М. В. Стержанов, С. С. Заливако, А. И. Гридасов
Белорусский государственный университет
информатики и радиоэлектроники

РАЗВИТИЕ ПРАКТИЧЕСКИХ НАВЫКОВ ПО КУРСУ «МАШИННОЕ ОБУЧЕНИЕ»

Кафедра Информатики Белорусского государственного университета информатики и радиоэлектроники ведет подготовку по специальности «Информатика и технологии программирования». «Машинное обучение» (МО) - одна из основных дисциплин при подготовке магистрантов очной и заочной форм обучения. Данная дисциплина знакомит учащихся с ключевыми математическими концепциями и методами, необходимыми для понимания машинного обучения (дискриминантный, кластерный и регрессионный анализ). Особый акцент при проведении занятий уделяется овладению навыками практического решения задач интеллектуального анализа данных. Курс читается на протяжении двух семестров: в первом семестре формой контроля является зачет, во втором - экзамен.

Обучение традиционно происходит в форме лекционных и лабораторных занятий, а также самостоятельной работы студентов. Теоретический материал излагается на лекциях. В соответствии с планом дисциплины, на лекционные занятия отводится по 6 часов в семестр: 4 часа в установочную сессию и 2 часа в экзаменационную. Очевидно, что такого объема недостаточно для детального изложения и подробного разбора материала. Поэтому проводится обзорная лекция,

затрагивающая основные принципы и концепции главных разделов курса. Основной учебный материал студентам предлагается освоить самостоятельно по предложенным литературным источникам (включая англоязычные статьи и книги). Для получения допуска студентам необходимо выполнить лабораторные работы и защитить реферат на заданную тему.

В данной работе рассматриваются некоторые задачи, предлагаемые для проработки материала по предмету МО и имеющие высокую практическую значимость. Лабораторные работы построены на базе курса [1].

При изучении рекомендательных систем студентам предлагается применить на практике два базовых подхода: коллаборативная фильтрация (collaborativefiltering) и контентная фильтрация(content-basedfiltering). Студентам следует изучить основные концепции, на которых основаны рекомендательные системы, и изучить алгоритмы, которые реализуют эти концепции. Перейдем к описанию практической части. Исходный набор данных содержит две матрицы *Y* и *R* - рейтинг 1682 фильмов среди 943 пользователей, соответственно. Значение *Rij* может быть равно 0 или 1 в зависимости от того оценил ли пользователь *j* фильм *i*. Матрица *Y* содержит числа от 1 до 5 - оценки в баллах пользователей, выставленные фильмам. Перед студентами ставятся следующие задачи:

- выбрать число признаков фильмов (*n*) для реализации алгоритма коллаборативной фильтрации;
- реализовать функцию стоимости для алгоритма;
- добавить *L2*-регуляризацию в модель;
- обучить модель с помощью градиентного спуска или других методов оптимизации;
- обучить модель с помощью сингулярного разложения матриц;
- реализовать функцию вычисления градиентов;
- добавить L2-регуляризацию в модель.

Градиентный бустинг — это широко распространенная техника машинного обучения для задач классификации и регрессии, которая строит модель предсказания в форме ансамбля слабых предсказывающих моделей, обычно деревьев решений. При выполнении работы студентам предлагается в цикле обучить последовательно 50 решающих деревьев с параметрами *max_depth*=5 и *random_state*=42 (остальные параметры выбираются по умолчанию). Каждое дерево должно обучаться на одном и том же множестве объектов, но ответы, которые учится прогнозировать дерево, будут

меняться в соответствии с отклонением истинных значений от предсказанных. В процессе реализации обучения студентам требуется реализовать функцию вычисления прогноза построенной на данный момент композиции деревьев на выборке *X*. Студенты исследуют процесс переобучения градиентного бустинга с ростом числа итераций, а также с ростом глубины деревьев. Выводы делаются посредством анализа соответствующих графиков. Последней задачей данной работы является сравнение качества, получаемого с помощью градиентного бустинга с качеством работы линейной регрессии. Для этого следует обучить с параметрами по умолчанию *LinearRegression* из *sklearn.linear_model* на обучающей выборке и оценить для прогнозов полученного алгоритма на тестовой выборке *RMSE*.

Одной из наиболее важных с точки зрения закрепления усвоенного материала работ является «Реализация криптографических атак с помощью машинного обучения на физически неклонируемые функции». Физически неклонируемые функции (ФНФ) часто используются в качестве криптографических примитивов при реализации протоколов аутентификации. Студенты рассматривают простейший протокол аутентификации с применением ФНФ [3]. В данном случае устройство *A*, содержащее реализацию ФНФ, может быть аутентифицировано с помощью набора запросов и проверки ответов на них. При этом использованные пары запрос-ответ удаляются из базы данных устройства.

Студентам предлагается самостоятельно проработать хрестоматийную работу У. Рурмаира [4], и сформулировать задачу о криптографических атаках на ФНФ в терминах машинного обучения. Студентам требуется обучить модель, которая могла бы предсказывать ответы по запросам, которых нет в обучающей выборке, применив как минимум три различных алгоритма (например, метод опорных векторов, логистическая регрессия и градиентный бустинг). В результате требуется выявить наиболее подходящую для оценки качества алгоритма метрику.

После успешного решения описанных задач учащийся магистратуры сможет самостоятельно сформулировать и решить практическую задачу машинного обучения, выбрать метрику качества, обучить модель, подобрать гиперпараметры, провести валидацию.

Список использованной литературы

1. https://www.coursera.org/learn/machine-learning [Электронный ресурс] - Дата доступа : 11.01.2020.

2. https://scikit-learn.org/stable/datasets/index.html#boston-dataset [Электронный ресурс] - Дата доступа : 11.01.2020.

3. U. Ruhrmair et al., «Modeling attacks on physical unclonable functions,» in Proc. ACM Conf. on Comp. and Comm. Secur. (CCS'10), Oct. 2010, pp. 237–249.

4. Иванюк, А. А. Проектирование встраиваемых цифровых устройств и систем: монография / А. А. Иванюк. — Минск :Бестпринт, 2012. — 337 с.