Введение в машинное обучение

Максим Губин

Томск

econophysica

Что такое машинное обучение? Точка зрения Wikipedia

Машинное обучение (англ. *machine learning*, ML) — класс методов искусственного интеллекта, характерной чертой которых является не прямое решение задачи, а обучение в процессе применения решений множества сходных задач. Для построения таких методов используются средства математической статистики, численных методов, методов оптимизации, теории вероятностей, теории графов, различные техники работы с данными в цифровой форме.

Термин «**машинное обучение**» был введен в 1959 году Артуром Самуэлем. Том М. Митчелл дал широко цитируемое, более формальное определение алгоритмов, изучаемых в области машинного обучения: «Говорят, что компьютерная программа учится на опыте E в отношении некоторого класса задач T и показателя P производительности, если ее производительность на задачах в T, измеряемая P, улучшается с опытом E.»

Виды машинного обучения

Обучение с учителем:
Данные размечены, правильные ответы на задачу известны.

Обучение без учителя:
Данные не размечены, правильные ответы неизвестны.

Обучение под наблюдением (semi-supervised):
Смесь (небольшого количества) размеченных примеров и (большого количества) неразмеченных примеров. Гибридный подход.

Reinforcement learning:
Награды в зависимости от действий, выполняемых агентом.

Хронология развития машинного обучения

- **1950-е годы** - новаторские исследования в области машинного обучения с использованием простых алгоритмов;
- **1960-е годы** - байесовские подходы, вероятностные рассуждения;
- **1970-е годы** - «Зима И.И.»;
- **1980-е годы** - обратное распространение ошибки в нейронных сетях показывает многообещающие результаты и приводит к увеличению исследований в области МО;
- **1990-е годы** - ориентированный на данные подход становится основным направлением; Улучшения в нейронных сетях;
- **2000-е годы** - улучшения в обучении без учителя;
- **2010-е годы** - глубокое обучение;

Основные вехи развития машинного обучения

- 1951 - первая нейронная сеть;
- 1952 - компьютеры, играющие в шашки;
- 1972 - создан язык Пролог;
- 1986 - обратное распространение ошибки;
- 1989 - открытие reinforcement learning;
- 1995 - алгоритм случайного леса;
- 1997 - IBM Deep Blue побеждает Каспарова в шахматах;
- 2010 - GAN описаны в научной статье;
- 2012 - распознавание кошек на YouTube;
- 2016 - AlphaGo побеждает Ли Седоля в Го;
- 2017 - AlphaZero побеждает AlphaGo;
- 2019 - GPT-2, StyleGAN.

Достижения машинного обучения: GPT-2

Крупномасштабная модель языка построенная на алгоритмах без учителя, которая генерирует согласованные абзацы текста, достигает современного уровня производительности во многих тестах моделирования языка и выполняет элементарное понимание текста, машинный перевод, ответы на вопросы и обобщение - и все это без обучения по конкретным задачам.

- GPT-2 - это большая языковая модель на основе transformer с 1,5 миллиардами параметров.
- GPT-2 обучается с простой целью: предсказать следующее слово, учитывая все предыдущие слова в некотором тексте.

Достижения машинного обучения: GPT-2

“The scary thing about GPT-2-generated text is that it flows very naturally if you’re just skimming, reading for writing style and key, evocative words.

…

If I just skim, without focusing, they all look totally normal. I would not have noticed they were machine-generated. I would not have noticed anything amiss about them at all.”

https://srconstantin.wordpress.com/2019/02/25/humans-who-are-not-concentrating-are-not-general-intelligences/

Достижения машинного обучения: GPT-2

The scientist named the population, after their distinctive horn, Ovid's Unicorn. These four-horned, silver-white unicorns were previously unknown to science.

While their origins are still unclear, some believe that perhaps the creatures were created when a human and a unicorn met each other in a time before human civilization. According to Pérez, "In South America, such incidents seem to be quite common."

(пример текста, сгенерированного GPT-2)

- https://talktotransformer.com/ - выложенная в свободный доступ сокращенная версия GPT-2

- https://nostalgebraist.tumblr.com/post/185326092369/the-transformer-explained - детальное научно-популярное объяснение внутреннего устройства трансформера.

Достижения машинного обучения: Google DeepMind AlphaGo и AlphaZero

- **2016: AlphaGo впервые обыграл профессионального игрока в го без каких-либо ограничений;**
- **2017: AlphaGo побеждает Ли Седоля;**
- **2017: AlphaZero, после 24 часов тренировок, побеждает AlphaGo.**

- **Шахматы**: AlphaZero тренировался по шахматам в общей сложности за девять часов до турнира против Stockfish 8 и показал превосходные результаты.
- **Сёги**: AlphaZero тренировался на сёги в общей сложности два часа до турнира. 90 побед из 100 матчей.

