МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ, СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ордена Трудового Красного Знамени

Федеральное Государственное бюджетное образовательное учреждение высшего образования

«Московский Технический Университет Связи и Информатики»

Кафедра «Информационная безопасность»

Дисциплина «Интеллектуальные технологии   
информационной безопасности»

Лабораторные работы

Выполнил студент

группы М102201(70)

Пальчун Д.А.

Преподаватель:

Раковский Д.И.

**Содержание**

[**Лабораторная работа 1. «Статистический анализ наборов данных».**](#_heading=h.sdrpzjwepoja) **2**

[**Лабораторная работа 2. «Исследование однослойных нейронных сетей на примере моделирования булевых выражений».**](#_heading=h.omejpectj0ii) **10**

[**Лабораторная работа 3. Оценка результатов классификации при помощи метрик TP, FP, FN, TN, Accuracy, Precision, AUC, F-мера, матрица ошибок и лабораторная работа 4: «Алгоритмы машинного обучения с учителем для решения задач классификации».**](#_heading=h.3znysh7) **11**

[**Лабораторная работа 8. Снижение размерности входных данных на примере алгоритмов PCA, SVD**](#_heading=h.6rvl8mpmqecl) **15**

# Лабораторная работа 1. «Статистический анализ наборов данных»

**Цель работы:** усвоить основные способы статистической оценки данных перед их обработкой интеллектуальными алгоритмами анализа данных.

**Теоретическая часть**

Говорят, что компьютерная программа обучается на опыте E относительно некоторого класса задач T и меры качества P, если ее качество на задачах, принадлежащих T, измеренное в соответствии с P, улучшается с увеличением опыта E [1].

Таким образом, существует много видов машинного обучения, зависящих от природы задачи T, решению которой необходимо обучить систему, природы меры качества P, используемой для оценки работы системы, и природы обучающего сигнала, или опыта E, на котором обучается система [2].

Перед применением инструментов машинного обучения (МО) к какой-либо задаче, необходимо провести разведочных анализ данных с целью выяснения наиболее очевидных закономерностей в наборе данных. Для первичного анализа данных потребуется знание основ математического анализа, математической статистики, теории информации, дискретной математики

**График парных отношений.**

Для табличных данных с небольшим числом признаков часто строят график парных отношений, на котором каждый подграф (i, j) содержит диаграмму рассеяния величин i и j, а диагональные элементы (i, i) показывают маргинальное распределение величины i. Обобщенная запись маргинального распределения для случайной величины записывается как:

| 𝑝(𝑋 = 𝑥) = ∑𝑝(𝑋 = 𝑥, 𝑌 = 𝑦) | (1.1) |
| --- | --- |

где суммирование производится по всем возможным значениям Y.

Ранее в русскоязычной литературе термин marginal distribution переводился как «частное распределение», сейчас более употребителен перевод «маргинальное распределение»); дополнительно все графики могут быть маркированы цветом, ассоциированным с меткой класса. Визуализация графика парных отношений приведена на рис. 1.1.

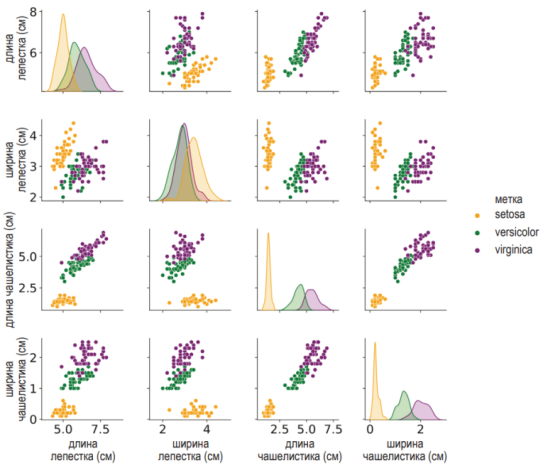


Рисунок 1.1 Визуализация построения попарной диаграммы рассеяния на наборе Iris.

**Частотная гистограмма распределения классов.**

Частотное распределение представляет собой столбчатую диаграмму для отображения частотности попадания наблюдаемых значений в определенные интервалы или классы. Пример построенной частотной гистограммы распределения классов для бинарного случая приведен на рис. 1.2.

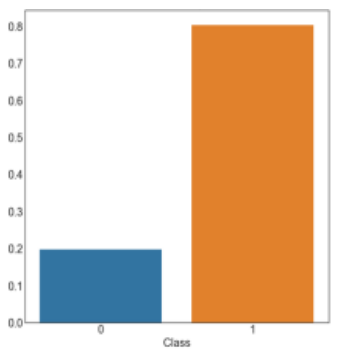


Рисунок 1.2 Визуализация построения частотной гистограммы распределения классов.

**Корреляционная диаграмма.**

Для оценки значимости и оценки количества атрибутов используется построение корреляционной диаграммы на основе оценок коэффициентов корреляции атрибутов методами Пирсона, Кендалла и Спирмена. Коэффициент корреляции Пирсона характеризует существование линейной зависимости между значениями двух выборок одинаковой размерности.

Ранговые корреляции Спирмена и Кенделла отличаются различной интерпретацией. Так если коэффициент корреляции Спирмена может рассматриваться как прямой аналог коэффициента корреляции Пирсона, вычисленный по рангам, то при вычислении коэффициента корреляции Кендалла проверяется наличие различий между вероятностями порядка (ранга) расположения наблюдаемых данных. Следует отметить, что в корреляции методом Спирмена инверсиям придаются дополнительные веса. В результате коэффициент корреляции Спирмена значительнее реагирует на несогласие выборок, чем коэффициент корреляции Кендалла. В большинстве случаев |ρ| > |τ|. Пример построения трех корреляционных диаграмм для одного и того же набора данных приведен на рис. 1.3.

