Лекция 1.

Тема: Введение в машинное обучение

Машинное обучение (machine learning, ML) — это дисциплина, находящаяся на стыке прикладной статистики, численных методов оптимизации и дискретного анализа. За последние годы она оформилась в самостоятельную и активно развивающуюся область с глубокой математической основой и широким инженерным применением.

В данном курсе рассматриваются фундаментальные задачи обучения по прецедентам. Основное внимание уделяется глубокому пониманию математических основ, взаимосвязей между методами, а также их достоинств и ограничений.

Ключевые темы курса:

1. Основы работы с данными: предобработка, очистка, feature engineering.
2. Классификация: алгоритмы для отнесения объектов к заранее известным категориям.
3. Кластеризация: методы для выявления скрытых структур и группировки схожих объектов.
4. Регрессия: прогнозирование непрерывных числовых значений.
5. Нейронные сети и глубокое обучение: от перцептронов до современных архитектур.
6. Компьютерное зрение: анализ и классификация изображений.
7. Обработка естественного языка (NLP): задачи, связанные с пониманием и генерацией текста.

Все методы в курсе излагаются по единой схеме с обеспечением системного подхода к их освоению:

Исходные идеи и эвристики: интуитивное объяснение подхода.
Формализация и математическая теория: строгое представление алгоритма.
Анализ: разбор достоинств, недостатков и границ применимости.
Пути развития: обсуждение методов устранения недостатков.
Сравнительный анализ: взаимосвязи с другими методами машинного обучения.
Практика: примеры решения прикладных задач.

Курс включает разбор дополнительных примеров, аспектов практического применения, особенностей работы с данными, программирования и проведения вычислительных экспериментов.

От студентов требуются знания курсов линейной алгебры, математического анализа, теории вероятностей, языка программирования Python (и библиотеки для анализа данных, такие как NumPy, Pandas, Scikit-learn).

Введение

История вычислений тесно связана с попытками решить задачи, непосильные для человека. Яркий пример — работа Алана Тьюринга по взлому шифра «Энигма» во время Второй мировой войны. Человеческий мозг был не в состоянии перебрать все возможные варианты шифра, но специальная машина — делала это с огромной скоростью.

Однако, важно понимать: далеко не всякую сложную для человека задачу можно решить просто написав алгоритм. Существует целый класс так называемых NP-трудных задач, для которых не существует эффективного алгоритма решения даже для самого мощного компьютера,.

Но что по-настоящему парадоксально: существует и обратная ситуация. Есть задачи, которые человек решает практически не задумываясь, но которые на удивление сложно формализовать и поручить компьютеру.
Классические примеры таких задач:

Распознать, что изображено на фотографии.

Поставить медицинский диагноз на основе симптомов.

Оценить рыночную стоимость квартиры.

Определить, какой документ более релевантный поисковому запросу.

Выполнить качественный перевод с одного языка на другой.

И именно машинное обучение появилось как попытка научить компьютер решать такого рода задачи.
Основы области были заложены в 1958 году, когда Фрэнк Розенблатт предложил архитектуру перцептрона — первую математическую модель искусственного нейрона — и реализовал её в виде физического устройства, «Марк-1». Это достижение было воспринято научным и общественным сообществом как прорыв: в публикации The New York Times перцептрон был охарактеризован как «эмбрион электронного компьютера, способного к самостоятельному обучению, распознаванию образов и самосознанию».

Понятие машинного обучения придумал американский исследователь Артур Самуэль, работавший в IBM. В 1959 году он создал

первую программу по игре в шашки, которая умела играть сама с собой и обучаться самостоятельно. По определению Артура Сэмюэла, машинное обучение — это "поле исследования, дающее компьютерам возможность учиться без явного программирования", что подчеркивает его способность адаптироваться и действовать на основе накопленного опыта.

