

**Федеральное государственное автономное образовательное
учреждение высшего образования
«Московский физико-технический институт
(национальный исследовательский университет)»**

УТВЕРЖДЕНО

**Директор физтех-школы
радиотехники и компьютерных
технологий**

Д.А. Гаврилов

	Рабочая программа дисциплины (модуля)
по дисциплине:	Теория информации
по направлению:	Прикладные математика и физика
профиль подготовки:	Радиотехника и компьютерные технологии Физтех-школа Радиотехники и Компьютерных Технологий центр образовательных программ ФРКТ
курс:	4
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Аудиторных часов: 30 всего, в том числе:

лекции: 30 час.

семинары: 0 час.

лабораторные занятия: 0 час.

Самостоятельная работа: 30 час.

Подготовка к экзамену: 30 час.

Всего часов: 90, всего зач. ед.: 2

Количество контрольных работ, заданий: 2

Программу составил: А.А. Григорьев, канд. техн. наук, доцент, доцент

Программа обсуждена на заседании центра образовательных программ ФРКТ 08.11.2024

Освоение основ теории информации, принципов сжатия данных и помехоустойчивого кодирования.

1. Цели и задачи

Цель дисциплины

- ознакомить студентов с основными проблемами, которые возникают при хранении, передаче и использовании информации, а также привить навыки научного решения этих проблем.

Задачи дисциплины

- рассмотрение и анализ обобщенных типовых моделей систем передачи информации, их характеристик и параметров;
- построение моделей источников информации и задание основной характеристики — энтропии, вычисление энтропии для типовых источников, включая наиболее популярные источники марковского типа;
- построение различных моделей дискретных, непрерывных и полунепрерывных каналов связи и вычисление основной характеристики — пропускной способности;
- освоение основных алгебраических понятий теории полей Галуа;
- рассмотрение наиболее эффективных алгебраических кодов — Хэмминга, Боуза—Чоудхури, Рида—Соломона.

2. Перечень формируемых компетенций

Освоение дисциплины направлено на формирование следующих компетенций:

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области
	ПК-4.3 Способен обосновать причинно-следственные отношения используемых понятий и моделей

3. Перечень планируемых результатов обучения по дисциплине (модулю)

В результате освоения дисциплины обучающиеся должны знать:

- основные принципы теории передачи и хранения информации;
- существующие проблемы в области информатики.

уметь:

- применять методы теории информации на практике: современные методы сжатия данных, эффективные методы кодирования и декодирования;
- анализировать и определять характеристики систем хранения и передачи информации;
- пользоваться технической литературой научного и прикладного характера.

владеть:

- культурой постановки и моделирования научных задач;
- навыками грамотной обработки результатов опыта и сопоставления их с теоретическими и табличными данными;
- навыками самостоятельного моделирования;
- навыками освоения большого объема информации;
- навыками самостоятельной работы с учебной, научной и справочной литературой, ведения поиска и ориентирования в библиографии.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины (модуля) и трудоемкости по видам учебных занятий

№	Тема (раздел) дисциплины	Трудоемкость по видам учебных занятий, включая самостоятельную работу, час.			
		Лекции	Семинары	Лаборат. работы	Самост. работа
1	Информационные меры. Энтропия и количество информации	2			2
2	Схема передачи информации. Побуквенное кодирование и условие однозначного декодирования	2			2
3	Практические методы сжатия данных	2			2
4	Арифметическое кодирование	2			2
5	Каналы связи. Теоремы Шеннона	2			2
6	Стратегии декодирования	2			2
7	Непрерывные источники	2			2
8	Непрерывные каналы	2			2
9	Группы, кольца, конечные поля	2			2
10	Расширенный алгоритм Евклида	2			2
11	Блочные коды	2			2
12	Границы Синглтона, Плоткина, Варшамова	2			2
13	Циклические коды	2			2
14	Коды Боуза—Чоудхури	2			2
15	Коды Рида—Соломона	2			2
Итого часов		30			30
Подготовка к экзамену		30 час.			
Общая трудоёмкость		90 час., 2 зач.ед.			

4.2. Содержание дисциплины (модуля), структурированное по темам (разделам)

Семестр: 7 (Осенний)

1. Информационные меры. Энтропия и количество информации

Различные определения информации. Информация, содержащаяся в реализации случайной величины. Энтропия (мера неопределенности) случайной величины и ее свойства. Условная энтропия при условии, что задано значение другой случайной величины. Условная энтропия при условии, что задана другая случайная величина. Цепное равенство. Информационная дивергенция.

2. Схема передачи информации. Побуквенное кодирование и условие однозначного декодирования

Схема дискретной передачи информации. Роль каждого из блоков в процессе передачи информации. Побуквенное кодирование. Необходимое и достаточное условие однозначного декодирования (неравенство Мак-Миллана). Префиксные коды и кодовые деревья. Неравенство Крафта. Обратная и прямая теоремы Шеннона для побуквенного кодирования. Кодирование стационарных источников. Обратная и прямая теоремы Шеннона для стационарных источников.

3. Практические методы сжатия данных

Практические методы сжатия данных. Коды Шеннона и Фано. Оптимальный код Крафта. Алгоритмы сжатия и восстановления Лемпела—Зива LZW и LZ77. Коэффициенты сжатия. Примеры для каждого случая.

4. Арифметическое кодирование

Арифметическое кодирование. Подробное объяснение этого метода на нескольких примерах. Вычисление коэффициента сжатия. Восстановление сжатого сообщения.

5. Каналы связи. Теоремы Шеннона

Дискретные каналы связи без памяти. Матрица переходных вероятностей. Каналы, симметричные по входу. Каналы, симметричные по выходу. Пропускная способность. Лемма об обработке данных. Лемма оценивания Фано. Теоремы Шеннона для канала с шумом. Принципы блочного кодирования.

6. Стратегии декодирования

Стратегии декодирования. Разделение всего пространства выходных сигналов на области по принципу наименьшей вероятности ошибки. Вывод формулы для вероятности ошибки. Два подхода – без отказов и с отказами от декодирования.

7. Непрерывные источники

Непрерывные источники. Информационные характеристики непрерывных источников. Теорема Котельникова о представлении непрерывного сообщения набором отсчётов в дискретные моменты времени.

8. Непрерывные каналы

Непрерывные каналы. Формула Шеннона для пропускной способности канала с белым Гауссовым шумом. Формула для пропускной способности с цветным Гауссовым шумом.

9. Группы, кольца, конечные поля

Группы, кольца, конечные поля. Аддитивные группы. Мультипликативные группы. Конечные кольца. Простые поля. Пространства.

10. Расширенный алгоритм Евклида

Многочлены над полем. Расширенный алгоритм Евклида. Расширенные поля.

11. Блочные коды

Блочные коды. Общие понятия. Длина, мощность и скорость кода. Границы Синглтона, Плоткина, Варшамова—Гилберта.

12. Границы Синглтона, Плоткина, Варшамова

Линейные коды. Порождающая матрица. Кодирование. Систематические коды. Проверочная матрица. Синдромное декодирование. Расстояние линейного кода.

13. Циклические коды

Циклические коды. Алгебраические методы построения циклических кодов. Порождающий многочлен.

14. Коды Боуза—Чоудхури

Коды Боуза—Чоудхури—Хоквингема (БЧХ). Конструкция и параметры. Проверочная матрица кодов БЧХ. Декодирование кодов БЧХ. Исправление одиночных и двойных ошибок. Общий случай исправления ошибок с помощью симметричных многочленов. Локаторы ошибок и их вычисление.

15. Коды Рида—Соломона

Коды Рида—Соломона. Конструкция и параметры кодов. Дискретное преобразование Фурье (ДПФ). Циклическая свертка и произведение Адамара. Кодирование кодов Рида—Соломона с помощью ДПФ. Исправление ошибок с помощью обратного ДПФ. Пример: исправление одиночных и двойных ошибок.

5. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебная аудитория, оснащенная компьютером и мультимедийным оборудованием (проектор, звуковая система).

6. Перечень рекомендуемой литературы

Основная литература

1. Лекции по теории информации [Текст] : учеб. пособие для вузов / Э. М. Габидулин, Н. И. Пилипчук ; М-во образования и науки, Моск. физ.-техн. ин-т (гос. ун-т), Каф. радиотехники. — М. : Изд-во МФТИ, 2007. — 214 с.
2. Лекции по алгебраическому кодированию [Текст] : учеб. пособие для вузов / Э. М. Габидулин ; М-во образования и науки РФ, Моск. физ.-техн. ин-т (гос. ун-т). — М. : МФТИ, 2015. — 107 с.

Дополнительная литература

1. Введение в дискретную теорию информации и кодирования, Электрон. версия печ. публикации / С. И. Чечёта. — Москва, МЦНМО, 2011
2. Вероятность и статистика в примерах и задачах. Том 3. Теория информации и кодирования, Электрон. версия печ. публикации / М. Я. Кельберт, Ю. М. Сухов. — Москва, МЦНМО, 2016

7. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

Не используются

8. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень необходимого программного обеспечения и информационных справочных систем (при необходимости)

Adobe Reader или любая другая программа для чтения PDF файлов.

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Внимательно слушать и конспектировать лекции, самостоятельно решать контрольные задачи, которые лектор задаёт в конце каждой лекции, анализировать ошибки, приходить на консультации к преподавателю, решать задачи из домашних заданий по мере поступления лекционного материала, не откладывая на последние дни перед указанным в задании сроком сдачи, в дополнение к лекциям читать учебные пособия по данному предмету и разбирать решения типовых задач, которые в пособии приведены.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

по направлению:	Прикладные математика и физика
профиль подготовки:	Радиотехника и компьютерные технологии Физтех-школа Радиотехники и Компьютерных Технологий центр образовательных программ ФРКТ
курс:	<u>4</u>
квалификация:	бакалавр

Семестр, формы промежуточной аттестации: 7 (осенний) - Экзамен

Разработчик: А.А. Григорьев, канд. техн. наук, доцент, доцент

1. Компетенции, формируемые в процессе изучения дисциплины

Код и наименование компетенции	Индикаторы достижения компетенции
УК-1 Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Анализирует задачу, выделяя этапы ее решения, действия по решению задачи
	УК-1.2 Находит, критически анализирует и выбирает информацию, необходимую для решения поставленной задачи
	УК-1.3 Рассматривает различные варианты решения задачи, оценивает их преимущества и недостатки
	УК-1.4 Грамотно, логично, аргументированно формирует собственные суждения и оценки
ОПК-1 Способен применять фундаментальные знания, полученные в области физико-математических и (или) естественных наук, и использовать их в профессиональной деятельности	ОПК-1.1 Способен анализировать поставленную задачу, намечать пути ее решения
	ОПК-1.2 Способен строить математические модели, производить количественные расчеты и оценки
	ОПК-1.3 Способен определять границы применимости полученных результатов
ОПК-4 Способен осуществлять сбор и обработку научно-технической и (или) технологической информации для решения фундаментальных и прикладных задач	ОПК-4.1 Владеет методами научного поиска и интеллектуального анализа информации при решении задач профессиональной деятельности
	ОПК-4.4 Владеет навыками работы с компьютером и компьютерными сетями с целью получения, хранения и обработки научной (технической, технологической) информации
ПК-4 Способен критически оценивать применимость используемых методик и методов	ПК-4.1 Знает численные порядки величин, характерных для соответствующей профессиональной области
	ПК-4.3 Способен обосновать причинно-следственные отношения используемых понятий и моделей

2. Показатели оценивания компетенций

В результате изучения дисциплины «Теория информации» обучающийся должен:

знать:

- основные принципы теории передачи и хранения информации;
- существующие проблемы в области информатики.