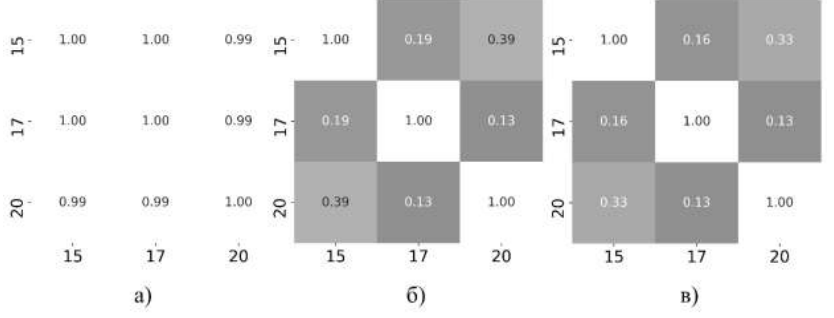


Рисунок 1.3 Визуализация построения корреляционной диаграммы. Корреляционные диаграммы, выполненные для атрибутов №15, №17, №20 методом: а) Пирсона; б) Спирмена; в) Кендалла.

**Ход работы:**

Dataset: IMDB Video Games (<https://www.kaggle.com/datasets/muhammadadiltalay/imdb-video-games>)

# 

Рисунок 1.3 Dataset: IMDB Video Games

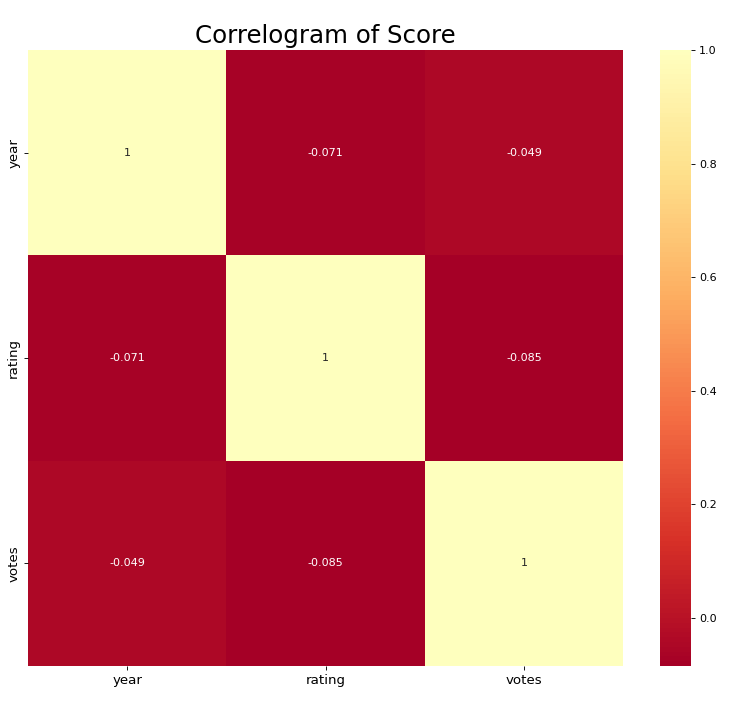


Рисунок 1.4 Корреляционная диаграмма

В данном наборе данных (рисунок 1.4) очевидно, что между годами выхода игр, количеством голосов на игру и рейтингом вышедших игр нет корреляции. Таким образом, мы можем утверждать, что заявление, которое не подкрепляется дополнительными аргументами, о том, что раньше игры делали лучше - ложно, также ложно утверждение, что нужно ориентироваться на качество игры исходя только из того, что за нее обращает внимание большое количество людей.

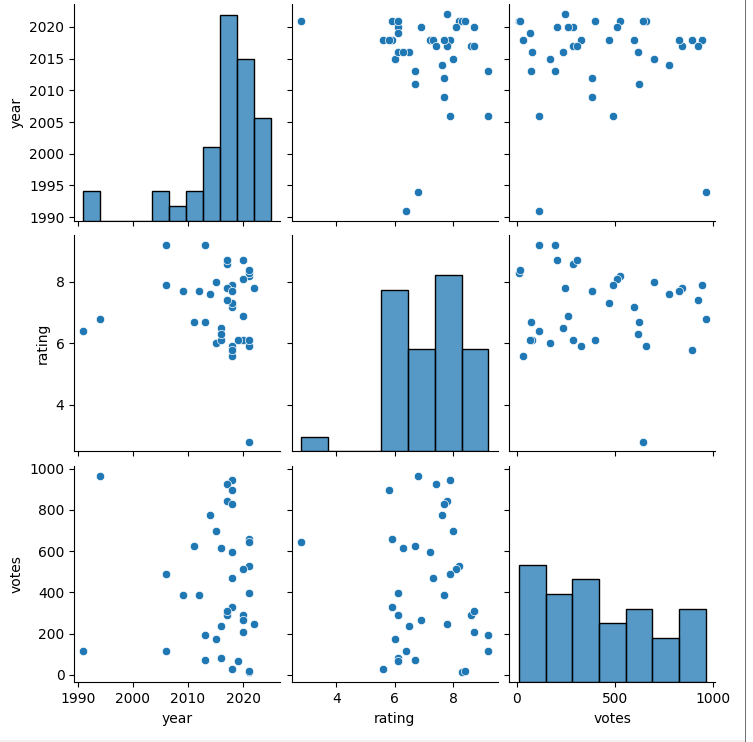


Рисунок 1.5 График парных отношений

На графике парных отношений (рисунок 1.5) мы можем наблюдать, что с 2015 года количество голосующих за рейтинг игр увеличилось, также видна тенденция того, что с течением лет количество оценок игр увеличивается, но высота оценки уменьшается. Также, видно, что люди неохотно ставят играм низкие оценки.

