шень, М. Вьялый .? Москва : МЦНМО: ЧеРо, 1999. 191 с.

2. М. Нильсен, И. Чанг. Квантовые вычисления и квантовая информация.— М : Мир, 2006 .— 824 с.

3. Ш. Имре, Ф. Балаж Квантовые вычисления и связь. Инженерный подход : перевод с английского / Ш. Имре, Ф. Балаж ; Пер. А. А. Калачева, Т. Г. Митрофановой, С. В. Петрушкина; Под ред. В. В. Самарцева .? Москва : Физматлит, 2008 .? 320 с.

4. Хренников, А. Ю. Введение в квантовую теорию информации [Электронный ресурс] / А. Ю. Хренников. - М. : ФИЗМАТЛИТ, 2008. - 284 с. http://e.lanbook.com/books/element.php?pl1_id=2176

9.3 Программное обеспечение и Интернет-ресурсы:

- Интернет-портал образовательных ресурсов КФУ - <http://www.kfu-elearning.ru/>
- Интернет-портал образовательных ресурсов по ИТ - <http://algolist.manual.ru>
- Интернет-портал по математическим наукам - <http://www.mathnet.ru>
- Интернет-портал ресурсов по математике - <http://www.allmath.com/>
- Интернет-портал ресурсов по математическим наукам - <http://www.math.ru/>

10. Материально-техническое обеспечение дисциплины (модуля)

Лекции по дисциплине проводятся в аудитории, оснащенной доской и мелом (маркером). Практические занятия требуют аудиторий, оснащенных компьютерами.

- Электронная библиотечная система «znanium.com»
- Электронная библиотечная издательства «Лань»

Программа составлена в соответствии с требованиями ФГОС ВО аспирантуры и с учётом рекомендаций по направлению подготовки.

Автор: к.ф.-м.н., доцент Гайнутдинова А.Ф.

Рецензенты: д.ф.-м.н., профессор Аблаев Ф.М.

Программа одобрена на заседании Учебно-методической комиссии Института ВМ и ИТ КФУ от 11 сентября 2014 г. протокол № 1.