уметь:

- применять методы теории информации на практике: современные методы сжатия данных, эффективные методы кодирования и декодирования;
- анализировать и определять характеристики систем хранения и передачи информации;
- пользоваться технической литературой научного и прикладного характера.

владеть:

- культурой постановки и моделирования научных задач;
- навыками грамотной обработки результатов опыта и сопоставления их с теоретическими и табличными данными;
- навыками самостоятельного моделирования;
- навыками освоения большого объема информации;
- навыками самостоятельной работы с учебной, научной и справочной литературой, ведения поиска и ориентирования в библиографии.

3. Перечень типовых (примерных) вопросов, заданий, тем для подготовки к текущему контролю

Проводится путем проведения коротких контрольных в конце каждой лекции и простых домашних заданий

4. Перечень типовых (примерных) вопросов и тем для проведения промежуточной аттестации обучающихся

Критерии оценивания

Оценка «отлично (10)» выставляется обучающемуся, если он правильно отвечает на все 10 вопросов, заданных ему на коллоквиуме.

Оценка «отлично (9)» выставляется обучающемуся, если он правильно отвечает на 9 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «отлично (8)» выставляется обучающемуся, если он правильно отвечает на 8 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «хорошо (7)» выставляется обучающемуся, если он правильно отвечает на 7 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «хорошо (6)» выставляется обучающемуся, если он правильно отвечает на 6 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «хорошо (5)» выставляется обучающемуся, если он правильно отвечает на 5 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «удовлетворительно (4)» выставляется обучающемуся, если он правильно отвечает на 4 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «удовлетворительно (3)» выставляется обучающемуся, если он правильно отвечает на 3 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «неудовлетворительно (2)» выставляется обучающемуся, если он правильно отвечает на 2 из 10 вопросов, заданных ему на коллоквиуме.

Оценка «неудовлетворительно (1)» выставляется обучающемуся, если он правильно отвечает на 1 из 10 заданных ему вопросов.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

3. Перечень типовых контрольных заданий, используемых для оценки знаний, умений, навыков

Перечень контрольных вопросов:

1. Задано совместное распределение двух случайных величин, принимающих два значения каждое. Найти маргинальные и условные распределения.
2. Считая известным совместное распределение двух случайных величин, записать определения энтропий и условных энтропий.
3. Входной алфавит состоит из 11 символов. Выходной алфавит состоит из трех символов 0,1,2. Построить разделимый код.
4. Заданы вероятности 6 входных сообщений. Построить оптимальный троичный код Хаффмена и дерево Хаффмена.
5. Задан входной блок длины 3 двоичного симметричного канала. Найти распределение выходного блока.
6. Случайные величины X, Y, Z образуют простую цепь Маркова. Доказать, что эти же случайные величины, взятые в обратном порядке Z, Y, X , также образуют простую цепь Маркова.
7. Проверить, что норма Хэмминга действительно норма.
8. $g_0(x)=x^4+x+1$. $g_1(x)=x^2$. Найти обратный к $g_1(x)$ элемент по модулю многочлена $g_0(x)$.
9. В кольце целых чисел по модулю q вес Ли целого числа i равен i , если $i < q$, и $q-i$ в противном случае. Доказать, что вес Ли является нормой.
10. Найти порождающую матрицу и минимальное кодовое расстояние кода с порождающим многочленом $1+x+x^2+x^4$.
11. Найти матрицу ДПФ, задаваемого корнем неприводимого двоичного многочлена степени 4. Найти ДПФ конкретного вектора.
12. Найти ранг некоторого вектора над полем $GF(64)$.

Студенты должны выполнить в течение семестра 2 задания. Все задания индивидуальные. Примеры типичных заданий:

Задание 1

А.

Пусть X, Y, Z --случайные величины, принимающие конечное число значений. Пусть $W = f(X,Z)$, где $f(*)$ -- произвольная функция. Доказать соотношения $H(XZW) = H(XZ)$; $H(W|Z) \leq H(X|Z)$; $I(XZW;Y) = I(XZ;Y)$.

При каких условиях имеет место знак равенства во втором соотношении?

В.

С помощью алгоритма LZ77 осуществить компрессию текста [B] [A] [D] [C] [C] [C] [B] [D] [D] [D][A] [A] [A] [C] [C] [A] [D] [B] [A] [D] [A] [B] [B] [D]. Найти коэффициент сжатия. Размер поискового буфера --- 8 символов, размер буфера необработанной части сообщения --- также 8 символов. Исходные символы кодируются 8 битами, позиция и длина в сжатом тексте кодируются 3 битами. Изначально поисковый буфер заполнен символами А.

С.

С помощью алгоритма LZW осуществить декомпрессию текста [C] [D] [A] [A] [D] [B] [A] [B] [257][C] [258] [B] [265] [267] [266] [D] [D] [C] [273] [A]. Найти

коэффициент сжатия, считая исходные символы 8-битовыми, а символы сжатого текста --- 9-битовыми. Примечание. Символ EOF не входит ни в исходные, ни в закодированные сообщения.

D.

Источник порождает двумерную случайную величину $\underline{U}=(X,Y)$, где X,Y - независимые двоичные случайные величины с распределениями $\{4/5, 1/5\}$ и $\{7/20, 13/20\}$. На входе приемника с вероятностью 0.45 регистрируется величина $Z=x + y$, а с вероятностью 0.55 регистрируется величина $Z=x + xy + 1$. Приемник выносит решения по правилу:

Если $Z=0$, то выносится решение $u=\{0 \& 0\}$ с вероятностью $1/5$.

Если $Z=1$, то выносится решение $u=\{0 \& 0\}$ с вероятностью $3/7$, $u=\{0 \& 1\}$ с вероятностью $3/7$, $u=\{1 \& 0\}$ с вероятностью $1/7$.

Если $Z=2$, то выносится решение $u=\{1 \& 0\}$ с вероятностью 1.

Если $Z=3$, то выносится решение $u=\{1 \& 1\}$ с вероятностью 1.

Найти взаимные информации $I(U;Z)$, $I(U;X)$, $I(U;Y)$ и проверить лемму об обработке. Найти оценку вероятности ошибки и точное значение вероятности ошибки.

E.

Для стационарного источника X_1, X_2, X_3, \dots , доказать существование предела $\lim_{n \rightarrow \infty} H(X_n | X_1, X_2, X_3, \dots, X_{n-1})$.

Пусть X_1, X_2, X_3, \dots - двоичный стационарный Марковский источник 1-го порядка такой, что $P_{X_i | X_{i-1}}(X_i=0 | X_{i-1}=0) = 1/10, P_{X_i | X_{i-1}}(X_i=1 | X_{i-1}=0) = 9/10, P_{X_i | X_{i-1}}(X_i=0 | X_{i-1}=1) = 1, P_{X_i | X_{i-1}}(X_i=1 | X_{i-1}=1) = 0$. Найти энтропию этого источника.

F.

Вход канала X является случайной величиной, равномерно распределенной в интервале $[0, 16]$. Выход канала равен $Z=X+Y$, где Y - не зависящая от X случайная величина с равномерным распределением в интервале $[0, 2]$. Найти распределение случайной величины Z , дифференциальные энтропии $H(Z)$, $H(X)$, $H(Y)$ и взаимную информацию $I(Z;X)$.

Задание 2

1. Найти все делители вида x^k-1 двучленов $x^{63}-1, x^{127}-1$ и $x^{255}-1$.
2. Пусть G_1 и G_2 - порождающие матрицы кодов (n_1, k, d_1) и (n_2, k, d_2) соответственно. Найдите параметры кода с порождающей матрицей $G = (G_1 | G_2)$.
3. Для линейного $(5,2)$ -кода с проверочной матрицей
$$H = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$
 найти порождающую матрицу G и множество лидеров смежных классов. Перечислить все исправляемые кодом ошибки. Найти результат декодирования блока $y = (1 \ 0 \ 0 \ 1 \ 0)$.
4. Рассмотрим код Рида-Соломона над $GF(8)$, исправляющий 2 ошибки. Укажите параметры кода. Найдите порождающий полином кода. Закодируйте сообщение $(1\alpha^2)$, α -- примитивный элемент $GF(8)$. Укажите параметры расширенного двоичного кода. Декодируйте сообщение $(0 \ 1\alpha^2\alpha^3 \ 1 \ 0)$.

Пример экзаменационных билетов (письменный экзамен):

1. Пусть X, Y, Z -- случайные величины, принимающие конечное число значений. Показать, что из того, что эти величины, взятые в обратном порядке, образуют цепь Маркова следует, что $H(Z|XY) = H(Z|Y)$.

2. С помощью алгоритма LZW осуществить декомпрессию текста [D] [C] [D] [B] [D] [260] [C] [A] [259][258] [257] [263] [B] [A] [A] [C] [262] [260] [A]. Найти коэффициент сжатия, считая исходные символы 8-битовыми, а символы сжатого текста --- 9-битовыми. Примечание. Символ EOF не входит ни в исходные, ни в закодированные сообщения.

3. Дискретный канал без памяти описывается матрицей переходных вероятностей

$$\begin{pmatrix} q & p \\ p & q \end{pmatrix}, \quad q = \frac{2}{3}, p = \frac{1}{3}.$$

Входной и выходной алфавиты состоят из символов 0, 1. Сообщения, подлежащие передаче, равны

$$\begin{array}{lll} \mathbf{x}_1 & = & (00000); \quad \mathbf{x}_2 = (11010); \\ \mathbf{x}_3 & = & (00111); \quad \mathbf{x}_4 = (11101). \end{array}$$

Найти оптимальные области декодирования для этих сообщений. Найти точные значения для вероятностей ошибок.

4. Проверочная матрица двоичного рангового кода длины $n=3$ с ранговым расстоянием $d=3$ равна

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha^4 \end{pmatrix}, \quad \text{где } \alpha - \text{корень многочлена } \varphi(x) = x^3 + x^2 + 1. \text{ Найти}$$

порождающую матрицу.

Сообщение передается как кодовый вектор \mathbf{v} . Декодировать сообщение, предполагая, что при передаче произошла ошибка \mathbf{e} ранга 1.

5. Найти наибольший общий делитель многочленов $r_1(x)$ и $r_2(x)$ в кольце $GF(2)[x]$, где

$$\begin{aligned} r_1(x) &= x^8 + x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1, \\ r_2(x) &= x^{14} + x^{13} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1. \end{aligned}$$

4. Критерии оценивания

Оценка	Баллы	Критерии
отлично	10	Выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины, проявляющему интерес к данной предметной области, продемонстрировавшему умение уверенно и творчески применять их на практике при решении конкретных задач, свободное и

		правильное обоснование принятых решений.
	9	Выставляется студенту, показавшему всесторонние, систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, свободное и правильное обоснование принятых решений.
	8	Выставляется студенту, показавшему систематизированные, глубокие знания учебной программы дисциплины и умение уверенно применять их на практике при решении конкретных задач, правильное обоснование принятых решений, с некоторыми недочетами.
хорошо	7	Выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но недостаточно грамотно обосновывает полученные результаты.
	6	Выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач некоторые неточности.
	5	Выставляется студенту, если он в основном знает материал, грамотно и по существу излагает его, умеет применять полученные знания на практике, но допускает в ответе или в решении задач достаточно большое количество неточностей.
удовлетворительно	4	Выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, недостаточно правильные формулировки базовых понятий, нарушения логической последовательности в изложении программного материала, но при этом он освоил основные разделы учебной программы, необходимые для дальнейшего обучения, и может применять полученные знания по образцу в стандартной ситуации.
	3	Выставляется студенту, показавшему фрагментарный, разрозненный характер знаний, допускающему ошибки в формулировках базовых понятий, нарушения логической последовательности в изложении программного материала, слабо владеет основными разделами учебной программы, необходимыми для дальнейшего обучения и с трудом применяет

		полученные знания даже в стандартной ситуации.
неудовлетворительно	2	Выставляется студенту, который не знает большей части основного содержания учебной программы дисциплины, допускает грубые ошибки в формулировках основных принципов и не умеет использовать полученные знания при решении типовых задач.
	1	Выставляется студенту, который не знает основного содержания учебной программы дисциплины, допускает грубейшие ошибки в формулировках базовых понятий дисциплины и вообще не имеет навыков решения типовых практических задач.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Экзамен проводится в письменной форме.