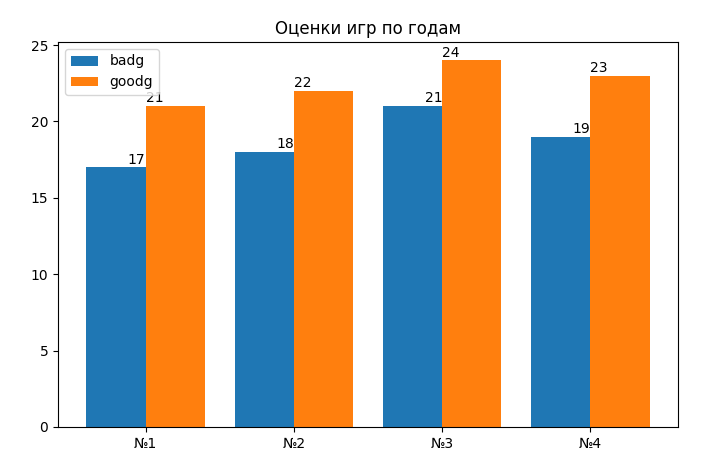


Рисунок 1.6 Частотная гистограмма распределения классов. №1 – Общий результат трех лет. №2 – Результат за 2013. №3 – результаты за 2018. №4 – результаты за 2020.

На рисунке 1.6 продемонстрирована гистограмма общего результата оценок за 3 года. Здесь мы видим, что количество игр, набравших более 7 баллов с течением лет увеличивается, как и общее количество игр.

**Вывод**

По результатам выполнения лабораторной работы были усвоены основные способы статистической оценки данных. Был проведен разведочный анализ данных с целью выяснения наиболее очевидных закономерностей в наборе данных. Проанализированы: график парных отношений, частотная гистограмма распределения классов и корреляционная диаграмма.

# Лабораторная работа 2. «Исследование однослойных нейронных сетей на примере моделирования булевых выражений»

**Цель работы**: исследовать функционирование простейшей нейронной сети (НС) на базе нейрона с нелинейной функцией активации посредством обучения ее по правилу Видроу-Хоффа.

**Постановка задачи:** получить модель булевой функции (БФ) на основе однослойной НС (единичный нейрон = персептрон (рис. 1)) с двоичными входами 𝑥1,𝑥2,𝑥3,𝑥4∈{0,1}, единичным входом смещения 𝑥0=1, синаптическими весами 𝑤0, 𝑤1, 𝑤2, 𝑤3, 𝑤4, двоичным выходом 𝑦∈{0,1} и заданной нелинейной функцией активации (ФА) 𝑓:𝑅→(0,1).

Для заданной БФ реализовать обучение НС с использованием:

* всех комбинаций переменных 𝑥1,𝑥2,𝑥3,𝑥4;
* части возможных комбинаций переменных 𝑥1,𝑥2,𝑥3,𝑥4, остальные комбинации являются тестовыми.

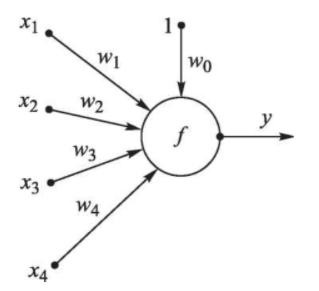


Рисунок 2.1. Однослойная нейронная сеть (персептрон).

Режимы работы НС: рабочий режим и режим обучения.

**Рабочий режим**: функционирование НС с пороговой ФА имеет вид:

Функционирование НС с логистической ФА имеет вид:

где out — сетевой (недискретизированный) выход НС.

**Режим обучения:** Для необученной НС её реальный выход y в общем случае отличается от целевого выхода – - булевой функции нескольких переменных . Имеется хотя бы один набор сигналов (𝑥1,𝑥2,𝑥3,𝑥4), для которого ошибка .

Каждая эпоха обучения 𝑘 = 1, 2, … включает в себя цикл последовательного предъявления всех образцов обучающей выборки на вход НС. Предъявление одного обучающего образца внутри эпохи является элементарным шагом обучения 𝑙 = 0, 1, 2, … , во время которого вектор весовых коэффициентов 𝐰 = (𝑤𝑖)𝑖 = 0, …, 4 корректируется согласно правилу Видроу — Хоффа (дельта-правило):

– коррекция веса на l-том шаге;

– норма обучения;

- ошибка.

На каждой эпохе k суммарная квадратичная ошибка E(k) равна расстоянию Хэмминга между векторами целевого и реального выходов.