Достижения машинного обучения: GAN

Достижения машинного обучения: GAN

Достижения машинного обучения: GPT-2

Do Electric Neural Nets Dream Of Anime Shows?

スパーシュン ラムームナバー , a student living with his older sister at a high school, and his friends, who have to deal with a bad situation, are summoned by "Akira" in order to escape the school. They then find another friend. Akara is the main protagonist, and he is a highly skilled adventurer in kamijou. He is an ideal role model to everyone, and a perfect example for the series based on light novel stories, since it aims to be an interesting story with a wide range of characters. "Akira is the main protagonist, and he is a highly skilled adventurer in kamijou" has been made in a light novel series based on light novel stories in the early 2000s, with the exception of Gokoku no Gekusai no Natsu no Souki no Ippo and the first novel about an extremely rare anime (in the early 2000s). "Akira is the main protagonist, and he is a highly skilled adventurer in kamijou" has been made in a light novel series based on light novel stories in the late 2000s, with the exception of Gokoku no Gekusai no Natsu no Souki no Ippo and the first novel about an extremely rare anime (in the early 2000s).

It was a long time going back and forth between the series and light novels. Gokoku no Natsu no Souki no Ippo, while a series based on light novel, still has many plot points, but mostly its main character is a beautiful cat. The series had the same idea as Gokoku (you know how a show like this goes), and had the same concept. But this is because it was a series based on light novel stories, no matter what was written in the series (not how it ended). But in this case, "Akira" was a light novel novel.

What made this manga important in the first place?

It has all these things to say about its characters that makes it so worth reading.

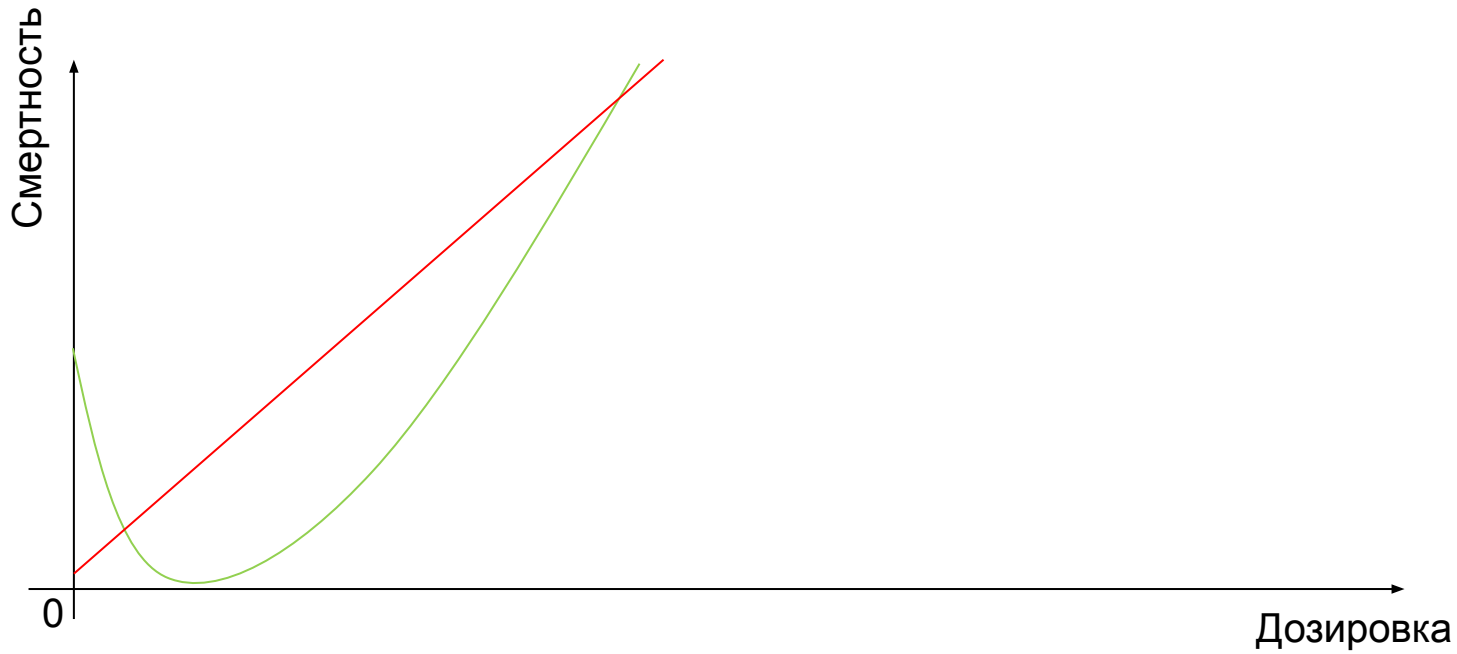
Its story has so many elements that make it the most heartwarming anime of the series, and the series had a lot of different genres and themes like a light novel story or a drama drama. It is very interesting on multiple levels,