Последующее развитие области столкнулось с ограничениями вычислительных мощностей и теоретической базы. Значительный прогресс произошел лишь в 1980-х годах, когда были формализованы теоретические основы обучения с учителем и без учителя, а также заложены фундаментальные принципы построения нейронных сетей и алгоритмов на основе деревьев решений. Именно в этот период машинное обучение оформилось как самостоятельная научная дисциплина, ориентированная на решение практических задач распознавания образов и классификации.

В 1990-е годы рост вычислительных ресурсов и увеличение объёмов доступных данных способствовали экспансии методов машинного обучения в такие области, как экономика, биомедицина и обработка естественного языка. На этом этапе начали активно развиваться методы глубокого обучения, которые впоследствии легли в основу современных систем распознавания речи, компьютерного зрения и машинного перевода.

Качественный скачок в развитии инфраструктуры машинного обучения произошёл в 2010-х годах. В 2011 году было основано подразделение Google Brain, ориентированное на масштабные исследования в области искусственного интеллекта. Вслед за этим Amazon и Microsoft представили облачные платформы для развёртывания ML-моделей, а Facebook в 2014 году внедрила систему DeepFace, демонстрирующую высокую точность в задаче верификации лиц.

В начале 2020-х годов развитие ускорилось: в 2018 году Google массово внедрила вычислительную фотографию, в 2019-м NVIDIA представила архитектуру StyleGAN для генеративной синтеза изображений, а в 2022-м публикация моделей ChatGPT и Midjourney ознаменовала новый этап в доступности использования ИИ-технологий.

Параллельно с академическими и коммерческими разработками, машинное обучение стало ключевым инструментом в решении социально значимых и промышленных задач. Так, в Москве с 2020 года системы компьютерного зрения используются для анализа более 11 миллионов медицинских исследований. В Финляндии разработан сервис VTT EnergyTeller, использующий ИИ для прогнозирования спроса на энергию. В России в 2023 году нейросетевая модель, разработанная «Газпром нефтью», позволила идентифицировать новое месторождение углеводородов в Западной Сибири, что свидетельствует о переходе ML в категорию критически важных технологий для промышленности и науки.

Ключевые аспекты, определяющие центральную роль машинного обучения в современных научных и прикладных исследованиях:

1. Автоматизация сложноформализуемых процессов.

Классические алгоритмические подходы требуют явного описания правил и эвристик, что зачастую невозможно для задач высокой семантической сложности. Машинное обучение, в частности, методы глубокого обучения, позволяют автоматически выявлять закономерные паттерны непосредственно из данных. Это устраняет необходимость создания исчерпывающих экспертных систем. Яркими примерами служат распознавание и синтез речи (модели обучаются напрямую на аудиосигналах и текстовых транскриптах, минуя создание ручных фонетических и грамматических правил) и компьютерное зрение (задачи классификации, детекции и сегментации изображений решаются путем обучения сверточных нейронных сетей на размеченных данных, а не через прописывание алгоритмических фильтров для каждого возможного объекта).

2. Анализ больших данных и обнаружение скрытых закономерностей.

В эпоху цифровой трансформации объемы генерируемых данных превышают возможности их обработки традиционными методами статистики. Машинное обучение предоставляет возможности для:

Выявления нетривиальных корреляций и зависимостей в многомерных пространствах признаков, неочевидных для человеческого восприятия.

Сокращения размерности и визуализации сложных данных без существенной потери информативности.

Кластеризации и выявления скрытых закономерностей, что критически важно в биоинформатике (классификация типов клеток), социологии (сегментация аудитории) и других дисциплинах.

3. Принятие решений на основе прогнозного моделирования.

Способность моделей МО к обобщению и экстраполяции на ранее не встречавшихся данных делает их незаменимым инструментом для построения прогнозных систем:

В экономике и финансах: это прогнозирование временных рядов (курсы акций, спрос на продукцию), оценка кредитных рисков и выявление мошеннических операций.

В науке: ускоряется процесс научного исследования — от предсказания свойств новых материалов и молекул до анализа астрономических данных.

В управлении: системы, основанные на обучении с подкреплением, начинают применяться для оптимизации сложных процессов, таких как логистические цепочки или управление энергосетями.