**Исходные данные:**

| **№ варианта** | **Моделируемая БФ** | **ФА\*** |
| --- | --- | --- |
| 13 |  | 1, 2 |
| ; |

**Ход решения**

Построим таблицу истинности заданной БФ:

| **№** | **X1** | **X2** | **X3** | **X4** | **¬X1** | **¬X2** | **¬X3** | **¬X1∨¬X2∨¬X3** | **¬X2∨¬X3∨X4** | **(¬X1∨¬X2∨¬X3)∧(¬X2∨¬X3∨X4)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **0** | **0** | **0** | **0** | **0** | **1** | **1** | **1** | **1** | **1** | **1** |
| **1** | **0** | **0** | **0** | **1** | **1** | **1** | **1** | **1** | **1** | **1** |
| **2** | **0** | **0** | **1** | **0** | **1** | **1** | **0** | **1** | **1** | **1** |
| **3** | **0** | **0** | **1** | **1** | **1** | **1** | **0** | **1** | **1** | **1** |
| **4** | **0** | **1** | **0** | **0** | **1** | **0** | **1** | **1** | **1** | **1** |
| **5** | **0** | **1** | **0** | **1** | **1** | **0** | **1** | **1** | **1** | **1** |
| **6** | **0** | **1** | **1** | **0** | **1** | **0** | **0** | **1** | **0** | **0** |
| **7** | **0** | **1** | **1** | **1** | **1** | **0** | **0** | **1** | **1** | **1** |
| **8** | **1** | **0** | **0** | **0** | **0** | **1** | **1** | **1** | **1** | **1** |
| **9** | **1** | **0** | **0** | **1** | **0** | **1** | **1** | **1** | **1** | **1** |
| **10** | **1** | **0** | **1** | **0** | **0** | **1** | **0** | **1** | **1** | **1** |
| **11** | **1** | **0** | **1** | **1** | **0** | **1** | **0** | **1** | **1** | **1** |
| **12** | **1** | **1** | **0** | **0** | **0** | **0** | **1** | **1** | **1** | **1** |
| **13** | **1** | **1** | **0** | **1** | **0** | **0** | **1** | **1** | **1** | **1** |
| **14** | **1** | **1** | **1** | **0** | **0** | **0** | **0** | **0** | **0** | **0** |
| **15** | **1** | **1** | **1** | **1** | **0** | **0** | **0** | **0** | **1** | **0** |

Практическое решение исполнено при помощи Microsoft Visual Studio 2017 на языке C++.

Вектор начальных весов взят равным (l=0; k=0):

Используем пороговую функцию активации . Норма обучения взята . Динамика персептрона отражена на рисунках 2.2-2.6. График суммарной ошибки отражен на рисунке 2.7.

| Рисунок 2.2. Параметры НС на эпохе 1 | Рисунок 2.3. Параметры НС на эпохе 2 |
| --- | --- |
| Рисунок 2.4. Параметры НС на эпохе 3 | Рисунок 2.5. Параметры НС на эпохе 29 |

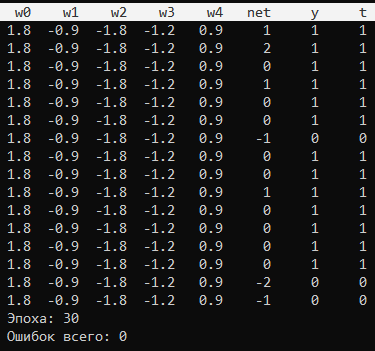


Рисунок 2.6. Параметры НС на эпохе 30

Итоговый весовой вектор:



Рисунок 7. Суммарная ошибка при пороговой ФА

Аналогичные таблицы (Рисунок. 2.8-2.10) построим для функции . График суммарной ошибки отражен на рисунке 2.11.

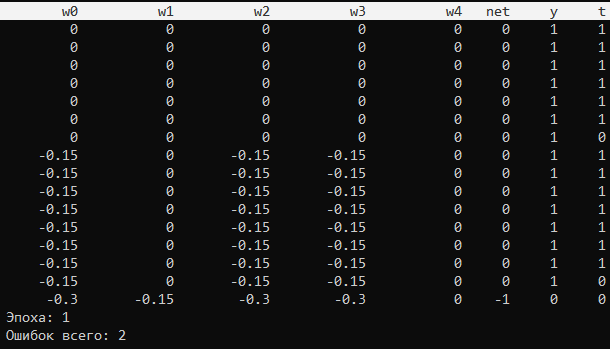


Рисунок 2.8. Параметры НС на эпохе 1

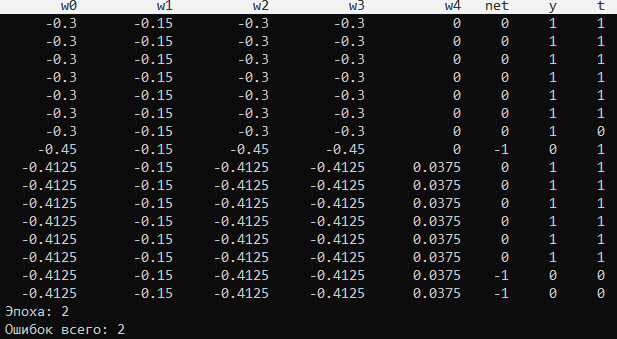


Рисунок 2.9. Параметры НС на эпохе 2

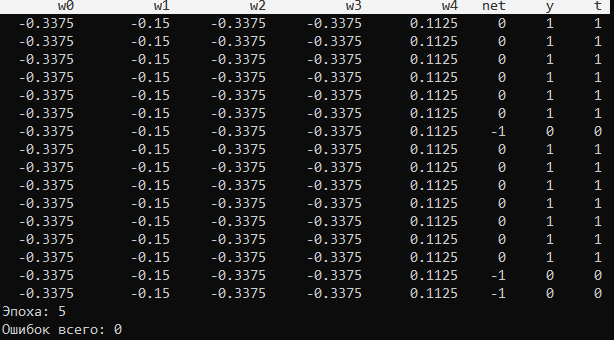


Рисунок 2.10. Параметры НС на эпохе 5

Итоговый весовой вектор:

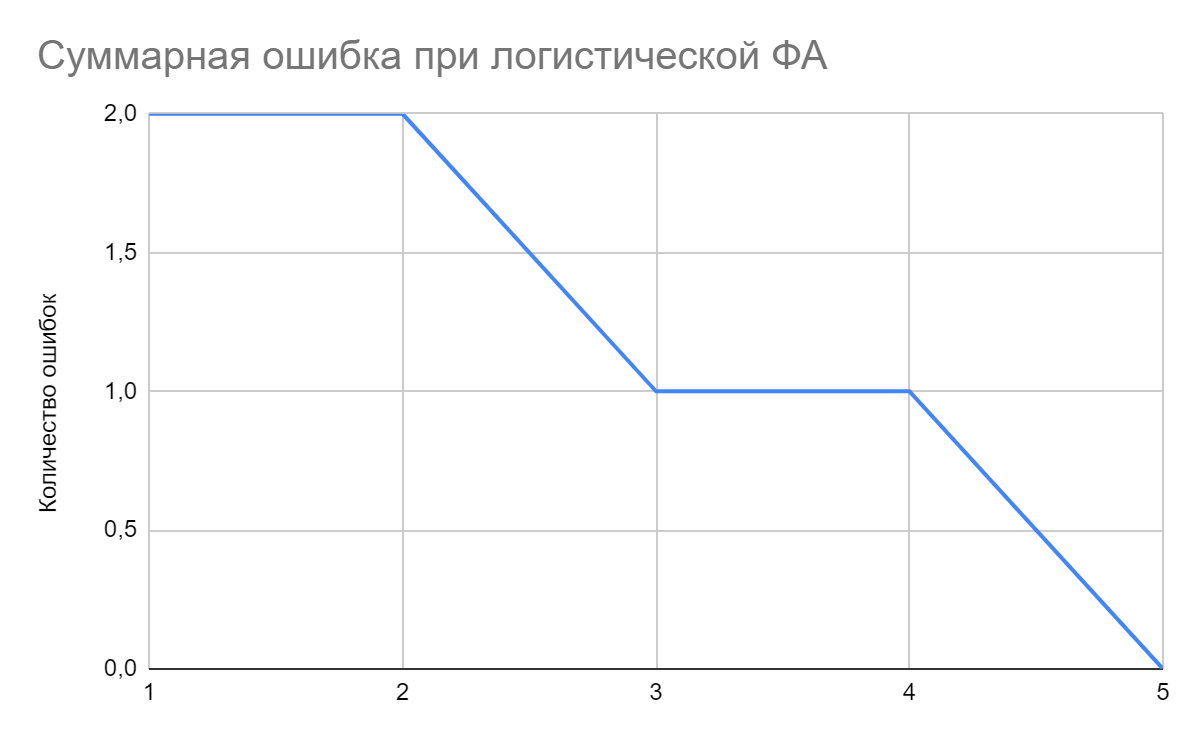


Рисунок 2.11. Суммарная ошибка при логистической ФА

Для пороговой функции уменьшим размер обучающей выборки при сохранении нулевой ошибки с целью уменьшения количества эпох, необходимых для обучения. Для функции:

Был обнаружен следующий набор выборки и изменена его последовательность, при которой сохраняется нулевая ошибка и уменьшается время обучения:

При этом время обучения удалось сократить до 6 эпох. Эпохи отражены на рисунках 2.12-2.15. Рисунок 2.16 отражает график суммарной ошибки. Рисунок 2.17 отражает результаты проверки.

| Рисунок 2.12. Параметры НС на эпохе 1 | Рисунок 2.13. Параметры НС на эпохе 2 |
| --- | --- |
| Рисунок 2.14. Параметры НС на эпохе 5 | Рисунок 2.15. Параметры НС на эпохе 6 |

Итоговый весовой вектор:

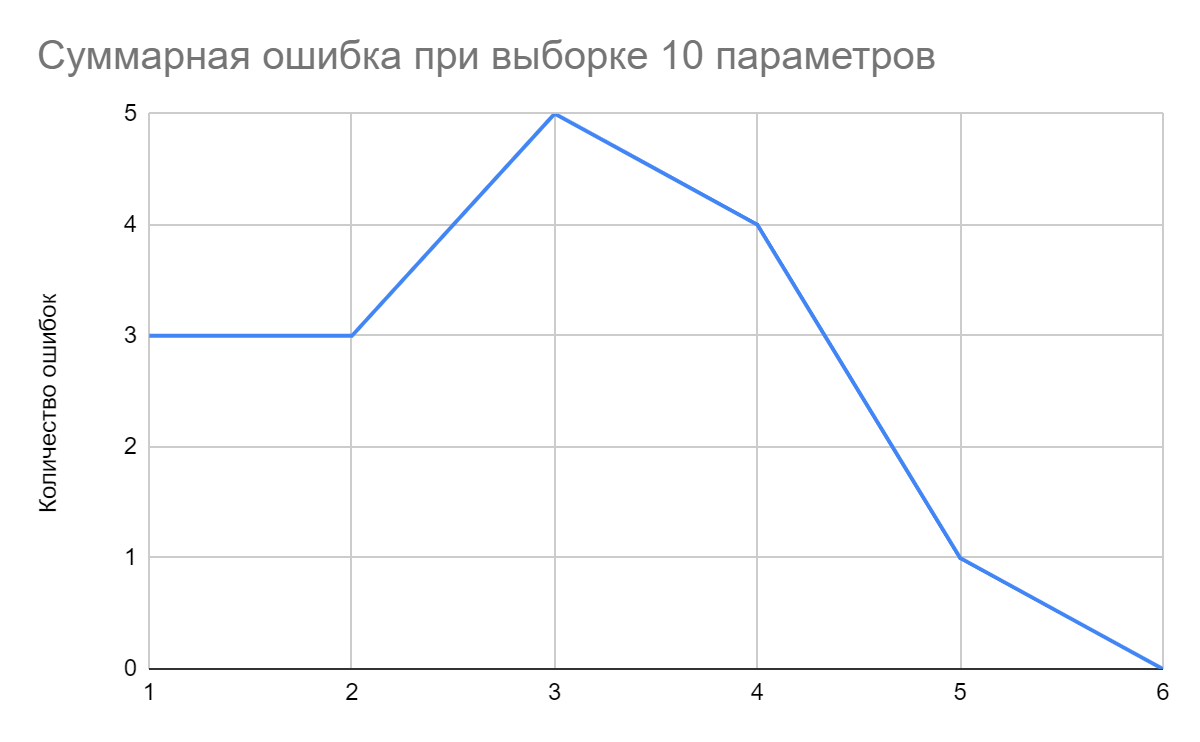


Рисунок 2.16. Суммарная ошибка НС при длине обучающей выборки равной 10

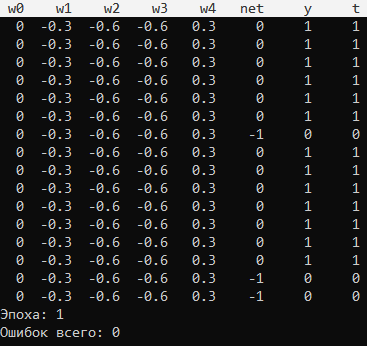


Рисунок 2.17. Результаты тестирования весового вектора на полной БФ.

**Вывод**

При использовании пороговой функции нейронная сеть обучалась достаточно долго, по сравнению с логистической. При попытке оптимизации методом выборки векторов было уменьшено время обучения на 80%, при тестировании полученного набора весов нейронная сеть не допустила ни одной ошибки. Из этого можно сделать вывод, что используя меньшее количество входных данных и определенную их последовательность, возможно сократить время обучения.

Таким образом, порядок начальных обучающих векторов определяет траекторию обучения НС.

# Лабораторная работа 3. Оценка результатов классификации при помощи метрик TP, FP, FN, TN, Accuracy, Precision, AUC, F-мера, матрица ошибок и лабораторная работа 4: «Алгоритмы машинного обучения с учителем для решения задач классификации»

**Цель работы:** исследовать функционирование алгоритмов машинного обучения с учителем для решения задач классификации. Освоить основные методы оценки метрик точности алгоритмов классификации.

**Теоретическая часть**

Классификация является одной из трех основных задач машинного обучения. Задача классификации подразумевает отнесение объекта к одной из категорий на основании его признаков.

Важнейшим аспектом задачи классификации, отличающей ее от задачи кластеризации, является известность признаков объекта (в том числе и меток/маркеров класса).

Для решений задачи классификации разработано большое количество методов машинного обучения. Один из алгоритмов, относящихся к методам вычислительного интеллекта, рассматривался в лабораторной работе №2 – однослойный персептрон (однослойная НС).

Рассмотрим один из алгоритмов метода машинного обучения – деревья решений. Основная идея алгоритмов, относящихся к данной категории – использование «древовидной» вложенной структуры вида if…else, позволяющей классифицировать данные по набору примитивных правил.

Для оценки качества построенного дерева вводится понятие энтропии.

Энтропия - это среднее количество информации, приходящееся на одно сообщение, символ, слово источника информации.

Энтропия характеризует также среднюю неопределённость ситуации. Чем больше энтропия, тем больше неопределённость ситуации и, следовательно, тем больше информации получает лицо, принимающее сообщение, устраняющее неопределённость.

Чаще всего дерево решений строится по принципу жадной максимизации прироста информации - на каждом шаге выбирается тот признак, при разделении по которому прирост информации оказывается наибольшим. Дальше процедура повторяется рекурсивно, пока энтропия не окажется равной нулю или какой-то малой величине. В разных алгоритмах применяются разные эвристики для "ранней остановки" или "отсечения", чтобы избежать построения переобученного дерева.

**Ход работы:**

Текущий набор данных представляет собой сведения о молоке и его запахе. В него входят такие параметры как: Температура, Вкус, Жирность, Мутность, Цвет и т.д.

Составим дерево решений, по которому можно будет определить тип гриба (рисунок 3.1).