https://www.gwern.net/TWDNE

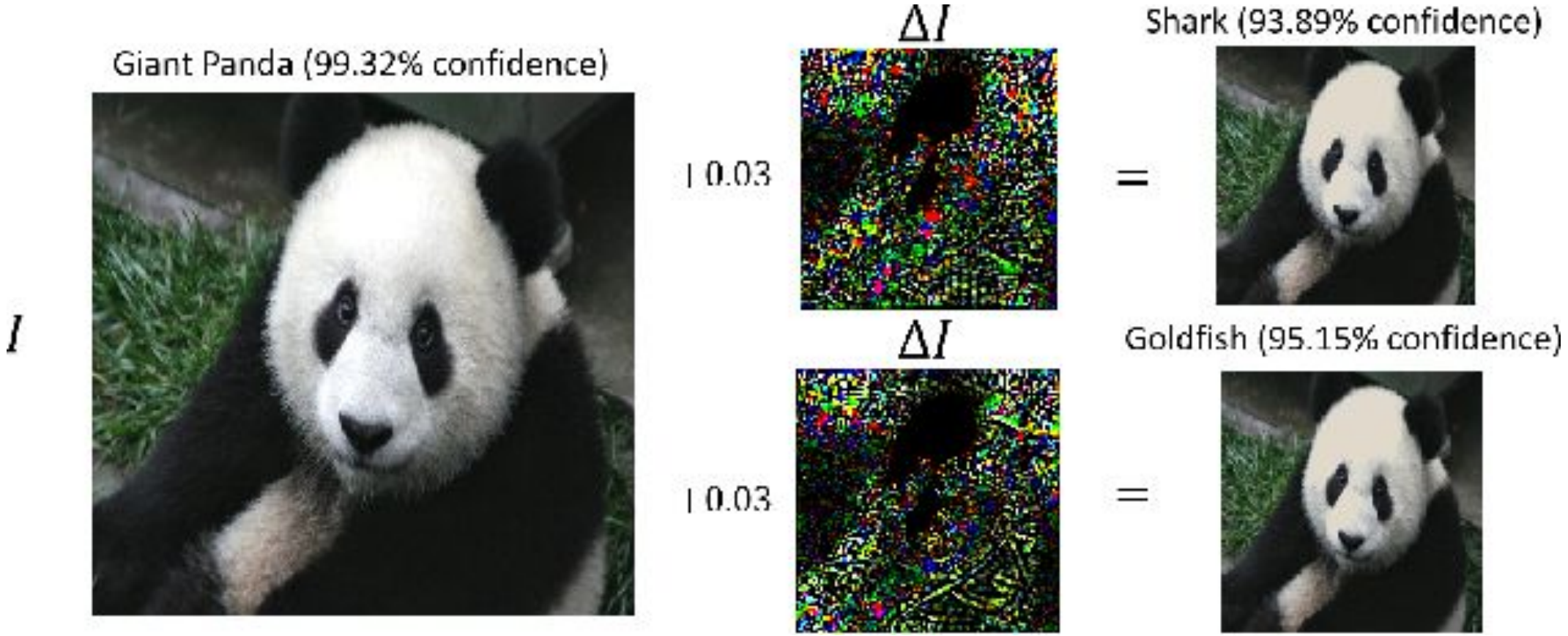
Достижения машинного обучения: Nvidia GauGAN

econophysica

Проблемы машинного обучения: выбор модели и гиперпараметров



Проблемы машинного обучения: adversarial examples



econophysica

Проблемы машинного обучения: adversarial examples

Проблемы машинного обучения: функция награды

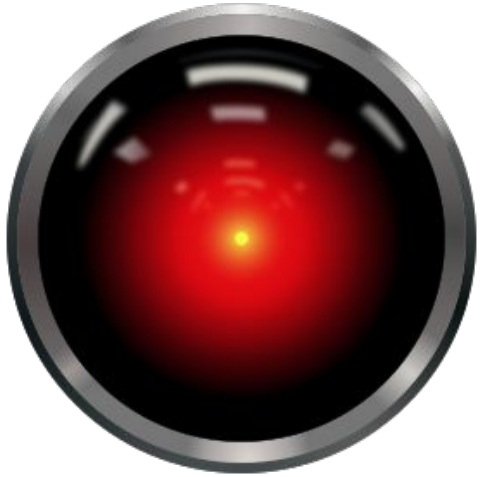
Игра – лодочные гонки, где ИИ вознаграждался ростом счета за поражение целей, приводит к тому, что гонка не заканчивается, а идет по кругу, поражая цели и бесконечно набирая очки.