Время проведения письменного экзамена составляет четыре астрономических часа.

Во время проведения экзамена обучающиеся могут пользоваться программой дисциплины, любыми пособиями по теории информации и алгебраическому кодированию, а также простыми калькуляторами. Пользование гаджетами, содержащими телефон, фотокамеру и другие средства удаленной связи не разрешается.

Задачи по теории информации

1. Общие вопросы, принцип максимума энтропии

1.1. Слабый закон больших чисел

Пусть (X_1, \dots, X_N) – блок одинаковых независимых случайных величин со средним $m = E[X]$ и дисперсией

$$\sigma^2 = E[(X - m)^2].$$

Пусть

$$S_N = \frac{\sum_n x_n}{N}.$$

Покажите что

$$E[S_N] = m; \quad \sigma^2(S_N) = E[(S_N - m)^2] = \frac{\sigma^2}{N}.$$

Пусть

$$V_N = \frac{\sum_n x_n}{\sqrt{N}}.$$

Покажите что

$$E[V_N] = m\sqrt{N}; \quad \sigma^2(V_N) = E[(V_N - m\sqrt{N})^2] = \sigma^2.$$

1.2. К формуле Стирлинга

Получить нижнюю и верхнюю границы для факториала:

$$e^{7/8}[n^n e^{-n} \sqrt{n}] < n! < e[n^n e^{-n} \sqrt{n}].$$

Сопоставить ее с известной асимптотической оценкой Стирлинга: $n! \sim n^n e^{-n} \sqrt{2\pi n}$. ($e^{7/8} = 2.399 < \sqrt{2\pi} = 2.507 < e = 2.718$).

1.3. Оценки биномиальных распределений

Показать, что

$$\binom{n}{k} \simeq 2^{h(\frac{k}{n})},$$

где $h(x) = -x \log x - (1-x) \log(1-x)$. Получить оценку для вероятности $P_n(k)$ выпадения k орлов в серии из n бросаний симметричной монеты:

$$P_n(k) = 2^{-n} \binom{n}{k} \simeq 2^{-n(1-h(\frac{k}{n}))}$$

Пусть монета несимметрична и вероятность выпадения орла составляет p . Показать, что в этом случае

$$P_n(k) = \binom{n}{k} p^k (1-p)^{n-k} \simeq 2^{-nD(\frac{k}{n}, p)},$$

где

$$D\left(\frac{k}{n}, p\right) = \frac{k}{n} \log \frac{\frac{k}{n}}{p} + \frac{n-k}{n} \log \frac{\frac{n-k}{n}}{p}.$$

Показать, что наиболее вероятное значение $\frac{k}{n}$ равно p .

1.4. Принцип максимума энтропии

Пусть имеется J городских районов с вместимостями L_j , $\sum_j L_j = N$ и K организаций с вместимостями W_k , $\sum_k W_k = N$. Пусть x_{jk} – пассажиропоток – число людей, живущих в районе L_j и работающих в организации W_k . Показать, что число $M(x_{jk})$ вариантов расселения/трудоустройства N людей, дающих заданный набор пассажиропотоков, оценивается величиной

$$M \simeq 2^{H(P)},$$

где

$$H(P) = - \sum_{jk} p_{jk} \log p_{jk}; \quad p_{jk} = \frac{x_{jk}}{N}.$$

При каком условии на p_{jk} число вариантов максимально.

1.5. Принцип максимума энтропии

Пусть имеется J городских районов с вместимостями L_j , $\sum_j L_j = N$ и K организаций с вместимостями W_k , $\sum_k W_k = N$. Пусть x_{jk} – пассажиропоток – число людей, живущих в районе L_j и работающих в организации W_k . Применив принцип максимума энтропии

$$H(P) = - \sum_{jk} p_{jk} \log p_{jk}; \quad p_{jk} = \frac{x_{jk}}{N}$$

найти пассажиропотоки x_{jk} .

1.6. Неравенство Йенсена

Пусть $f(x)$ – выпуклая вниз функция, а $X = \{x\}$ – случайная величина со средним значением $E[x]$. Показать, что

$$E[f(x)] \geq f(E[x])$$

Решение

Значения выпуклой вниз функции лежат выше касательной, проведенной к ней в любой точке x_0 :

$$f(x) \geq f(x_0) + \alpha(x - x_0).$$

Имеем

$$E(f(x)) \geq E[f(x_0) + \alpha(x - x_0)] = f(x_0) + \alpha(E[x] - x_0).$$

Выбрав $x_0 = E[x]$, придем к

$$E(f(x)) \geq f(E(x)).$$

1.7. Применение неравенства Йенсена

Применив неравенство Йенсена, покажите, что центр масс системы из нанизанных на веревку шариков находится выше веревки, см. рисунок.

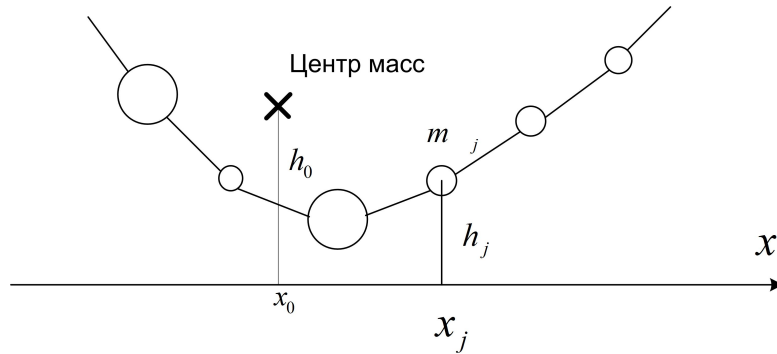


Рис. 1. Шарики на веревке

2. Свойства энтропийных функций

2.1. q -ичная энтропия

Найти формулу для энтропии $H_q(p)$ распределения на q -точках с $p_1 = 1 - p$ и $p_2 = \dots = p_q = \frac{p}{q-1}$. При каком значении параметра p достигается максимум $H_q(p)$ и каково значение этого максимума ?

2.2. Границы для энтропии

Пусть случайная величина принимает M значений. Покажите, что

$$0 \leq H(X) \leq \log M.$$

При каких условиях нижняя и верхняя границы достигаются.

2.3. Информационная дивергенция

Пусть $P = \{p(x)\}$ $Q = \{q(x)\}$ – два распределения вероятностей на одном и том же числе точек. Введем информационную дивергенцию между распределениями:

$$D(P||Q) = \sum_x p(x) \log \frac{p(x)}{q(x)}.$$

Покажите, что

$$D(P||Q) \geq 0.$$

При каком условии достигается равенство ?.

2.4. К информационной дивергенции

Пусть $P = \{p(x)\}$ $Q = \{q(x)\}$ – два распределения вероятностей на одном и том же числе точек. Рассмотрим функционал

$$F(P||Q) = \sum_x p(x) \log \frac{1}{q(x)}.$$

На каком распределении P достигается максимум $F(P||Q)$? На каком распределении Q достигается минимум $F(P||Q)$? Вывести отсюда границу

$$D(P||Q) = \sum_x p(x) \log \frac{p(x)}{q(x)} = F(P||Q) - H(P) \geq 0$$

для информационной дивергенции.

2.5. Аддитивность энтропии

Пусть во множестве значений случайной величины $X = \{x_1, x_2, \dots, x_k, x_{k+1} \dots x_n\}$ с распределением $P = \{p_1, p_2, \dots, p_k, p_{k+1}, \dots, p_n\}$ выделен агрегат $A = \{x_1, x_2, \dots, x_k\}$ с полной вероятностью $p_A = \sum_{j=1}^k p_j$ и распределением $P_A = \{\frac{p_1}{p_A}, \dots, \frac{p_k}{p_A}\}$ и его дополнение – агрегат \bar{A} с вероятностью $1 - p_A$ и распределением $P_{\bar{A}} = \{\frac{p_{k+1}}{1-p_A}, \dots, \frac{p_n}{1-p_A}\}$. Показать, что

$$H(X) = h(p_A) + p_A H(A) + (1 - p_A) H(\bar{A}).$$

2.6. Укорочение случайной величины

Пусть $X_n = \{x_1, x_2, \dots, x_n\}$ – случайная величина с распределением $P = (p_1 = p, p_2, \dots, p_n)$. Укоротим ее до случайной величины $X_{n-1} = \{x_2, \dots, x_n\}$ с распределением $P = (\frac{p_2}{1-p}, \dots, \frac{p_n}{1-p})$. Показать, что

$$H(X_n) = h(p) + (1 - p) H(X_{n-1}).$$

2.7. Разбиение множества значений

Пусть множество значений случайной величины $X = \{x\}$ с распределением $P = \{p(x)\}$ разбито на M непересекающихся подмножеств X_m – агрегатов с полными вероятностями $P_m = \sum_{x \in X_m} p(x)$ и распределениями $P_m = \{p_m(x) = \frac{p(x)}{P_m}\}$. Показать, что

$$H(X) = H(P_1, P_2, \dots, P_M) + \sum_{j=1}^M P_m H(X_m).$$

2.8. Оценки энтропийных функций

Пусть A, B, C – статистически независимые случайные величины с распределением $P_{ABC}(abc) = P_A(a)P_B(b)P_C(c)$ и энтропиями $H(A), H(B), H(C)$. Для случайных величин $X = (A, B)$ и $Y = (B, C)$ найти $H(XY), H(X), H(Y), H(X|Y), H(Y|X), I(X, Y), R(X, Y)$.

2.9. Вычисление энтропийных функций

Пусть X, Y независимые случайные величины с равновероятными значениями 0 и 1. Введем случайные величины $S = (X + Y) \bmod 2$ и $M = XY$. Найти

$$H(SM), H(S), H(M), H(S|M), H(M|S), I(S, M), R(S, M) = H(S|M) + H(M|S)$$

Проверить что

$$H(SM) = H(S) + H(M|S) \quad H(SM) = H(M) + H(S|M) \quad H(SM) = I(S, M) + R(S, M).$$

2.10. Добавление случайной величины

Покажите что энтропия совместного распределения больше энтропии маргинального:

$$H(XY) \geq H(X); \quad H(XY|Z) \geq H(X|Z).$$

При каких условиях достигаются равенства.

2.11. Добавление условия

Покажите что добавление условия снижает энтропию:

$$H(X|Y) \leq H(X); \quad H(X|YZ) \leq H(X|Z).$$

При каких условиях достигаются равенства.