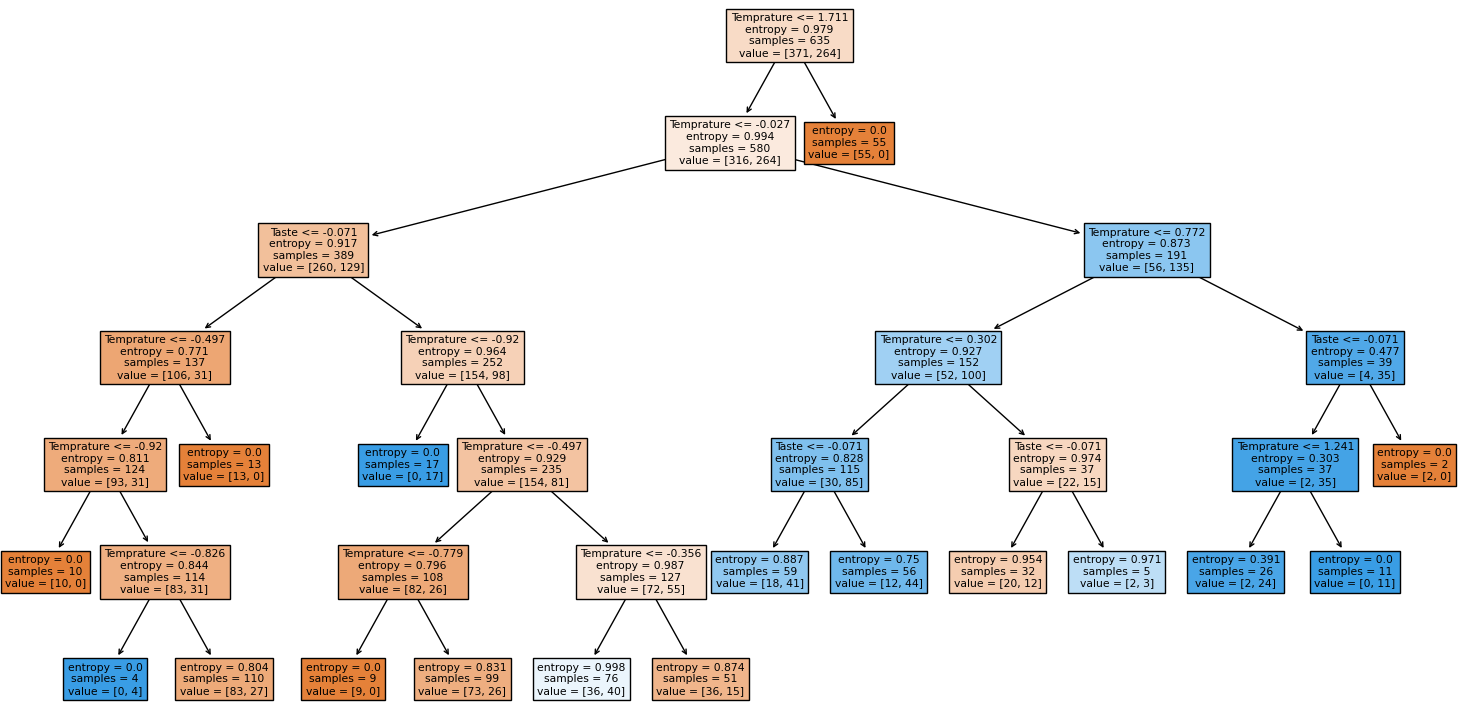


Рисунок 3.1. Дерево решений

Для построения дерева решений были выбраны следующие параметры:

| 1. Temperature  2. Taste  3. Fat  4. Turbidity  5. Colour | 1. Температура  2. Вкус  3. Жирность  4. Мутность  5. Цвет |
| --- | --- |

Оранжевый цвет - хороший запах, синий – плохой. Все данные сыграли примерно одинаково полезную роль при классификации и дали хороший результат.

Проведем анализ результатов обучения (Рис. 3.2-3.4).

| Рисунок 3.2. Матрица ошибок | Рисунок 3.3. Метрики |
| --- | --- |

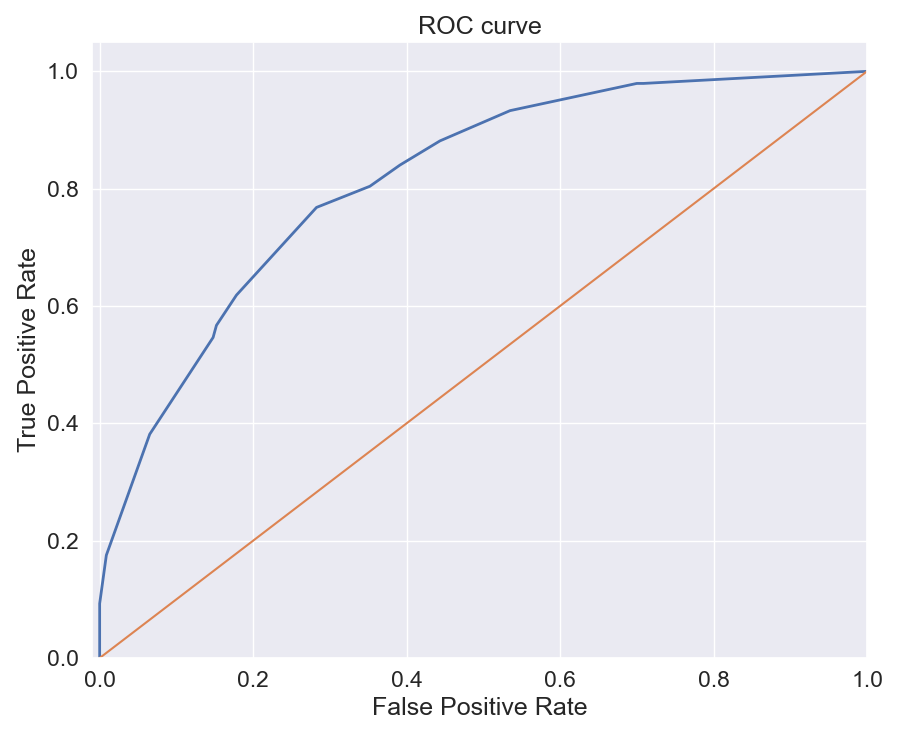


Рисунок 3.4. ROC кривая

На рисунке 3.2. (0 – хороший запах, 1 – плохой запах) видно, что доля неудовлетворительных ответов находиться на среднем уровне. Как можно заметить на рисунке 3.3. доля правильных ответов составляет 74%, что является хорошим результатом.