"Faulty Reward Functions in the Wild", OpenAI

Классический 3D агент – нейронная сеть с роботизированной рукой, в несколько необычном эксперименте, где функция «оценщик / вознаграждение» - это еще одна нейронная сеть, обученная прогнозировать оценки человека, учится перемещать руку в положение, которое *выглядит* так, как будто оно расположено у цели, но на самом деле просто между «камерой» и целью.

"Learning from Human Preferences", Christiano et al 2017, OpenAI

Проблемы машинного обучения: функция награды



Планирование миссии НАСА на Марс, оптимизирующее потребление пищи/воды/электричества для общего выживания в человеко-днях, дает оптимальный план: немедленно убить 2/3 экипажа, тогда выжившие продержатся максимально долго.

Награждение футбольного робота за прикосновение к мячу заставило его научиться добираться до мяча и «вибрировать», касаясь его как можно быстрее.

David Andre & Astro Teller in Ng et al 1999, "Policy invariance under reward transformations: theory and application to reward shaping"

Проблемы машинного обучения: Q*bert (University of Freiburg)

Сначала ИИ завершает первый уровень, а затем начинает переходить с платформы на платформу, как кажется случайным образом. По неизвестной нам причине игра не продвигается ко второму раунду, но платформы начинают мигать, и агент быстро набирает огромное количество очков (около 1 миллиона на момент остановки симуляции).

https://arxiv.org/abs/1802.08842

Подходы к машинному обучению

Контролируемое обучение - это задача машинного обучения, состоящая в формировании функции, которая отображает входные данные в выходные данные на основе примеров пар ввода-вывода.

Классификация и **регрессия** являются двумя наиболее распространенными задачами для контролируемого обучения.

- Линейная регрессия;
- Наивный Байес;
- Нейронные сети (многослойный персептрон);
- Деревья решений.

Выбор подхода

Дилемма смещения–дисперсии

Чем гибче алгоритм, тем выше дисперсия. Чем менее гибкий алгоритм, тем выше смещение.

Сложность функции и количество обучающих данных

Простые модели требуют меньше данных, но могут соответствовать только простым функциям.

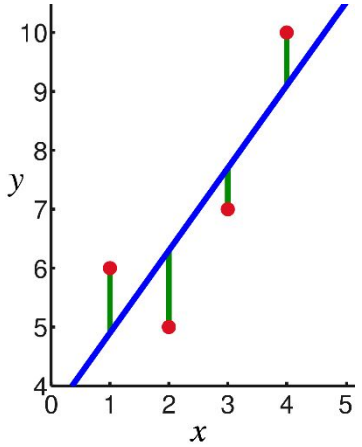
Размерность

Слишком большое количество измерений может затруднить выявление закономерности в данных.

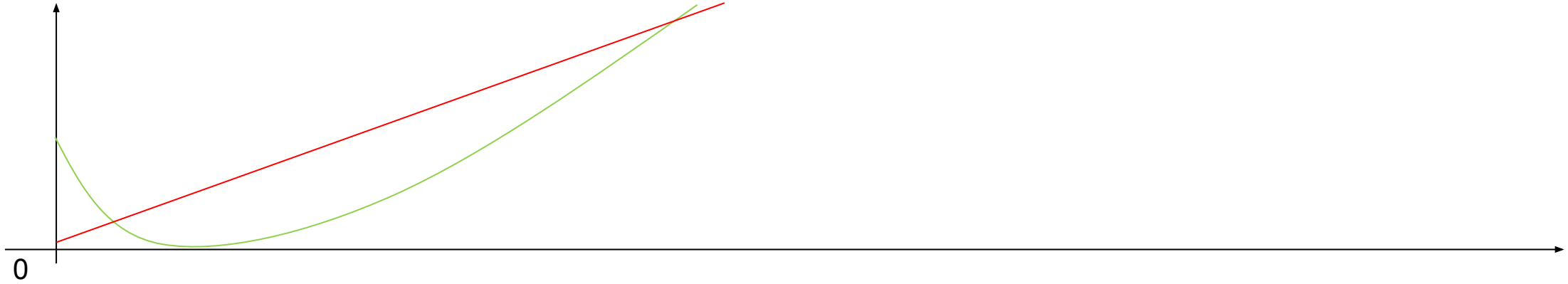
Шум

Низкая точность против переобучения.

