Reliable ML

Dmitry Kolodezev & Irina Goloshchapova

Jul 02, 2023

CONTENTS

Концепция Reliable ML рассказывает о том, что делать, чтобы результат работы data команд был, во-первых, применим в бизнес-процессах компании-заказчика, а, во-вторых, приносил этой компании пользу.

Для этого нужно уметь: правильно собрать портфель проектов, продумать дизайн системы каждого проекта, преодолеть разные трудности при разработке прототипа, создать заслуживающий боевого тестирования MVP, провести пилотный эксперимент, внедрить ваше решение в бизнес-процессы, настроить мониторинг решения в проде.

В книге авторы делятся фреймворком работы с ML-проектами, основанном на широкой практике разработки и внедрения ML-решений в бизнес, приносящих крупную прибыль, несмотря на множество набитых шишек.

Part I

Введение

CHAPTER

ONE

КОНЦЕПЦИЯ RELIABLE ML

Удачные и неудачные ML-проекты и где они обитают. О том, как появилась концепция Reliable ML.

Part II

Reliable ML: бизнес

CHAPTER

TWO

ВЫБОР ML-ПРОЕКТА

Как выбрать направление работы, которое будет наиболее полезно компании.

Правильно собрать портфель проектов.

Идентифицировать стейкхолдеров?

Роли в команде.

CHAPTER

THREE

ML SYSTEM DESIGN

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

3.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

FOUR

РАЗРАБОТКА ПРОТОТИПА

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

4.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

FIVE

ПИЛОТИРОВАНИЕ И ОЦЕНКА ЭФФЕКТА

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

5.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

SIX

ВНЕДРЕНИЕ РЕШЕНИЯ

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

6.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

SEVEN

МОНИТОРИНГ МОДЕЛЬНОГО РИСКА

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

7.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

Part III

Reliable ML: техника

CHAPTER

EIGHT

ОБЪЯСНИМОЕ МАШИННОЕ ОБУЧЕНИЕ

Разрабатывая и внедряя ML-модели, мы фактически перепоручаем алгоритмам приняние решений. Нам нужно объяснять принятые решения другим участникам бизнес-процесса. Нам нужно контролировать качество принятых решения, а для этого хорошо бы понимать - как они были приняты. И - нам нужно разбираться с ошибками, работать над качеством моделей, данных и процессов.

eXplainable AI (XAI) - набор подходов и библиотек, позволяющих объяснять предсказания моделей машинного обучения и исследовать то, как они принимают решения. Иногда разделяют Explaination - т.е. объяснение процесса принятия решения, и Interpretation - аттрибутирование принятого решения входными признаками. Разницу можно понять на следующем примере:

Нейронная сеть - функция, вычислимая через последовательные матричные преобразования входных данных, и в этом смысле она полностью объяснима - мы можем проследить путь от входного признака до результата, но таких преобразований слишком много, они “не уместятся в голове” пользователей. С другой стороны, интерпретация может звучать как “эта нейронная сеть определяет пол взрослых животных по их окраске, а детенышей она различает по силуэту” - что будет, скорее всего, очень вольным описанием происходящего - зато понятным для пользователя.

Инструменты XAI постоянно развиваются. За подробным описанием мы отсылаем читателя к книге Кристофа Мольнара [Mol22]. Здесь мы хотели бы остановиться на некоторых основополагающих подходах, которые полезно понимать и использовать.

CHAPTER

NINE

CAUSAL INFERENCE IN ML

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

9.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

TEN

MLOPS

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

10.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

ELEVEN

DATA CENTRIC AI

Датацентричный подход (Data Centric AI) - набор подходов и техник, позволяющий улучшить набор данных, на котором учится наша модель. Часто работа над качеством данных - самый надежный путь для улучшения качества ML-модели.

Алгоритмы для поиска и исправления типичных проблем в данных, в основном в данных для обучения с учителем.

Классический подход Model Centric AI концентрируется на том, чтобы подобрать лучшую модель для имеющегося датасета, используя разные типы моделей (нейронные сети, решающие деревья и т.д.), техники (регуляризация, оптимизаторы функции потерь), техники подбора гиперпараметров и ансамблирование моделей. Все это делается исходя из предположения, что данные для обучения фиксированы и повлиять на них нельзя.

В реальных приложениях данные чаще всего не фиксированы - мы можем модифицировать датасет, собирать дополнительные данные, перепроверять разметку и исключать данные, вносящие шум.

Данные в реальных проектах часто грязные, и содержат столько проблем, что улучшение набора данных обычно - обязательный шаг на пути к хорошей модели. Как часто говорят, мусор на входе - мусор на выходе.

Data Centric AI - систематический подход к работе с данными для того, чтобы модели на них обучались лучше.

Два основных подхода:

1) Алгоритмы, анализирующие данные и использующие эту информацию для улучшения модели. Например, Curriculum Learning - обучение модели сначала на простых данных, а потом на сложных.

2) Алгоритмы, модифицирующие данные для того, чтобы улучшить модель. Confident Learning - пример такого подхода, в котором модель учится на данных, из которых удалены ошибочно размеченные данные.

Определение “легких для обучения” и ошибочно размеченных данных выполняется автоматическм с помощью алгоритма, анализирующего работу обученной ML - модели.

Задача Model Centric AI - построить наилучшую модель для имеющегося датасета. Задача Data Centric AI - систематически и алгоритмически улучшать датасет, чтобы сделать его более полезным для модели. Для получения хорошего результата нужно сочетать оба подхода.

Например, процесс построения ML-модели может выглядеть так:

1. Проводим разведочный анализ данных (Exploratory Data Analysis). Исправляем основые проблемы данных. Преобразуем их в формат, удобный для моделирования.
2. Обучаем черновую (baseline) версию модели.
3. Используя модель, улучшаем набор данных.
4. Обучаем модель на улучшенном датасете. При необходимости возвращаемся на шаг 3 и пробуем сделать данные еще лучше.

Пример техник, используемых в датацентричном подходе:

- Детектирование и исключение аномалий
- Выявление и коррекция ошибок разметки
- Поиск консенсуса в разметке, полученной из разных источников
- Аугментация данных (добавление данных в модель на основе априорного знания о природе данных)
- Генерация и отбор признаков
- Активное обучение - выбор наиболее информативных данных для доразметки
- Cirriculum Learning - упорядочивание примеров для обучения от простого к сложному

Надежность ML-модели в значительной степени зависит от качества данных, на которых она обучалась.

Part IV

ReliableML: тренды

CHAPTER

TWELVE

ТРЕНД НОМЕР ОДИН

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

12.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

Part V

Приложения

CHAPTER

THIRTEEN

ШАБЛОН ДИЗАЙН-ДОКУМЕНТА

Whether you write your book's content in Jupyter Notebooks (`.ipynb`) or in regular markdown files (`.md`), you'll write in the same flavor of markdown called **MyST Markdown**. This is a simple file to help you get started and show off some syntax.

13.1 What is MyST?

MyST stands for "Markedly Structured Text". It is a slight variation on a flavor of markdown called "CommonMark" markdown, with small syntax extensions to allow you to write **roles** and **directives** in the Sphinx ecosystem.

CHAPTER

FOURTEEN

ЛИТЕРАТУРА

BIBLIOGRAPHY

[Mol22] Christoph Molnar. *Interpretable Machine Learning*. 2 edition, 2022. URL: https://christophm.github.io/interpretable-ml-book.