2.12. Добавление случайной величины

Покажите, что

$$H(Y, Z) - H(Z) \geq H(X, Y, Z) - H(X, Y).$$

(Добавление X повышает разность между энтропиями совместного и маргинального распределений)

2.13. Мера взаимной случайности

Пусть $R(X, Y) = H(X|Y) + H(Y|X)$ – мера взаимной случайности между X и Y . Покажите, что

$$0 \leq R(X, Y) \leq H(X) + H(Y).$$

При каких условиях эти границы достигаются? Проверьте выполнение неравенства треугольника:

$$R(X, Y) \leq R(X, Z) + R(Z, Y).$$

2.14. К взаимной информации

Докажите эквивалентность представлений для взаимной информации

$$\begin{aligned} I(X, Y) &= H(X) - H(X|Y) = H(Y) - H(Y|X) = \\ &= H(X) + H(Y) - H(X, Y) = H(X, Y) - R(X, Y). \end{aligned}$$

Покажите, что $I(X, Y) \leq H(X)$, $I(X, Y) \leq H(Y)$. Когда эти границы достигаются.

2.15. К взаимной информации

Покажите, что совместная взаимна информация превышает маргинальную:

$$I(XY, Z) \geq I(X, Z),$$

$$I(XY, Z) \geq I(Y, Z).$$

При каких условиях достигаются равенства.

2.16. Шифрование

Пусть открытый текст – случайная величина M и ключ K преобразуются в шифротекст C так, что открытый текст однозначно восстанавливается по C и K – $H(M|KC) = 0$.

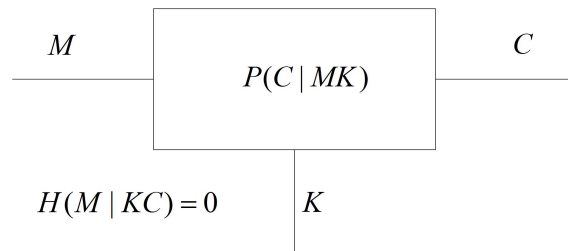


Рис. 2. Схема шифрования

Докажите границу

$$I(M, C) \geq H(M) - H(K).$$

3. Кодирование источника с потерями

3.1. Общая граница Чебышева

Пусть $\varphi(x)$ неотрицательна ($\varphi(x) \geq 0$) и такова, что из $x > a$ вытекает $\varphi(x) > \varphi(a)$. Покажите, что для любой случайной величины $X = \{x\}$ с матожиданием $E(\varphi(X))$ справедлива оценка:

$$P(x \geq a) \leq \frac{E(\varphi(X))}{\varphi(a)}.$$

3.2. Элементарная граница Чебышева

Пусть $X = \{x\}$ – неотрицательная случайная величина с матожиданием $E(X)$. Покажите, что

$$P(x \geq a) \leq \frac{E(X)}{a}.$$

Приведите пример ситуации, когда эта граница достигается.

3.3. Граница Чебышева для дисперсии

Пусть $X = \{x\}$ – случайная величина с матожиданием $E(X) = m$ и дисперсией $E[(X - m)^2] = \sigma^2$. Покажите что,

$$P(|x - m| \geq a) \leq \frac{\sigma^2}{a^2}.$$

3.4. Граница Чебышева для дисперсии суммы

Пусть $S_N = \sum_{k=1}^N x_k$ сумма одинаковых независимых случайных величин X с матожиданием $E[X] = m$ и дисперсией $E[(X - m)^2] = \sigma^2$. Покажите, что

$$P(|S_N - m| \geq a) \leq \frac{\sigma^2}{Na^2}.$$

Выведите отсюда следствие:

$$P\left(|S_N - m| \geq \frac{C}{\sqrt{N}}\right) \leq \frac{\sigma^2}{C^2}.$$

3.5. Граница Чебышева для суммы двоичных величин

Пусть $X = \{0, 1\}$ – двоичная случайная величина с $P(1) = p$, $P(0) = 1 - p$. Покажите, что для суммы независимых случайных величин этого рода справедлива оценка:

$$P\left(\left|\frac{\sum_{k=1}^N x_k}{N} - p\right| \geq a\right) = P(|S_N - p| \geq a) \leq \frac{p(1-p)}{Na^2}.$$

В частности,

$$P\left(|S_N - p| \geq \frac{C}{\sqrt{N}}\right) \leq \frac{p(1-p)}{C^2}.$$

3.6. Граница Чернова

Вывести границу Чернова:

$$P(x \geq a) \leq \min_{\mu \geq 0} (e^{-\mu a} E[e^{\mu x}]).$$

Показать, что для гауссовского распределения с плотностью $\varrho(x) = \frac{1}{\sqrt{2\pi}} e^{-\frac{x^2}{2}}$ граница Чернова дает:

$$P(x \geq a) \leq e^{-\frac{a^2}{2}}.$$

3.7. К конструкции множества типичных блоков

Пусть $X_N = (X_1, \dots, X_N)$ – блок независимых случайных величин с энтропией $H = H(X_k)$ каждая. Показать, что

$$P\left(\left|\frac{1}{N} \log \frac{1}{P(x_1 \dots x_n)} - H\right| \geq \beta\right) \leq \frac{\sigma^2}{N\beta^2},$$

где

$$\sigma^2 = E\left[\left(\log \frac{1}{P(x)} - H\right)^2\right]$$

3.8. Множество типичных блоков

Пусть $X_N = (X_1, \dots, X_N)$ – блок независимых случайных величин с энтропией $H = H(X_k)$ каждая. Показать, что в пространстве значений $X_N = \{\bar{x} = (x_1, \dots, x_N)\}$ можно выбрать подмножество типичных блоков

$$T_\beta(N) = \{\bar{x} : \left|\frac{1}{N} \log \frac{1}{P(\bar{x})} - H\right| \leq \beta\}$$

с вероятностями, «почти» равными 2^{-NH} в смысле

$$2^{-N(H+\beta)} \leq P(\bar{x}) \leq 2^{-N(H-\beta)}$$

и при этом

$$P(T_\beta(N)) \geq 1 - \frac{1}{N\beta^2} \rightarrow 1.$$

3.9. Оценки мощности множества типичных блоков

Пусть $X_N = (X_1, \dots, X_N)$ – блок независимых случайных величин с энтропией $H = H(X_k)$ каждая, $X^N = \{\bar{x} = (x_1, \dots, x_N)\}$ – пространство их значений,

$$T_\beta(N) = \{\bar{x} : \left|\frac{1}{N} \log \frac{1}{P(\bar{x})} - H\right| \leq \beta\}$$

множество типичных блоков в нем. Вывести границы для мощности множества $T_\beta(N)$:

$$\left(1 - \frac{\sigma^2}{N\beta^2}\right)2^{N(H-\beta)} \leq |T_\beta(N)| \leq 2^{N(H+\beta)}$$

3.10. Прямая теорема кодирования источника

Покажите, что во множестве $X^N = \{\bar{x} = (x_1, \dots, x_N)\}$ блоков независимых символов от источника с энтропией H можно выбрать подмножество S_δ с $P(S_\delta) \geq 1 - \delta$ мощности не превышающей $2^{N(H+\epsilon)}$, что обеспечит возможность кодирования с скоростью не более $N(H + \epsilon)$ битов на блок при вероятности ошибки не более δ .

3.11. Обращение теоремы кодирования источника

Пусть $X^N = \{\bar{x} = (x_1, \dots, x_N)\}$ множество блоков независимых символов от источника с энтропией H . Покажите, что при любом выборе подмножества S_δ мощности $|S_\delta| \leq 2^{N(H-\epsilon)}$ вероятностная мера этого множества $P(S_\delta)$ стремится к нулю при $N \rightarrow \infty$.

4. Кодирование источника без потерь

4.1. Неравенство Крафта

Пусть l_j – набор длин слов двоичного кода с однозначным декодированием. Докажите неравенство Крафта:

$$S = \sum_j 2^{-l_j} \leq 1.$$

4.2. Нижняя граница для длины двоичного префиксного кода

Пусть M символов источника с вероятностями p_m закодированы двоичным префиксным кодом с длинами слов l_m . Докажите нижнюю границу для средней длины кодового слова:

$$L = \sum_m p_m l_m \geq H,$$

где $H = -\sum_m p_m \log p_m$ – энтропия источника.

4.3. Нижняя граница для длины q -ичного префиксного кода

Пусть M символов источника с вероятностями p_m закодированы q -ичным префиксным кодом с длинами слов l_m . Докажите нижнюю границу для средней длины кодового слова:

$$L = \sum_m p_m l_m \geq \frac{H}{\log q},$$

где $H = -\sum_m p_m \log p_m$ – энтропия источника.

4.4. Верхняя граница для длины двоичного префиксного кода

Покажите, что для M -символьного источника с распределением вероятностей p_m и энтропией H существует двоичный префиксный код со средней длиной слова, удовлетворяющей границе:

$$L \leq \sum_m p_m l_m \leq H + 1.$$

4.5. Верхняя граница для длины q -ичного префиксного кода

Покажите, что для M -символьного источника с распределением вероятностей p_m и энтропией H существует q -ичный префиксный код со средней длиной слова, удовлетворяющей границе:

$$L \leq \sum_m p_m l_m \leq \frac{H}{\log q} + 1.$$

4.6. Уточненная верхняя граница для длины двоичного префиксного кода

Покажите, что для M -символьного источника с распределением вероятностей p_m и энтропией H существует двоичный префиксный код со средней длиной слова, удовлетворяющей границе:

$$L \leq \sum_m p_m l_m \leq H + \mu,$$

где $\mu = \sum_m p_m \mu_m$ среднее значение дополнения логарифма $\log \frac{1}{p_m}$ до ближайшего целого сверху: $l_m = \log \frac{1}{p_m} + \mu_m$, $0 \leq \mu_m < 1$.

4.7. Случай равенства средней длины и энтропии

Покажите, что если вероятности p_m всех M символов источника выражаются степенями двойки ($p_m = 2^{-l_m}$), то существует двоичный префиксный код со средней длиной, равной энтропии источника H : $L = \sum_m p_m l_m = H$. Покажите также, что набор l_m длин этого кода удовлетворяет равенству Крафта:

$$\sum_m 2^{-l_m} = 1.$$

4.8. Конструкция двоичного кода Хаффмана

Постройте оптимальный двоичный код Хаффмана для источника (a, b, c, d, e) с вероятностями символов $(0.25, 0.25, 0.2, 0.15, 0.15)$.

4.9. Конструкция двоичного кода Хаффмана

Постройте оптимальный код Хаффмана для кодирования восьми двоичных 3-блоков из независимых символов с вероятностью единицы $p = 1/3$. Оцените среднюю длину слова.

4.10. Конструкция двоичного кода Хаффмана

Постройте оптимальный код Хаффмана для кодирования восьми двоичных 3-блоков из независимых символов с вероятностью единицы $p = 1/4$. Оцените среднюю длину слова.

4.11. К двоичному коду Хаффмана

Обратившись к конструкции кода Хаффмана для кодирования восьми двоичных 3-блоков из независимых символов с вероятностью единицы p , покажите, что ни при каком значении p длина оптимального кода Хаффмана не может достигать 7.

4.12. К проблеме единственности кода Хаффмана

Для 4-символьного источника (a, b, c, d) с вероятностями $(\frac{1}{6}, \frac{1}{6}, \frac{1}{3}, \frac{1}{3})$ постройте все различные оптимальные коды Хаффмана. Проверьте факт совпадения их длин.

4.13. Полные коды Хаффмана

Префиксный код назовем полным, если в его дереве отсутствуют свободные листья, то есть, неравенство Крафта выполняется с равенством. При каких размерах M алфавита источника существуют полные q -ичные префиксные коды ?

4.14. Полные коды Хаффмана

Префиксный код назовем полным, если в его дереве отсутствуют свободные листья, то есть, неравенство Крафта выполняется с равенством. Покажите, что полный двоичный префиксный код существует при любом размере $M \geq 2$ алфавита источника.