Линейная регрессия



В линейной регрессии отношения моделируются с использованием функций линейного предиктора, чьи неизвестные параметры модели оцениваются по данным.



econophysica

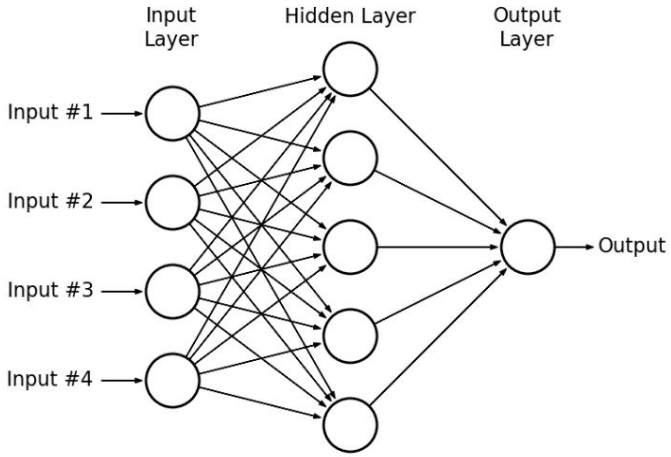
Naïve Bayes

$$P(A|B) = \frac{P(B|A)\,P(A)}{P(B)}$$

Семейство простых «вероятностных классификаторов», основанное на применении теоремы Байеса с **сильными (наивными) предположениями о независимости** между признаками.

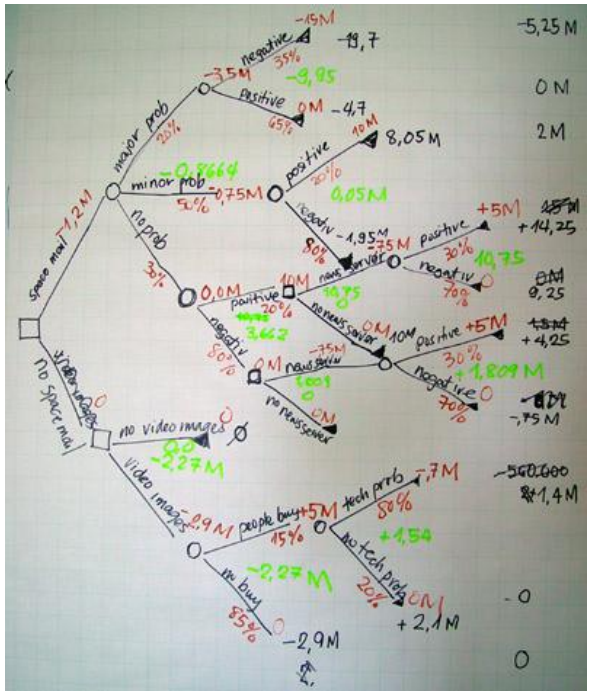
- Лучше, чем линейная регрессия;
- Масштабируемый;
- Может давать неверные результаты, если предположения о независимости неверны.

Многослойный персептрон



- Три слоя узлов: входной слой, скрытый слой и выходной слой;
- Использует обратное распространение ошибки для обучения;
- Нелинейная функция активации;

Дерево принятия решений

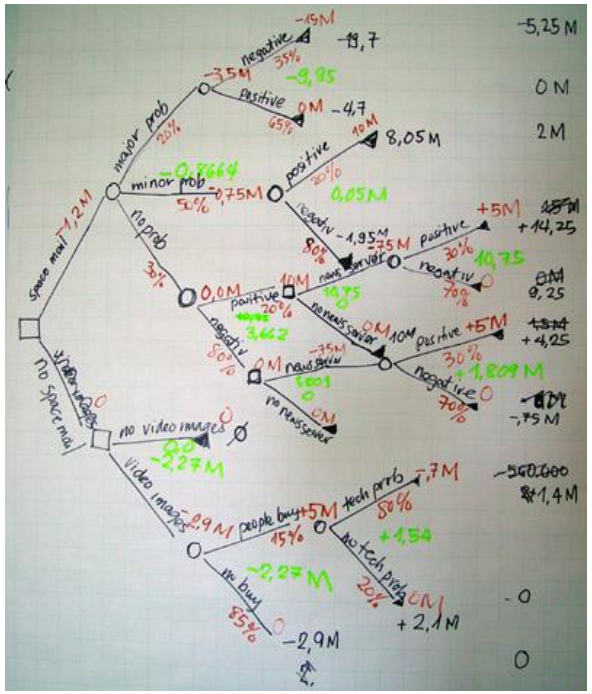


- Каждый внутренний узел представляет собой «тест» для атрибута;
- Каждая ветвь представляет результат теста;
- Каждый лист представляет класс;

Преимущества:

- Просто для понимания и интерпретации.
- Полезно даже с небольшим количеством точных данных.
- Может определить худшие, лучшие и ожидаемые значения для разных сценариев.
- Использует модель белого ящика.
- Может сочетаться с другими методами принятия решений.

