

Вопросы на зачет по Верификации систем ИИ

1. Задача классификации, оценки обобщающей способности методами кросс-валидации
 - Записать общую формулу байесовского классификатора (надо помнить формулу).
 - Что такое наивный байесовский классификатор?
2. Линейная классификация, линейный классификатор как модель нейрона
3. Понятие отступа, непрерывные аппроксимации функции потерь
 - Как выражается функция потерь в логистической регрессии (надо помнить формулу).
 - Какая функция потерь используется в методе опорных векторов (SVM)?
4. Оценка качества классификатора на основе диаграммы ранжированной выборки по отступам
5. Метод стохастического градиента для линейной классификации
6. Проблема мультиколлинеарности и регуляризация для линейной классификации, настройка параметра регуляризации кросс-валидацией
7. Логистическая регрессия, связь с оптимальным байесовским классификатором, оценивание рисков по методике VaR
8. Метод опорных векторов, использование кросс-валидации для настройки параметра регуляризации
9. Метод LASSO, использование кросс-валидации для настройки параметра селективности
10. Оценивание качества обучения с помощью ROC-кривой
11. Непараметрическое восстановление плотности методом Парзена-Розенблатта. Метод скользящего контроля для настройки ширины окна.
12. Многослойные нейронные сети. Проблема полноты, вычислительные возможности нейронных сетей.
 - Почему любая булева функция представима в виде нейронной сети? Сколько в ней слоёв?
 - Что такое «паралич» сети, и как его избежать?
13. Особенности глубоких нейронных сетей, сверточные нейронные сети: свертки и агрегирующие функции (пулинги).
14. Методы формальной верификации искусственных нейронных сетей
 - верификация и валидация ПО
 - тестирование и формальная верификация искусственных нейронных сетей
 - понятия "свойства" нейронной сети и "контрпримера"
 - линейная релаксация для верификации нейронной сети с функцией активации RELU
 - точное моделирование функции активации RELU в модели частично целочисленного линейного программирования (ЧЦЛП)

- точное моделирование функции максимума в модели ЧЦЛП

Литература

- А.Б. Мерков. Распознавание образов. Введение в методы статистического обучения. 2011. 256 с.
- Р.М. Селевенко, Е.Н. Строева. Исследование и разработка алгоритма формальной верификации и метрики оценки качества на основе методов понижения размерности ИНС. International Journal of Open Information Technologies ISSN: 2307-8162 vol. 12, no. 6, 2024. <http://injoit.org/index.php/j1/article/download/1899/1702>
- Е.Н. Строева, А.А. Тонких. Методы формальной верификации искусственных нейронных сетей: обзор существующих подходов. International Journal of Open Information Technologies. vol. 10, no. 10, 2022. <http://injoit.org/index.php/j1/article/viewFile/1417/1304>
- К.В. Воронцов. Машинное обучение. Курс лекций. 2011. <http://www.machinelearning.ru/wiki/images/6/6d/Voron-ML-1.pdf>
- К.В. Воронцов. Машинное обучение 2019. Видео-лекции. Школа анализа данных Яндекс. 2019. <https://www.youtube.com/playlist?list=PLJOzdkh8T5krxc4HsHbB8g8f0hu7973fK>
- ГОСТ Р ИСО/МЭК 24029-2-2024 Искусственный интеллект. Оценка робастности нейронных сетей. Часть 2. Методология использования формальных методов. https://allgosts.ru/35/020/gost_r_iso!mek_24029-2-2024
- Tjeng V., Xiao K., Tedrake R. Evaluating Robustness of Neural Networks with Mixed Integer Programming. The International Conference on Learning Representations. 2019 <https://arxiv.org/abs/1711.07356>