4.15. Элементарный код Танстолла

Пусть двоичный префиксный код Танстолла со словами $(0, 10, 11)$ используется для преобразования потока равновероятных двоичных символов источника в троичный алфавит (A, B, C) . Найти энтропию на символ троичного выходного потока и сравнить ее со средним числом битов источника на троичный символ.

4.16. Код Танстолла

Построить двоичный префиксный код Танстолла для кодирования потока независимых двоичных символов с вероятностью единицы $p = 1/3$ на девять 2-блоков символов троичного алфавита (A, B, C) . Оценить среднее число битов на троичный 2-блок.

4.17. Арифметическое кодирование

Пусть арифметический кодер преобразует поток независимых двоичных символов с вероятностью нуля, равной $1/3$ в двоичный же выходной поток. На вход кодера уже поступили два символа – $(0, 0)$, $(0, 1)$, $(1, 0)$ или $(1, 1)$. Для каждого из этих четырех вариантов укажите: Какие символы уже могут быть посланы на выход? Какие символы следует добавить, чтобы оборвать процесс кодирования с возможностью восстановления переданной пары?

4.18. Арифметическое кодирование 2

Пусть на вход арифметического кодера, преобразующего поток независимых равновероятных троичных символов A, B, C в двоичный выходной поток поступили два символа. Для каждой из девяти возможных пар укажите двоичный код, посланный на выход кодера.

4.19. Двоичный кодер Лемпеля

Пусть двоичный кодер Лемпеля преобразует входной битовый поток в последовательность пар $(n)b$, где n – номер слова из текущего словаря кодовых блоков, а b – бит 0 или 1, которым входной блок отличается от блока из словаря. Вначале словарь пуст. По результату формирования каждой пары $(n)b$ в словарь заносится очередное слово. Слова нумеруются с единицы в порядке добавления.

Найти результат кодирования двоичного блока: 0 00 1 11 10 111 1111 000. Какой словарь будет составлен кодером?

4.20. Двоичный кодер Лемпеля

Пусть двоичный кодер Лемпеля преобразует входной битовый поток в последовательность пар $(n)b$, где n – номер слова из текущего словаря кодовых блоков, а b – бит 0 или 1, которым входной блок отличается от блока из словаря. Вначале словарь пуст – состоит только из пустого слова номер 0. По результату обработки каждой пары $(n)b$ в словарь заносится очередное слово. Слова нумеруются с единицы в порядке добавления.

Получен следующий поток пар:

$$(0)0|(1)0|(0)1|(3)1|(3)0|(4)1|(6)1|(2)0$$

Восстановить входной двоичный блок. Какой словарь будет составлен декодером?

5. Байесовское оценивание

5.1. Байесовская оценка вероятности

Пусть в последовательности из $n = 100$ бросаний несимметричной монеты с неизвестной вероятностью p выпадения орла выпало $k = 50$ орлов и $n - k = 50$ решек.

По результату наблюдения k построить байесовскую оценку плотности $\rho(p)$ апостериорного распределения параметра p , считая априорное распределение $\rho_0(p)$ равномерным. Найти матожидание $E[p]$ параметра p по плотности $\rho(p)$ – эмпирическую оценку вероятности p . Принять во внимание, что

$$\int_0^1 p^n (1-p)^m dp = \frac{n!m!}{(n+m+1)!}.$$

5.2. Лемма о совместительстве

Пусть на Ваш выбор предложено N мест работы с окладами S_n , $n = [1, N]$. Допускается частичная занятость с выплатой $q_n S_n$, пропорциональной доле q_n рабочего времени. Требуется распределить рабочее время (выбрать набор долей q_n с $\sum_n q_n = 1$) так, чтобы максимизировать суммарный доход

$$S = \sum_{n=1}^N q_n S_n.$$

5.3. Оценка максимума апостериорной вероятности

Пусть решения относительно значений символа $X = \{x\}$ выносятся по результату наблюдения значения $Y = \{y\}$ на выходе канала с матрицей условных вероятностей $P_{Y|X}(y|x) = P(y|x)$. Покажите, что решение по максимуму апостериорной вероятности

$$\tilde{x} = \operatorname{argmax}_x P_{X|Y}(x|y)$$

минимизирует среднюю вероятность ошибки

$$P_e = \sum_{\tilde{x} \neq x} P(x, \tilde{x}).$$

5.4. Оценка максимума правдоподобия

Пусть решения относительно значений символа $X = \{x\}$ выносятся по результату наблюдения значения $Y = \{y\}$ на выходе канала с матрицей условных вероятностей $P_{Y|X}(y|x) = P(y|x)$. Покажите, что при равномерном априорном распределении ($P(x) = \frac{1}{|X|}$) оценка по максимуму апостериорной вероятности

$$\tilde{x} = \operatorname{argmax}_x P_{X|Y}(x|y)$$

сводится к оценке по максимуму правдоподобия:

$$\tilde{x} = \operatorname{argmax}_x P_{Y|X}(y|x).$$

5.5. Сложение отношений правдоподобия

Пусть решения относительно значений двоичного символа $X = \{0, 1\}$ с вероятностью $P(x = 1) = q$ выносятся по результату наблюдения значения $Y = \{y\}$ на выходе канала с матрицей условных вероятностей $P_{Y|X}(y|x) = P(y|x)$. Покажите, что логарифм отношения правдоподобия для апостериорного распределения представляется суммой

$$\ln \frac{P(x = 0|y)}{P(x = 1|y)} = \ln \frac{P(y|x = 0)}{P(y|x = 1)} + \ln \frac{1-q}{q}.$$

5.6. Сложение отношений правдоподобия независимых наблюдений

Пусть решения относительно значений двоичного символа $X = \{0, 1\}$ с вероятностью $P(x = 1) = q$ выносятся по результатам двух независимых наблюдений значения $Y = \{y\}$ и $Z = \{z\}$ на выходах каналов с матрицами условных вероятностей $P_{Y|X}(y|x) = P(y|x)$ и $P_{Z|X}(z|x) = P(z|x)$. Покажите, что логарифм отношения правдоподобия для апостериорного распределения представляется суммой

$$\ln \frac{P(x = 0|yz)}{P(x = 1|yz)} = \ln \frac{P(y|x = 0)}{P(y|x = 1)} + \ln \frac{P(z|x = 0)}{P(z|x = 1)} + \ln \frac{1 - q}{q}$$

5.7. Отношение правдоподобия суммы

Пусть $z = x + y$ сумма по модулю два двух случайных битов с вероятностями единиц $P(x = 1) = p$, $P(y = 1) = q$ (логарифмами отношений правдоподобия $\lambda_x = \ln \frac{1-p}{p}$ и $\lambda_y = \ln \frac{1-q}{q}$). Покажите, что логарифм отношения правдоподобия λ_z для суммы z представляется в виде:

$$\lambda_z = \ln \frac{1 + \text{th}(\frac{\lambda_x}{2}) \text{th}(\frac{\lambda_y}{2})}{1 - \text{th}(\frac{\lambda_x}{2}) \text{th}(\frac{\lambda_y}{2})}.$$

5.8. Максимум апостериорной вероятности в двоичном случае

Пусть двоичная случайная величина X с вероятностью $P(x = 1) = q$ оценивается по двоичным значениям Y на выходе двоичного симметричного канала с вероятностью ошибки $p < 1/2$. Покажите, что оценивание x по максимуму апостериорной вероятности сводится к решению $\tilde{x} = y$ при $q > p$ и решению $\tilde{x} = 0$ при $q < p$. Каковы средние вероятности ошибок в одном и другом случае.

5.9. Отношение правдоподобия и двоичная случайная величина в гауссовском шуме

Пусть двоичная случайная величина $X = 0, 1$ наблюдается на выходе гауссовского канала с условными плотностями

$$\varrho(y|0) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-c)^2}{2\sigma^2}}; \quad \varrho(y|1) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y+c)^2}{2\sigma^2}};$$

Пусть

$$\lambda(y) = \ln \frac{\varrho(y|0)}{\varrho(y|1)}$$

– логарифм отношения правдоподобия. Покажите, что

$$\lambda(y) = \frac{2yc}{\sigma^2}, \quad \varrho(y|0) = \frac{1}{1 + e^{-\lambda}}; \quad \varrho(y|1) = \frac{1}{1 + e^{\lambda}};$$

5.10. Оценивание двоичной случайной величины в гауссовском шуме

Пусть двоичная случайная величина $X = 0, 1$ с $P(x = 1) = q$ наблюдается на выходе гауссовского канала с условными плотностями

$$\varrho(y|0) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y-c)^2}{2\sigma^2}}; \quad \varrho(y|1) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(y+c)^2}{2\sigma^2}};$$

Предложите правила оценивания X по наблюдению y по максимуму апостериорной вероятности и максимуму правдоподобия.

6. Пропускная способность, теоремы кодирования

6.1. Граница Фано

Пусть значения K -значной случайной величины X оцениваются по наблюдениям Y на выходе канала с матрицей условных вероятностей $P(Y|X)$. Покажите, что при любом алгоритме оценивания $Q(\tilde{X}|Y)$ вероятность ошибки

$$P_e = \sum_{x \neq \tilde{x}, y} P(x)P(y|x)Q(\tilde{x}|y)$$

удовлетворяет границе Фано:

$$h(P_e) + P_e \log_2(K-1) \geq H(X|\tilde{X}),$$

где $h(x) = -x \log x - (1-x) \log(1-x)$ - двоичная энтропия.

6.2. Двоичная граница Фано

Пусть значения двоичной случайной величины $X = 0, 1$ оцениваются по наблюдениям Y на выходе канала с матрицей условных вероятностей $P(Y|X)$. Покажите, что при любом алгоритме оценивания $Q(\tilde{X}, Y)$ вероятность ошибки

$$P_e = \sum_{x \neq \tilde{x}, y} P(x)P(y|x)Q(\tilde{x}|y)$$

удовлетворяет границе Фано:

$$h(P_e) \geq H(X|\tilde{X}),$$

где $h(x) = -x \log x - (1-x) \log(1-x)$ - двоичная энтропия.

6.3. К марковским цепям 1

Пусть случайные величины $X \rightarrow Y \rightarrow Z$ образуют цепь Маркова в том смысле, что

$$P(X, Y, Z) = P(X)P(Y|X)P(Z|Y).$$

Покажите что $H(Z|X, Y) = H(Z|Y)$, $H(X|Y, Z) = H(X|Y)$.

6.4. К марковским цепям 2

Пусть случайные величины $X \rightarrow Y \rightarrow Z$ образуют цепь Маркова в том смысле, что

$$P(X, Y, Z) = P(X)P(Y|X)P(Z|Y).$$

Покажите что $H(X, Z|Y) = H(X|Y) + H(Z|Y)$.

6.5. Лемма об обработке информации 1

Пусть случайные величины $X \rightarrow Y \rightarrow Z$ образуют цепь Маркова в том смысле, что

$$P(X, Y, Z) = P(X)P(Y|X)P(Z|Y).$$

Покажите что

$$I(X, Y) \geq I(X, Z).$$

6.6. Лемма об обработке информации 2

Пусть случайные величины $X \rightarrow Y \rightarrow Z$ образуют цепь маркова в том смысле, что

$$P(X, Y, Z) = P(X)P(Y|X)P(Z|Y).$$

Покажите что

$$I(Y, Z) \geq I(X, Z).$$

6.7. Лемма об обработке информации 3

Пусть случайные величины $U \rightarrow X \rightarrow Y \rightarrow V$ образуют цепь маркова в том смысле, что

$$P(U, X, Y, V) = P(U)P(X|U)P(Y|X)P(V|Y).$$

Покажите что

$$I(U, V) \leq I(X, Y).$$

6.8. Обращение теоремы кодирования

Пусть информационные двоичные K -блоки U преобразуются кодером в слова X длины L над некоторым алфавитом, передаются по каналу с матрицей условных вероятностей $P(Y|X)$ и пропускной способностью C битов на символ. Получающиеся на выходе L -блоки Y преобразуются декодером в выходные двоичные K -блоки V , см. рисунок.