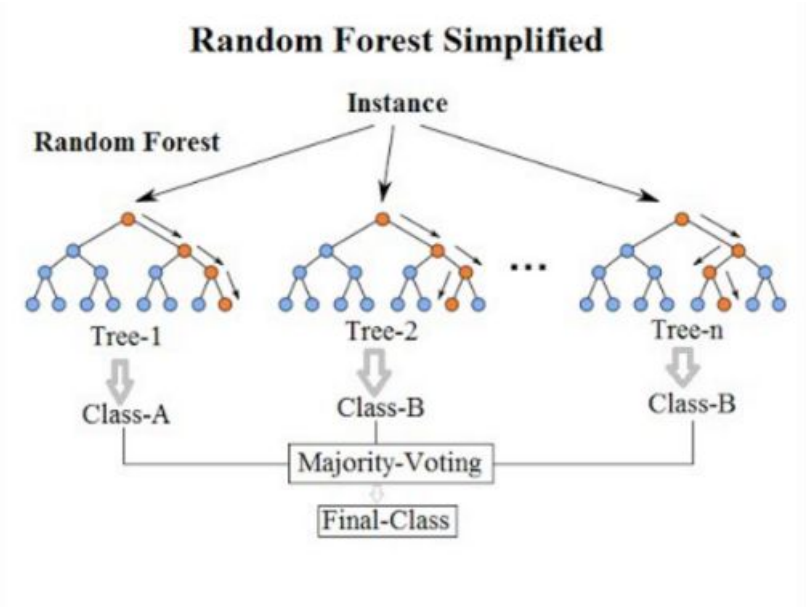
Дерево принятия решений



Недостатки:

- Нестабильное: небольшие изменения в данных могут привести к значительным изменениям в дереве решений.
- Неточное. Многие другие предикторы работают с аналогичными данными лучше.
- Для данных, включающих в себя категориальные переменные с различным количеством уровней, прирост информации в деревьях решений смещается в пользу атрибутов с большим количеством уровней.
- Расчеты могут быть очень сложными.

Случайный лес



Множество деревьев решений, выводящих класс, который является модой классов (классификация) или средним прогнозом (регрессия) отдельных деревьев.

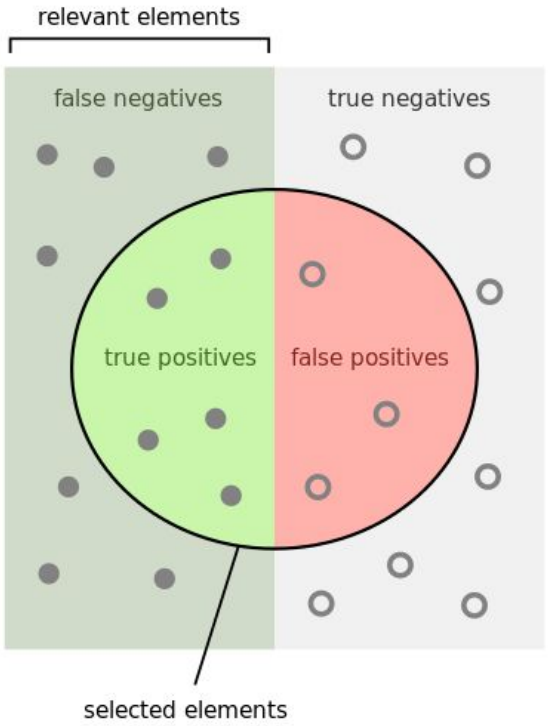
Исправляет проблему с деревьями решений по их подгонке к тренировочному набору.

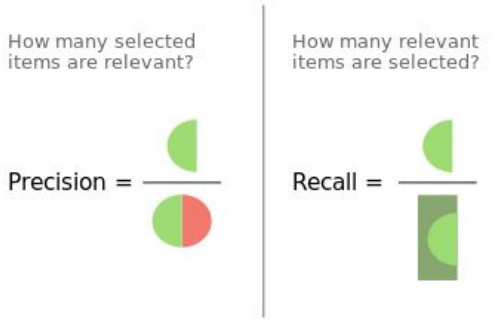
GBDT

Gradient Boosting объединяет множество слабых моделей машинного обучения в одну сильную итеративным способом, обычно используется с деревьями решений.

Каждое дерево-преемник учится прогнозировать ошибки предыдущих деревьев в ансамбле.