**Вывод**

По результатам выполнения лабораторных работ №3 и №4, был реализован алгоритм машинного обучения с учителем для решения задач классификации и была проведена оценка результатов классификации при помощи метрик TP, FP, FN, TN, Accuracy, Precision, AUC, F-мера, матрица ошибок. Алгоритм способен выдать в 74% верный результат, следовательно, есть 26% риск найти плохое молоко.

# Лабораторная работа 8. Снижение размерности входных данных на примере алгоритмов PCA, SVD

Цель работы: с использованием библиотеки scikit-learn изучить принципы работы алгоритмов сокращения размерности SVD и PCA.

Теоретическая часть

При работе с данными высокой размерности часто бывает полезно понизить размерность путем проецирования на подпространство меньшей размерности, которое улавливает основные особенности данных. Один из подходов к этой проблеме – предположить, что все наблюдаемые многомерные выходы 𝑥𝑛 ∈ ℝ𝐷 порождены множеством скрытых, т. е. ненаблюдаемых латентных факторов низкой размерности 𝑧𝑛 ∈ ℝ𝐾.

Простейшим примером является применение факторного анализа. В частном случае, факторный анализ сводится к модели вероятностного метода главных компонент (principal components analysis — PCA

Cингулярное разложение (SVD), является обобщением спектрального разложения на прямоугольные матрицы. Любую вещественную матрицу A размера m´n можно разложить в произведение:

****

где U – матрица 𝑚 × 𝑚 с ортонормированными столбцами (т. е. 𝑼 = 𝑰𝒎), V – матрица 𝑛 × 𝑛 с ортонормированными строками и столбцами (т. е. 𝑽 = 𝑽 = 𝑰𝒏), а S – матрица 𝑚 × 𝑛, содержащая r = min(m, n) сингулярных чисел 𝜎𝑖 ≥ 0 на главной диагонали и нули во всех остальных позициях. Столбцы U называются левыми сингулярными векторами, а столбцы V – правыми сингулярными векторами.

**Ход работы:**

| Рисунок 4.1. Тренировочный набор | Рисунок 4.2. Тестовый набор |
| --- | --- |

На рисунках 4.1-4.2 видно, что часть плохого молока (1) находятся в зоне хорошего (0), а часть хорошего на стороне плохого.

| Рисунок 4.3. Метрики | Рисунок 4.4. Метрики |
| --- | --- |

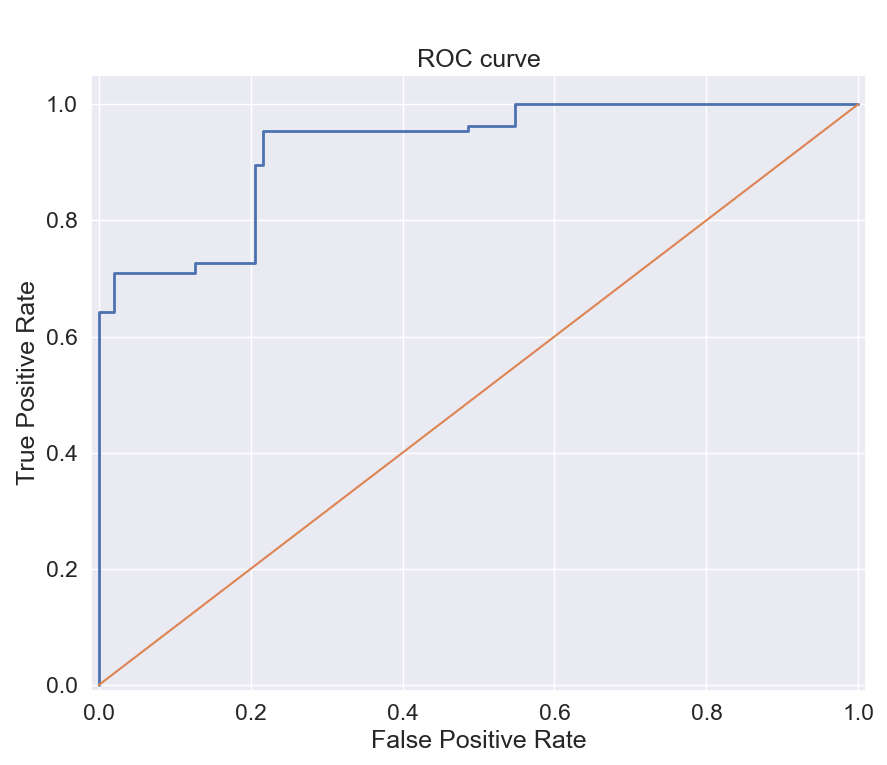


Рисунок 4.5. ROC-кривая

Анализируя метрики можно сделать вывод, что алгоритм классификации работает корректно, точность составляет 82% .

**Вывод**

В общем случае по данным результатам следует сказать следующее. При возникновении сомнений по поводу съедобности молока стоит его пропустить. Количество неверно классифицированного молока, а именно пропавшего, среднее. Следует отметить, что употребление пропавшего молока с таким процентом его выявления не повлечет для человека серьезных последствий, следовательно, наличие данного алгоритма лучше, чем его отсутствие.