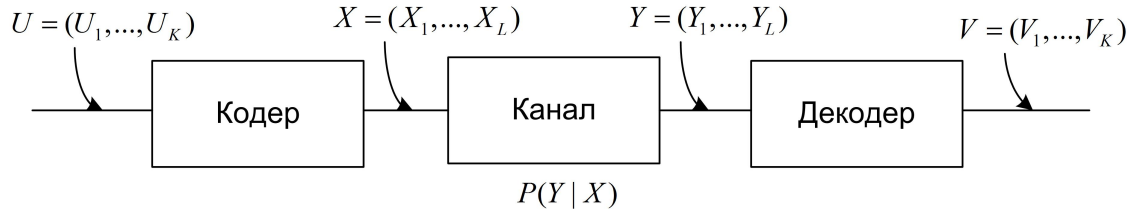


Рис. 3. Модель канала

Пусть $P_b(k) = P(U_k \neq V_k)$ – вероятность ошибки в k -ом бите, $P_b = \frac{1}{K} \sum_{k=1}^K P_b(k)$ – средняя вероятность ошибки на бит. Покажите, что

$$h(P_b) \geq 1 - \frac{C}{R},$$

где $R = \frac{K}{L}$ битов на использование канала, а $h(x)$ – двоичная энтропия. Постройте набросок графика этой границы.

6.9. Совместно-типичные блоки

Пусть совместное распределение вероятностей $P(X, Y)$ с энтропией $H(X, Y)$ определяет совместное распределение вероятностей N -блоков (X^N, Y^N)

$$X^N = \{x^N = (x_1, x_2, \dots, x_N); x_j \in X\} \quad Y^N = \{y^N = (y_1, y_2, \dots, y_N); y_j \in Y\}$$

по правилу

$$P(x^N, y^N) = \prod_j P(x_j, y_j).$$

Введем множество J_β типичных пар

$$J_\beta = \left\{ (x^N, y^N) : \left| \frac{1}{N} \log \frac{1}{P(x^N, y^N)} - H(X, Y) \right| \leq \beta \right\}$$

Показать, что для мощности множества J_β справедлива оценка

$$|J_\beta| \leq 2^{N(H(X, Y) + \beta)}$$

6.10. Граница для вероятности независимого выбора типичной пары

Пусть $P(X, Y)$ – совместное распределение вероятностей с энтропией $H(X, Y)$, а $P(X)$, $P(Y)$ – соответствующие маргинальные распределения с энтропиями $H(X)$, $H(Y)$. Рассмотрим порожденные ими распределения вероятностей N -блоков

$$X^N = \{x^N = (x_1, x_2, \dots, x_N); x_j \in X\} \quad Y^N = \{y^N = (y_1, y_2, \dots, y_N); y_j \in Y\} :$$

$$P(x^N, y^N) = \prod_j P(x_j, y_j); \quad P(x^N) = \prod_j P(x_j); \quad P(y^N) = \prod_j P(y_j).$$

Введем множество J_β совместно типичных пар:

$$J_\beta = \left\{ (x^N, y^N) : \left| \frac{1}{N} \log \frac{1}{P(x^N, y^N)} - H(X, Y) \right| \leq \beta \right\}$$

Пусть блоки x^N, y^N выбраны независимо согласно маргинальным распределениям $P(X^N)$, $P(Y^N)$. Показать, что вероятность того, что пара (x^N, y^N) окажется совместно типичной не превышает

$$P\left((x^N, y^N) \in J_\beta\right) \leq 2^{-N(I(X, Y) - 3\beta)},$$

где $I(X, Y)$ – взаимная информация между X и Y .

6.11. Лемма о выбрасывании

Пусть для некоторого канала предложен код $C = \{c^N = (c_1, \dots, c_N)\}$ длины N и мощности $M = |C|$ и схема декодирования, такие что средняя вероятность P_e ошибки на блок не превышает ϵ :

$$P_e = \sum_{c^N \neq \tilde{c}^N} P(c^N, \tilde{c}^N) < \epsilon.$$

Покажите, что выбросив не более половины из M кодовых слов можно добиться того, чтобы максимальная вероятность ошибки

$$P_{max} = \max_{c^N} \max_{\tilde{c}^N \neq c^N} P(c^N, \tilde{c}^N)$$

не превышала 2ϵ . К какой потере скорости кода приведет такое выбрасывание ?

6.12. Границы для вероятности ошибки на бит

Пусть кодер канала отображает равновероятные двоичные K -блоки на 2^K кодовых слов c . Декодер выносит решения \tilde{c} относительно переданных слов со средней вероятностью ошибки на слово, равной $P_e = \sum_{\tilde{c} \neq c} P(c, \tilde{c})$. Показать, что для средней вероятности ошибки в переданном P_b бите имеют место границы:

$$\frac{P_e}{K} \leq P_b \leq P_e.$$

6.13. Пропускная способность двоичного симметричного канала

Найти пропускную способность C двоичного симметричного канала с входом $X = 0, 1$, выходом $Y = 0, 1$ и вероятностями ошибки $P(y = 1|x = 0) = P(y = 0|x = 1) = p$. Построить график зависимости $C(p)$.
не зависит от y . Так что $C = 1 - h(p)$.

6.14. Пропускная способность q -ичного симметричного канала

Найти пропускную способность C q -ичного симметричного канала со входом $X = 1, 2, \dots, q$, выходом $Y = 1, 2, \dots, q$ и вероятностями $P(y = x) = 1 - p$ $P(y \neq x) = \frac{p}{q-1}$. Построить график зависимости $C(p)$. При каком значении p пропускная способность обращается в нуль?

6.15. Сумасшедшая пишущая машинка

Найти пропускную способность C q -ичной сумасшедшей пишущей машинки – канала с одинаковыми входным и выходным алфавитами $X = Y = (0, 1, \dots, q-1)$ и такого, что каждый данный символ s переходит в себя с вероятностью $1 - 2p$, а с равными вероятностями p отображается на соседние символы $(s-1) \bmod q$ и $(s+1) \bmod q$. Для частного случая $p = \frac{1}{3}$ и $q = 3^m$ предложить схему кодирования, достигающую пропускной способности.

6.16. Пропускная способность канала со стираниями

Найти пропускную способность C двоичного симметричного канала со стираниями: вход $X = 0, 1$, выход $Y = 0, 1, z$, $p(z|0) = p(z|1) = p$, $p(0|0) = p(1|1) = 1 - p$. Построить график зависимости $C(p)$.

6.17. (В БИЛЕТАХ) Пропускная способность Z -канала

Найти выражение для пропускной способности $C(p)$ Z -канала с двоичным входом $X = \{0, 1\}$, двоичным выходом $Y = \{0, 1\}$ и матрицей условных вероятностей $P(y = 0|x = 0) = 1$, $P(y = 1|x = 1) = p$, $P(y = 0|x = 1) = 1 - p$. Найти численное значение пропускной способности при $p = 1/2$. Каковы предельные значения $C(p)$ при $p \rightarrow 0$ и $p \rightarrow 1$.

6.18. Пропускная способность параллельного соединения независимых каналов - общий случай

Пусть два независимых канала со входами X_1, X_2 и выходами Y_1, Y_2 соединены параллельно, образуя векторный канал с матрицей условных вероятностей $P(Y_1 Y_2 | X_1 X_2) = P(Y_1 | X_1) P(Y_2 | X_2)$. Покажите, что пропускная способность параллельного соединения равна сумме пропускных способностей каналов.

6.19. Пропускная способность параллельного соединения независимых каналов

Найти пропускную способность параллельного соединения пары двоичных симметричных каналов с вероятностями искажения символа p и q – канала с векторным входом (X_1, X_2) , $X_1, X_2 = \{0, 1\}$, векторным выходом (Y_1, Y_2) , $Y_1, Y_2 = \{0, 1\}$ и вероятностями ошибки p в субканале $X_1 \rightarrow Y_1$ и q – в субканале $X_2 \rightarrow Y_2$.

6.20. Пропускная способность параллельных каналов с общим входом

Найти пропускную способность параллельного соединения пары двоичных симметричных каналов с объединенным входом $X = \{0, 1\}$, векторным выходом (Y_1, Y_2) $Y_1, Y_2 = \{0, 1\}$ и вероятностями p и q искажения в субканалах $X \rightarrow Y_1$ и $X \rightarrow Y_2$. Учесть, что пропускная способность достигается на равномерном распределении вероятностей входов. Какой окажется эта пропускная способность при $q = 0$, $q = 1/2$, $q = 1$.

6.21. Дифференциальная энтропия одномерной гауссовской плотности

Найти дифференциальную энтропию $H = \int_x g(x) \log \frac{1}{g(x)} dx$ гауссовской плотности вероятностей

$$g(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

с дисперсией σ^2 и средним значением μ . Показать, что

$$H = \int_x \rho(x) \log \frac{1}{g(x)} dx, \quad \text{если} \quad \int_x x^2 \rho(x) dx = \sigma^2.$$

6.22. Граница для информационной дивергенции

Пусть $p(x), g(x)$ – две плотности вероятностей. Показать, что

$$\int p(x) \log \frac{p(x)}{g(x)} dx \geq 0$$

с равенством при $p(x) = g(x)$.

6.23. Дифференциальная энтропия двумерной гауссовской плотности

Найти дифференциальную энтропию двумерной гауссовской плотности вероятностей

$$g(z) = \frac{1}{2\pi\sigma^2} e^{-\frac{|z|^2}{2\sigma^2}}, \quad z = x + jy, |z|^2 = x^2 + y^2,$$

с дисперсией $2\sigma^2$.

6.24. Экстремальность гауссовской плотности

Показать, что в классе плотностей вероятностей $\rho(x)$ с нулевым средним и заданной дисперсией $\sigma^2 = \int x^2 \rho(x) dx$ гауссовская плотность

$$g(x) = \frac{1}{\sqrt{2\pi}\sigma} e^{-\frac{x^2}{2\sigma^2}}$$

обладает максимальной энтропией.

6.25. Вероятность ошибки в двоичном гауссовском канале - максимум правдоподобия

Пусть бит (0 или 1) передается по каналу противоположными сигналами $x_0(t) = +cp(t)$, $x_1(t) = -cp(t)$, где $\int p^2(t)dt = 1$, а $E_c = c^2 = \int x_{0,1}^2(t)dt$ – энергия сигнала. Принятая реализация $y(t) = x_{0,1}(t) + n(t)$ отличается добавлением белого гауссовского шума $n(t)$. Согласованный фильтр приемника вычисляет проекцию $y(t)$ на опорный импульс $p(t)$. Результатом

$$y = \int y(t)p(t)dt = \pm c \int p^2(t)dt + \int n(t)p(t)dt = \pm c + w$$

оказывается отсчет y , равный $\pm c$ плюс случайная шумовая добавка w с дисперсией σ^2 . Решения относительно переданного бита выносятся по максимуму правдоподобия. Найти зависимость средней вероятности ошибочного P_e от отношения сигнал/шум $\mu^2 = \frac{c^2}{\sigma^2} = \frac{E_c}{\sigma^2}$.