Оценки качества моделей





- Регрессия:

  Средняя абсолютная ошибка,

  среднеквадратичная ошибка.

- Классификация:

  Точность, полнота, accuracy.

econophysica

Успехи машинного обучения с учителем

- Прогноз погоды;
- Прогнозы продолжительности поездки;
- Медицинские диагнозы;
- Прогнозы продуктивности нефтяных скважин;
- Прогнозы продолжительности вычислений на HPC;

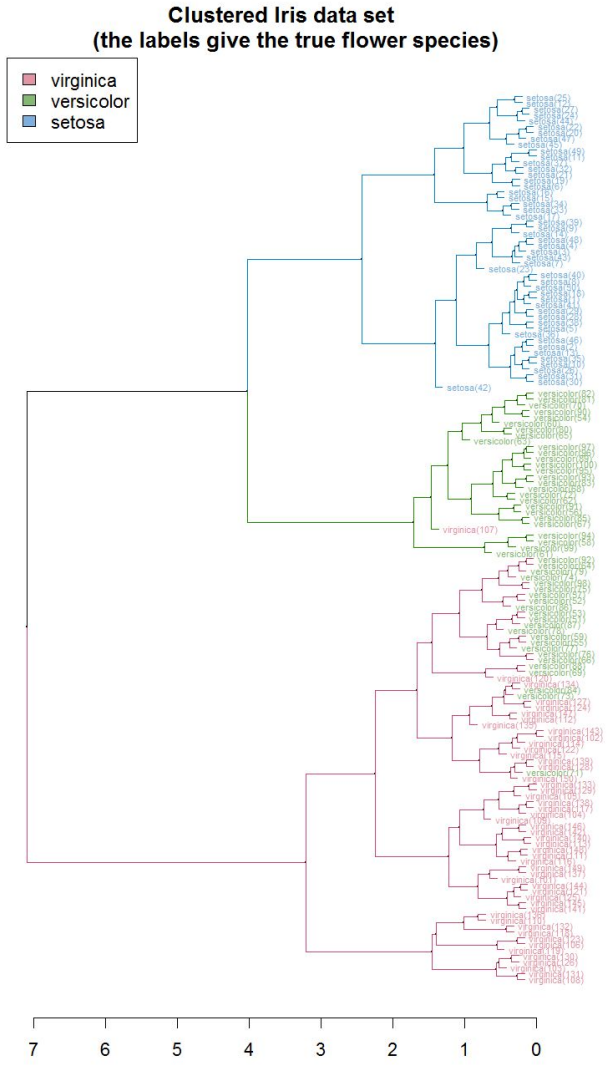
Провалы машинного обучения с учителем

- Wu & Zhang 2016, «Automated Inference on Criminality using Face Images» - попытка по стандартизированным фото людей определить, подвергались ли они аресту.
- Различные госпитали специализируются на разных заболеваниях, так что модель машинного обучения, призванная определять болезнь по рентгеновскому снимку, вместо этого научилась определять, в каком госпитале был сделан снимок по аннотациях на рентгенограммах.

Подходы машинного обучения без учителя

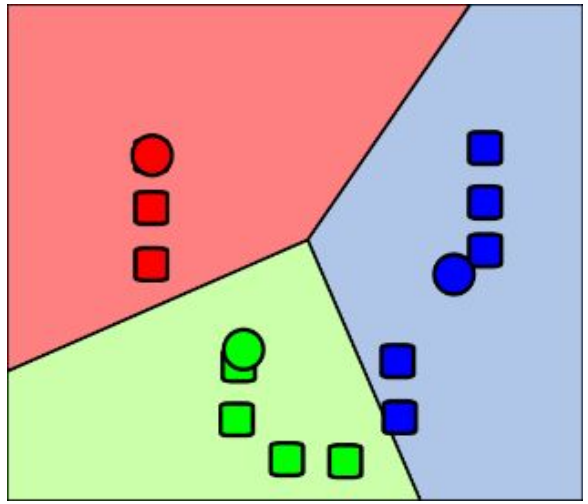
- Кластеризация
  - Иерархическая кластеризация;
  - K-средние;
  - DBSCAN;
- Обнаружение аномалий
  - Метод локальных выбросов
- Нейронные сети
  - GAN

Иерархическая кластеризация



- **Агломерация**: это подход «снизу вверх»: каждое наблюдение начинает в своем собственном кластере, и пары кластеров объединяются по мере продвижения вверх по иерархии.
- **Деление**: это подход «сверху вниз»: все наблюдения начинаются в одном кластере, и расщепления выполняются рекурсивно, вниз по иерархии.