Таким образом, машинное обучение трансформируется из академической дисциплины в ключевой кросс-дисциплинарный инструмент, позволяющий решать задачи, которые ранее считались не поддающимися алгоритмизации, и извлекать знание из данных масштабов, ранее недоступных для анализа.

Основные понятия и типы задач

1. Данные (Data)

Данные — это исходная информация, представленная в структурированном или неструктурированном виде, которая используется для обучения моделей и последующего анализа. Данные могут включать числовые, категориальные, текстовые или мультимедийные значения.

Качество и репрезентативность данных напрямую влияют на эффективность модели. Принцип «мусор на входе — мусор на выходе» (Garbage in, garbage out) особенно актуален в машинном обучении.

Примеры:

Табличные данные (например, CSV-файл с информацией о домах).

Изображения, аудиозаписи, тексты.

Временные ряды (например, котировки акций).

2. Признаки (Features)

Признаки — это характеристики объектов в данных, которые используются для прогнозирования или классификации. Каждый признак представляет собой измеряемое свойство объекта.

Инженерия признаков (Feature Engineering) — процесс создания новых признаков или преобразования существующих для улучшения качества модели.

Отбор признаков (Feature Selection) — выбор наиболее значимых признаков для упрощения модели и ускорения обучения.

Примеры:

Для объекта «дом» признаками могут быть: площадь, район, этаж, год постройки.

Для объекта «текст»: длина предложения, частота слов, наличие определенных терминов.

3. Целевая переменная (Target Variable)

Целевая переменная — это зависимая переменная, которую модель обучается предсказывать на основе признаков. В задачах обучения с учителем целевая переменная известна на этапе обучения. Важно: В задачах без учителя целевая переменная отсутствует (например, кластеризация).

Примеры:

В задаче предсказания цены дома: цена (числовая величина).

В задаче классификации emails: метка «спам/не спам» (категориальная величина).

4. Модель (Model)

Модель — это математический алгоритм, который обучается на данных для выявления взаимосвязей между признаками и целевой переменной. Обученная модель способна делать прогнозы на новых данных. Модели могут быть интерпретируемыми (например, линейная регрессия) или «черным ящиком» (например, глубокие нейронные сети).

Примеры моделей:

Линейная регрессия (для прогнозирования числовых значений).

Дерево решений (для классификации и регрессии).

Нейронная сеть (для сложных задач, таких как распознавание изображений).

5. Обучение (Training)

Обучение — процесс настройки параметров модели таким образом, чтобы она максимально точно предсказывала целевую переменную на обучающих данных. Это итеративный процесс минимизации ошибки предсказания.

Ключевые понятия:

Обучающая выборка (Training Dataset) — данные, используемые для обучения модели.

Функция потерь (Loss Function) — метрика, которая измеряет ошибку предсказания и которую модель стремится минимизировать.

Гиперпараметры — параметры, которые задаются до начала обучения (например, скорость обучения, количество деревьев в ансамбле).

6. Прогноз (Inference)

Определение:

Прогноз (или вывод) — процесс применения обученной модели к новым, ранее не виденным данным для получения предсказаний. На этом этапе модель использует выявленные закономерности для практического применения. Эффективность модели оценивается на тестовой выборке (данных, которые не использовались при обучении), чтобы проверить ее способность к обобщению.

Пример:

Использование обученной модели для предсказания цены нового дома на рынке на основе на его признаков.

Основные задачи машинного обучения

Классификация – метод машинного обучения, который заключается в разделении множества объектов на конечное число групп и присвоение класса каждой из таких групп.

Примеры: классификация отзывов на отрицательные и положительные, классификация музыкальных композиция по жанрам.

Кластеризация – метод машинного обучения, который используется для группировки похожих объектов в кластеры, так чтобы объекты внутри одного кластера были более похожи друг на друга, чем на объекты из других кластеров.

Пример: кластеризация доходов населения

Регрессия – метод исследования влияния одной или нескольких независимых переменных на зависимую переменную.