6.26. Вероятность ошибки в двоичном гауссовском канале - максимум апостериорной вероятности

Пусть бит (0 или 1) передается по каналу противоположными сигналами $x_0(t) = +cp(t)$, $x_1(t) = -cp(t)$, где $\int p^2(t)dt = 1$, а $E_c = c^2 = \int x_{0,1}^2(t)dt$ – энергия сигнала. Принятая реализация $y(t) = x_{0,1}(t) + n(t)$ отличается добавлением белого гауссовского шума $n(t)$. Согласованный фильтр приемника вычисляет проекцию $y(t)$ на опорный импульс $p(t)$. Результатом

$$y = \int y(t)p(t)dt = \pm c \int p^2(t)dt + \int n(t)p(t)dt = \pm c + w$$

оказывается отсчет y , равный $\pm c$ плюс случайная шумовая добавка w с дисперсией σ^2 . Решения относительно переданного бита выносятся по максимуму апостериорной вероятности с априорной гипотезой о том, что $P(1) = q$. Найти зависимость средней вероятности ошибочного P_e от отношения сигнал/шум $\mu^2 = \frac{c^2}{\sigma^2} = \frac{E_c}{\sigma^2}$. Сколь малым должно быть q , чтобы демодулятор максимума апостериорной вероятности принимал равновероятные решения при передаче единицы.

6.27. Пропускная способность вещественного непрерывного гауссовского канала

Найти пропускную способность вещественного непрерывного гауссовского канала $y = x + w$ со средней энергией передаваемого вещественного символа $E[x^2] = c^2 = E$ и дисперсией шума $E[w^2] = \sigma^2 = N_0/2$. Выразить ее через энергию на бит $E_b = E/R$ и одностороннюю спектральную плотность шума N_0 . Показать, что надежная передача данных возможно только при $\frac{E_b}{N_0} > \ln 2$.

6.28. Пропускная способность комплексного непрерывного гауссовского канала

Найти пропускную способность непрерывного комплексного канала $y = x + w$ со средней энергией передаваемого вещественного символа $E[|x|^2] = c^2 = E$ и дисперсией шума $E[|w|^2] = 2\sigma^2 = N_0$. Выразить ее через энергию на бит $E_b = E/R$ и одностороннюю спектральную плотность шума N_0 . Показать, что надежная передача данных возможно только при $\frac{E_b}{N_0} > \ln 2$.

6.29. Параллельные гауссовские каналы

Найти пропускную способность системы из N параллельных вещественных непрерывных гауссовских каналов $y_n = x_n + w_n$, $n = 1..N$ со средней энергией передаваемого вещественного символа $E[x_n^2] = E_n$, дисперсией шума $E[w_n^2] = \sigma_n^2$. Какое распределение энергий между каналами с фиксированной полной энергией $E_0 = \sum_n E_n$ максимизирует эту пропускную способность? Как распределить энергию E_0 , когда все дисперсии одинаковы? Какой окажется при этом пропускная способность?

6.30. Вещественные и комплексные гауссовские каналы

Найти пропускную способность пары параллельных вещественных непрерывных гауссовских каналов $y_n = x_n + w_n$, $n = 1, 2$ со средней энергией передаваемого вещественного символа $E[x_n^2] = E_n$, дисперсией шума $E[w_n^2] = \sigma_n^2$. Какое распределение энергий между каналами при фиксированной полной энергии $E_0 = E_1 + E_2$ максимизирует эту пропускную способность? Как распределить энергию E_0 , когда обе дисперсии одинаковы? Показать, что при одинаковых дисперсиях пропускная способность параллельного соединения равна пропускной способности комплексного гауссовского канала.

6.31. К параллельному соединению каналов

Пусть имеется пара непрерывных вещественных гауссовских каналов с одинаковой дисперсией шума σ^2 . Для передачи символа выделена фиксированная энергия E . Что лучше в плане пропускной способности – вложить всю эту энергию в один канал, или распределить ее между двумя каналами поровну? Оценить выигрыш в пропускной способности. Как этот выигрыш зависит от отношения сигнал/шум $\mu^2 = \frac{E}{\sigma^2}$?

6.32. (В БИЛЕТАХ) Предельная пропускная способность системы параллельных каналов

Пусть для передачи символа выделена фиксированная энергия E_0 . Если всю ее вложить в один гауссовский канал с дисперсией шума $\sigma^2 = N_0/2$, получится пропускная способность $C = \frac{1}{2} \log(1 + \frac{2E_0}{N_0})$. Какой пропускной способности можно достичь, равномерно распределив энергию E_0 между $N \rightarrow \infty$ одинаковым гауссовскими каналами?

6.33. Предельная скорость передачи по радиоканалу 1

Пусть отношение сигнал/шум в комплексном радиоканале составляет $\mu^2 = \frac{E_s}{2\sigma^2} = \frac{E_s}{N_0} = 7$. Какова при этом предельная скорость R надежной передачи данных в битах на измерение? Какова реальная скорость передачи R_b в битах в секунду, если полоса канала составляет $F = 1\text{MHz}$. Каково при этом отношение $\frac{E_b}{N_0}$? Насколько оно удалено от шенноновского предела $\frac{E_b}{N_0} > \ln 2$?

6.34. Предельная скорость передачи по радиоканалу 2

Пусть отношение сигнал/шум в комплексном радиоканале $\mu^2 = \frac{E_s}{2\sigma^2} = \frac{E_s}{N_0}$ составляет 0.0718. Предельная скорость R надежной передачи данных в битах на измерение составляет при этом $R = \log(1 + \mu^2) = 0.1$. Какова реальная предельная скорость передачи R_b в битах в секунду, если полоса канала составляет $F = 1\text{MHz}$? Каково отношение $\frac{E_b}{N_0}$? Насколько оно удалено от шенноновского предела $\frac{E_b}{N_0} > \ln 2$?

6.35. Предельная скорость передачи по радиоканалу 3

Пусть отношение сигнал/шум в вещественном канале составляет $\mu^2 = \frac{E_s}{\sigma^2} = \frac{2E_s}{N_0} = 3$. Какова при этом предельная скорость R надежной передачи данных в битах на измерение. Какова реальная скорость передачи R_b в битах в секунду, если полоса канала составляет $F = 1\text{MHz}$. Каково при этом отношение $\frac{E_b}{N_0}$. Насколько оно удалено от шенноновского предела $\frac{E_b}{N_0} > \ln 2$

6.36. Предельная скорость передачи по радиоканалу 4

Пусть отношение сигнал/шум в вещественном канале составляет $\mu^2 = \frac{E_s}{\sigma^2} = \frac{2E_s}{N_0} = 1$. Какова при этом предельная скорость R надежной передачи данных в битах на измерение. Какова реальная скорость передачи R_b в битах в секунду, если полоса канала составляет $F = 1\text{MHz}$. Каково при этом отношение $\frac{E_b}{N_0}$. Насколько оно удалено от шенноновского предела $\frac{E_b}{N_0} > \ln 2$

6.37. Пропускная способность двоичного гауссовского канала - жесткие решения

Пусть бит (0 или 1) передается по каналу противоположными сигналами $x_0(t) = +cp(t)$, $x_1(t) = -cp(t)$, где $\int p^2(t)dt = 1$, а $E_c = c^2 = \int x_{0,1}^2(t)dt$ – энергия сигнала. Принятая реализация $y(t) = x_{0,1}(t) + n(t)$ отличается добавлением белого гауссовского шума $n(t)$. Согласованный фильтр приемника вычисляет проекцию $y(t)$ на опорный импульс $p(t)$. Результатом

$$y = \int y(t)p(t)dt = \pm c \int p^2(t)dt + \int n(t)p(t)dt = \pm c + w$$

оказывается отсчет y , равный $\pm c$ плюс случайная шумовая добавка w с дисперсией σ^2 . Жесткие решения относительно переданного бита выносятся по максимуму правдоподобия. Найти зависимость $C_b(\mu)$ пропускной способности этого канала отношения сигнал/шум $\mu^2 = \frac{c^2}{\sigma^2} = \frac{E_c}{\sigma^2}$.

6.38. Пропускная способность двоичного гауссовского канала - мягкие решения

Пусть бит (0 или 1) передается по каналу противоположными сигналами $x_0(t) = +cp(t)$, $x_1(t) = -cp(t)$, где $\int p^2(t)dt = 1$, а $E_c = c^2 = \int x_{0,1}^2(t)dt$ – энергия сигнала. Принятая реализация $y(t) = x_{0,1}(t) + n(t)$ отличается добавлением белого гауссовского шума $n(t)$. Согласованный фильтр приемника вычисляет проекцию $y(t)$ на опорный импульс $p(t)$. Результатом

$$y = \int y(t)p(t)dt = \pm c \int p^2(t)dt + \int n(t)p(t)dt = \pm c + w$$

оказывается отсчет y , равный $\pm c$ плюс случайная шумовая добавка w с дисперсией σ^2 . Решения относительно переданного бита по выносятся наблюдению y по максимуму правдоподобия. Найти выражение для $C_s(\mu)$ – зависимости пропускной способности этого канала от отношения сигнал/шум $\mu^2 = \frac{c^2}{\sigma^2} = \frac{E_c}{\sigma^2}$.

7. Нелинейные блочные коды

7.1. К расстоянию Хэмминга

Показать, что для расстояние Хэмминга $d_H(x, y)$ между двумя n -блоками над q -ичным алфавитом обладает свойствами метрики:

$$0 \leq d_H(x, y) \leq n,$$

$$d_H(x, y) = 0 \quad \Rightarrow \quad x = y,$$

$$d_H(x, y) \leq d_H(x, z) + d_H(z, y).$$

7.2. Число ошибок

Показать, что произвольный q -ичный $[n, k, d]_q$ -код, $k = \log M$ длины n , мощности M с минимальным расстоянием $d = 2t + 1$ гарантированно обнаруживает $2t$ ошибок и гарантированно исправляет t ошибок.

7.3. Число стираний

Показать, что произвольный q -ичный $[n, k, d]_q$ -код, $k = \log M$ длины n , мощности M с минимальным расстоянием d гарантированно обнаруживает $(d - 1)$ -ую ошибку и исправляет $d - 1$ стирание.

7.4. Число ошибок и стираний

Показать, что произвольный q -ичный $[n, k, d]_q$ -код, $k = \log M$ длины n , мощности M с минимальным расстоянием $d = 2t + e + 1$ гарантированно исправляет e стираний и t ошибок.

7.5. Объем шарового слоя

Пусть $V_q(n, t) = \{x : d_H(c, x) \leq t\}$ – хэмминговская сфера радиуса $t \leq n/2$. Показать, что

$$\frac{|V_q(n, t)| - |V_q(n, t - 1)|}{|V_q(n, t)|} \leq \frac{1}{1 + \frac{1}{q-1} \frac{t}{n-t+1}},$$

то есть, что при $n \rightarrow \infty$ в n -мерном хэмминговском пространстве объем шарового слоя единичной толщины асимптотически равен объему всей сферы.

7.6. Асимптотическая оценка объема сферы

Пусть $V_q(n, d) = \{x : d_H(c, x) \leq d\}$ – хэмминговская сфера радиуса t . Показать, при $n \rightarrow \infty$

$$|V_q(n, d)| \sim 2^{nh_q(\delta)} + o(\delta),$$

где $\delta = \frac{d}{n}$, а $h_q(\delta) = h(\delta) + \delta \log(q - 1)$.