Пример: по числовым показателям недвижимости определить её цену продажи, по погодным числовым характеристикам определить площадь возгорания лесов.

Прогнозирование временных рядов – это множество методов, позволяющих определить следующее значение x_{t+1} временного ряда $X = x_1 x_2 \ldots x_t$, в котором все значения принадлежат некоторому конечному алфавиту A.

Пример: прогнозирование погоды, повышение/понижение курса валюты.

Уменьшение размерности – алгоритм, позволяющий уменьшить количество описывающих признаков, не изменив при этом структуру множества объектов.

Основные требования к методам понижения размерности заключаются в том, что количество новых признаков, описывающих объекты исходного множества должно быть меньше, чем количество исходных признаков, и при этом новые признаки должны содержать как можно больше информации из исходных признаков.

Классификация методов по типу обучения

1. Обучение с учителем

Есть размеченные данные (известны и входы, и правильные ответы). Обучающая выборка содержит пары “входные данные - желаемый выход” (или метка класса). Модель учится отображать входные данные на соответствующие выходы на основе этих пар.

Задачи:

Классификация: Предсказание категории (спам/не спам, кошка/собака). Пример: распознавание цифр с вашего скриншота.

Регрессия: Предсказание числа (цена, температура, вероятность).

2. Обучение без учителя

Обучающая выборка содержит только входные данные без соответствующих меток или желаемых выходов. Найти скрытые структуры, паттерны и закономерности в данных.

Задачи:

Кластеризация: Разделение данных на группы (кластеры) по схожести. Пример: сегментация клиентов.

Понижение размерности: Упрощение данных без потери важной информации.

3. Обучение с подкреплением

Агент учится, взаимодействуя со средой и получая "награды" за правильные действия.

Пример: AlphaGo [1].

Как работает ML? Жизненный цикл проекта

I. Процесс машинного обучения

1. Сбор и подготовка данных: "Мусор на входе — мусор на выходе".
2. Разведочный анализ и визуализация: Поиск аномалий, закономерностей, разделение данных на обучающую и тестовую выборки.
3. Выбор и обучение модели.
4. Оценка качества модели: Метрики (точность, ошибка и т.д.).
5. Развертывание и мониторинг: Как модель используется в реальном мире.

II. Переобучение и недообучение

Недообучение: Модель слишком простая, плохо учится даже на тренировочных данных. Аналогия: пытаться сдать экзамен, прочитав только оглавление учебника.

Переобучение: Модель выучила тренировочные данные слишком хорошо, включая их шум и случайности, и плохо работает на новых данных. Аналия: зазубрил билеты, а на экзамене попались другие вопросы.

Заключение

Машинное обучение сформировалось как целостная методологическая парадигма, основанная на системном извлечении знаний из данных. Ключевые концепции — от базовых терминов данных, признаков и целевых переменных до процессов обучения и прогнозирования — образуют взаимосвязанный каркас, лежащий в основе любой практической реализации методов машинного обучения.

Важно подчеркнуть, что освоение машинного обучения требует не только понимания алгоритмов, но и развития особого типа мышления — способности критически оценивать качество данных, корректно формулировать целевую переменную и интерпретировать результаты моделирования в предметной области.

Перспективы развития поля состоят в углублении теоретических основ искусственного интеллекта, создании эффективных алгоритмов и разработке методов обучения на малых данных.

Дальнейшее погружение в дисциплину потребует изучения конкретных алгоритмических реализаций, методов валидации моделей и практического освоения инструментов реализации.

Литература

1. *Лапань М.* Глубокое обучение с подкреплением. AlphaGo и другие технологии. – "Издательский дом" Питер"", 2020.
2. *Алханов А. А.* Машинное обучение и его применение в современном мире //Проблемы науки. – 2021. – №. 7 (66). – С. 25-27.
3. *Флах П.* Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных. – Litres, 2022.
4. *Рашка С.* Python и машинное обучение. – Litres, 2022.
5. *Серрано Л.* Грокаем машинное обучение. – "Издательский дом" Питер"", 2024.