7.7. Граница Варшимова-Гильберта

Доказать существование q -ичного $[n, k, d]_q$ -кода с мощностью M , ($k = \log M$), удовлетворяющей границе

$$M \geq \frac{q^n}{|V_q(n, d-1)|}.$$

Вывести отсюда асимптотическую границу

$$R \geq \log q - h_q(\delta),$$

где $R = \frac{\log M}{n} = \frac{k}{n}$, $\delta = \frac{d}{n}$, а $h_q(\delta) = h(\delta) + \delta \log(q-1)$. Построить график зависимости $R(\delta)$ для $q = 2$.

7.8. Декодирование до границы минимального расстояния

Покажите, что при декодировании двоичных кодов до границы минимального расстояния (то есть с исправлением на более $t = \frac{d-1}{2}$ ошибок) пропускная способность двоичного симметричного канала не достигается.

7.9. Верхняя граница Хэмминга

Доказать, что мощность M , ($k = \log M$) q -ичного $[n, k, d]_q$ -кода с минимальным расстоянием $d = 2t + 1$ не превышает границы Хэмминга

$$M \leq \frac{q^n}{|V_q(n, t)|}.$$

$$R \leq \log q - h_q(\delta/2),$$

где $R = \frac{\log M}{n} = \frac{k}{n}$, $\delta = \frac{d}{n}$, а $h_q(\delta) = h(\delta) + \delta \log(q-1)$. Построить график зависимости $R(\delta)$ для $q = 2$. Привести пример совершенного двоичного кода, для которого граница Хэмминга выполняется с равенством.

7.10. Верхняя граница Синглтона

Доказать, что мощность M , ($k = \log M$) q -ичного $[n, k, d]_q$ -кода с минимальным расстоянием $d = 2t + 1$ не превышает границы Синглтона:

$$M \leq q^{(n-d+1)}.$$

Построить асимптотическую границу

$$\frac{R}{\log q} \leq (1 - \delta),$$

где $R = \frac{\log M}{n}$, $\delta = \frac{d}{n}$. Привести пример МДР-кода, лежащего на границе Синглтона.

8. Элементы алгебры

8.1. Подгруппы и смежные классы. Составная циклическая группа.

Найти подгруппы аддитивной группы кольца Z_{10} целых чисел по модулю 10. Перечислить элементы их смежных классов. Охарактеризовать фактор группы. Показать, что декартово произведение подгрупп эквивалентно группе Z_{10} .

8.2. Подгруппы и смежные классы. Примарная циклическая группа.

Найти подгруппы аддитивной группы кольца Z_{16} целых чисел по модулю 16. Перечислить элементы их смежных классов. Охарактеризовать фактор группы. Показать, что в группе существует цепочка вложенных подгрупп с фактор-группами Z_2 , в то время как сама она не изоморфна декартову произведению четырех групп Z_2 .

8.3. Диадическая группа

Перечислить все подгруппы в группе $Z_2 \times Z_2 \times Z_2$ – декартовом произведении трех групп Z_2 целых чисел по модулю 2. Для каждой из подгрупп найти смежные классы.

8.4. Расширенный алгоритм Евклида

Найти представление равного единице наибольшего общего делителя чисел 5 и 3 в виде линейной формы $1 = \alpha 5 + \beta 3$ с целыми коэффициентами $\alpha, \beta \in Z$.

8.5. Простые поля

Покажите, что кольцо Z_p целых чисел по простому модулю p является полем. Почему никакое кольцо Z_{nm} по составному модулю полем не является?

8.6. Характеристика поля

Покажите, что в любом поле F существует простое подполе F' эквивалентное либо одному из полей $Z_p = F_p$ (характеристика p), либо полю рациональных чисел (характеристика 0).

8.7. Автоморфизм Фробениуса

Покажите, что в любом поле F характеристики p отображение $\varphi(x) = x^p$ является автоморфизмом – отображением поля в себя, сохраняющим операции сложения и умножения.

8.8. Основная теорема алгебры

Покажите, что многочлен $h(x) = x^n + h_{n-1}x^{n-1} + \dots + h_1x + h_0$ степени n не может иметь более n корней ни в каком поле.

8.9. Сопряженные корни

Пусть $h(x) = x^n + h_{n-1}x^{n-1} + \dots + h_1x + h_0$ – многочлен с коэффициентами из простого подполя F_p некоторого поля F характеристики p . Пусть $\alpha \in F$ – корень $h(x)$: $h(\alpha) = 0$. Покажите, что все сопряженные про Фробениусу элементы $\varphi(\alpha) = \alpha^p$, $\varphi(\varphi(\alpha)) = (\alpha^p)^p = \alpha^{p^2}$, $\alpha^{p^3} \dots$ также являются его корнями. Покажите, что таких элементов не может быть больше n .

8.10. Орбиты сопряженных элементов

Пусть $\alpha \in F$ – некоторый элемент поля F характеристики p . Рассмотрим множество (орбиту) сопряженных с ним по Фробениусу элементов

$$\{\alpha, \alpha^p, \alpha^{p^2}, \alpha^{p^3}, \dots, \alpha^{p^{n-1}}, \alpha^{p^n} = \alpha\}.$$

Пусть

$$h(x) = \prod_{k=0}^{n-1} (x - \alpha^{p^k})$$

многочлен степени n , имеющий своими корнями все элементы орбиты. Покажите, что все коэффициенты многочлена $h(x)$ принадлежат простому подполю $F_p \in F$.

8.11. Линейное пространство

Покажите, что мощность (число элементов) n -мерного линейного пространства $L_n(F_q)$ составляет над конечным полем F_q из q элементов составляет q^n . Какова мощность одномерного подпространства (прямой), подпространства размерности k , гиперплоскости (подпространства размерности $n-1$).

8.12. Отображения линейных пространств

Пусть $\varphi : L_n \rightarrow L_m$ – линейное отображение (морфизм) пространства $L_n(F_q)$ в $L_m(F_q)$. Рассмотрим его ядро

$$\text{Ker}(\varphi) = \{x \in L_n : \varphi(x) = 0\},$$

и образ

$$\text{Im}(\varphi) = \{y \in L_m : \exists x \in L_n \quad y = \varphi(x)\}.$$

Покажите, что $\text{Ker}(\varphi)$ и $\text{Im}(\varphi)$ – линейные подпространства в L_n и L_m . Покажите, что

$$\frac{\dim L_n}{\dim \text{Ker}(\varphi)} = \dim \text{Im}(\varphi),$$

где \dim – размерность пространства.

8.13. Линейные формы

Пусть $\varphi : L_n \rightarrow F_q$ – линейное отображение пространства $L_n(F_q)$ в поле F_q . Покажите, что его ядро

$$\text{Ker}(\varphi) = \{x \in L_n : \varphi(x) = 0\},$$

является гиперплоскостью – подпространством размерности $n-1$. Сколько элементов в фактор-пространстве $L_n/\text{Ker}(\varphi)$, каковы их образы при отображении φ . Какие линейные отображения определяют одну и ту же гиперплоскость.

8.14. Двойственное пространство

Пусть $L_n(F_q)$ – линейное пространство размерности n над полем F_q . Покажите, что множество линейных отображений $\varphi : L_n \rightarrow F_q$ образует (двойственное) линейное пространство $L_n^*(F_q)$. Какова его размерность? Докажите, что для любого базиса (e_1, \dots, e_n) L_n можно построить двойственный базис (f_1, \dots, f_n) в L_n^* , такой что $f_j(e_k) = \delta_{j,k}$.

8.15. Линейные отображения и матрицы

Покажите, что любое линейное отображение $\varphi : L_n \rightarrow L_m$ линейных пространств над полем F_q можно представить (m, n) матрицей с элементами из F_q . Каков класс матриц, задающих одно и то же линейное отображение.

8.16. Линейные отображения и матрицы

Покажите, что любое линейное отображение $\varphi : L_n \rightarrow L_m$ линейных пространств над полем F_q можно представить (m, n) -матрицей с элементами из F_q . Каким свойством должна обладать эта матрица, чтобы отображение φ было наложением (отображением на), таким что $\dim \text{Im}(\varphi) = m$.

9. Линейные блочные коды

9.1. Эквивалентные коды, порождающая матрица

Линейные коды назовем эквивалентными, если один получается из другого перестановкой слов, перестановкой координат слов и покоординатным умножением всех слов на фиксированный блок (s_1, s_2, \dots, s_n) с ненулевыми координатами: $(c_1, c_2, \dots, c_n) \rightarrow (s_1 c_1, s_2 c_2, \dots, s_n c_n)$. Покажите, что эквивалентные коды обладают одинаковыми $[n, k, d]_q$ параметрами. Какие преобразования порождающей матрицы дают эквивалентные коды. Покажите, что среди эквивалентных кодов всегда существует код с порождающей матрицей в систематической форме.

9.2. Эквивалентные коды, проверочная матрица

Линейные коды назовем эквивалентными, если один получается из другого перестановкой слов, перестановкой координат слов и покоординатным умножением всех слов на фиксированный блок (s_1, s_2, \dots, s_n) с ненулевыми координатами: $(c_1, c_2, \dots, c_n) \rightarrow (s_1 c_1, s_2 c_2, \dots, s_n c_n)$. Покажите, что эквивалентные коды обладают одинаковыми $[n, k, d]_q$ параметрами. Какие преобразования проверочной матрицы дают эквивалентные коды. Покажите, что среди эквивалентных кодов всегда существует код с проверочной матрицей в систематической форме.

9.3. Порождающая-проверочная матрицы

Пусть задана (n, k) порождающая матрица G в систематической форме. Предложить алгоритм построения систематической проверочной H матрицы этого кода.

9.4. Линейные коды на границе Синглтона - проверочная матрица

Покажите, что если параметры линейного $[n, k, d]_q$ -кода лежат на границе Синглтона (МДР-код с $d = n - k + 1$), то все $(n - k, n - k)$ квадратные подматрицы его $(n - k, n)$ проверочной матрицы невырождены. Предложите эффективный алгоритм исправления $d - 1 = n - k$ стираний МДР-кодом.

9.5. Линейные коды на границе Синглтона - проверочная матрица

Покажите, что если параметры линейного $[n, k, d]_q$ -кода лежат на границе Синглтона (МДР-код с $d = n - k + 1$), то все (k, k) квадратные подматрицы его (n, k) порождающей матрицы невырождены, то есть никакое ненулевое кодовое слово не может принимать нулевые значения в произвольном образом заданных k -позициях. В частности, безошибочный прием любых k координат вполне определяет кодовое слово в целом. Предложите алгоритм исправления $d - 1 = n - k$ стираний по проверочной матрице МДР-кода.

9.6. Оценка минимального расстояния случайного линейного кода

Покажите, что минимальное расстояние d случайного линейного $[n, k, d]_2$ кода лежит на границе Варшамова-Гильберта:

$$h\left(\frac{d}{n}\right) \simeq 1 - R = 1 - \frac{k}{n}.$$

9.7. Код повторения

Покажите, что $[n, k, d]_2$ код повторения с параметрами $[n = 2t + 1, 1, 2t + 1]_2$ совершенен. Какова скорость этого кода, каково число гарантированно исправляемых ошибок? Как выглядят его порождающая матрица?

9.8. Код Хэмминга

Покажите, что $[n, k, d]_2$ код Хэмминга с параметрами $[n = 2^m - 1, n - m, 3]_2$ совершенен. Какова скорость этого кода, каково число гарантированно исправляемых ошибок? Как выглядят его порождающая матрица?

9.9. Выкалывание

Пусть имеется линейный $[n, k, d]_q$ -код с $d \geq 2$. Построить на его основе выколотый код с параметрами $[n - 1, k, d - 1]_q$.

9.10. Укорочение

Пусть имеется линейный $[n, k, d]_q$ -код. Построить на его основе укороченный код с параметрами $[n - 1, k - 1, d]_q$.