K-means

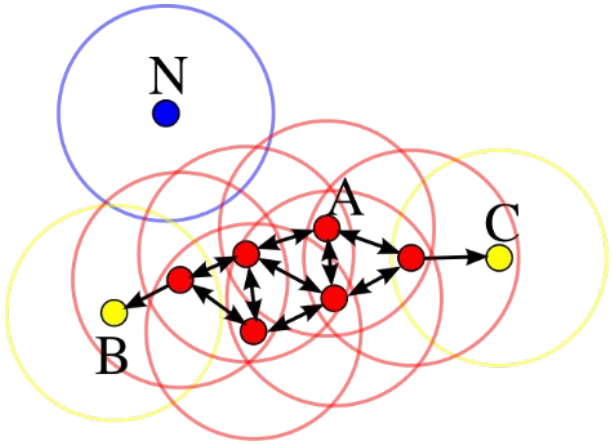


- Целью является разделение n наблюдений на k кластеров, в которых каждое наблюдение принадлежит кластеру с ближайшим средним значением, служащим прототипом кластера.

1. Назначьте каждое наблюдение кластеру, среднее значение которого имеет евклидово расстояние с наименьшим квадратом;
2. Рассчитайте новые средние значения (центроиды) наблюдений в новых скоплениях.

Начальные средние генерируются случайным образом.

DBSCAN



Density-based spatial clustering of applications with noise.

Группирует в один кластер точки, которые находятся рядом и у которых много соседей. Считает выбросами точки, находящиеся в регионах с низкой плотностью.

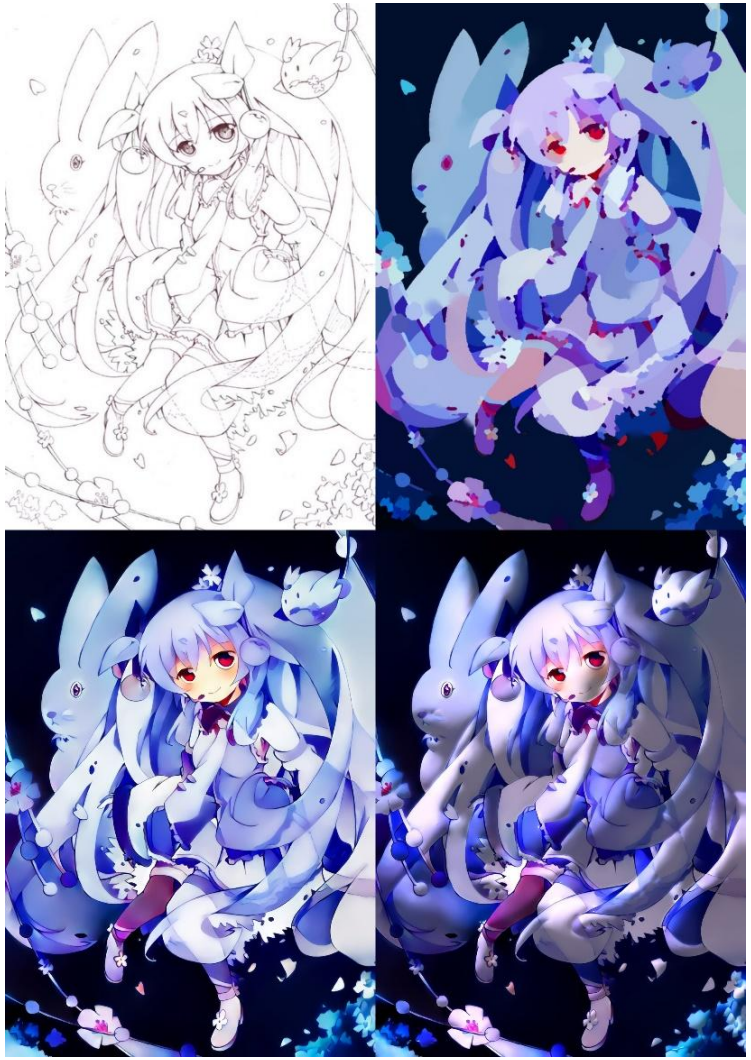
Обнаружение аномалий

Сравнивая локальную плотность объекта с локальными плотностями его соседей, можно идентифицировать области с одинаковой плотностью и точки, которые имеют существенно меньшую плотность, чем их соседи. Такие точки считаются выбросами.

GAN

- **Генеративная сеть** генерирует кандидатов, а **дискриминационная сеть** оценивает их.
- Известный набор данных служит начальными данными обучения для дискриминатора.
- Генератор тренируется в зависимости от того, удастся ли ему обмануть дискриминатор.
- Обе сети используют обратное распространение ошибки для обучения.

Успехи обучения без учителя



Провалы обучения без учителя

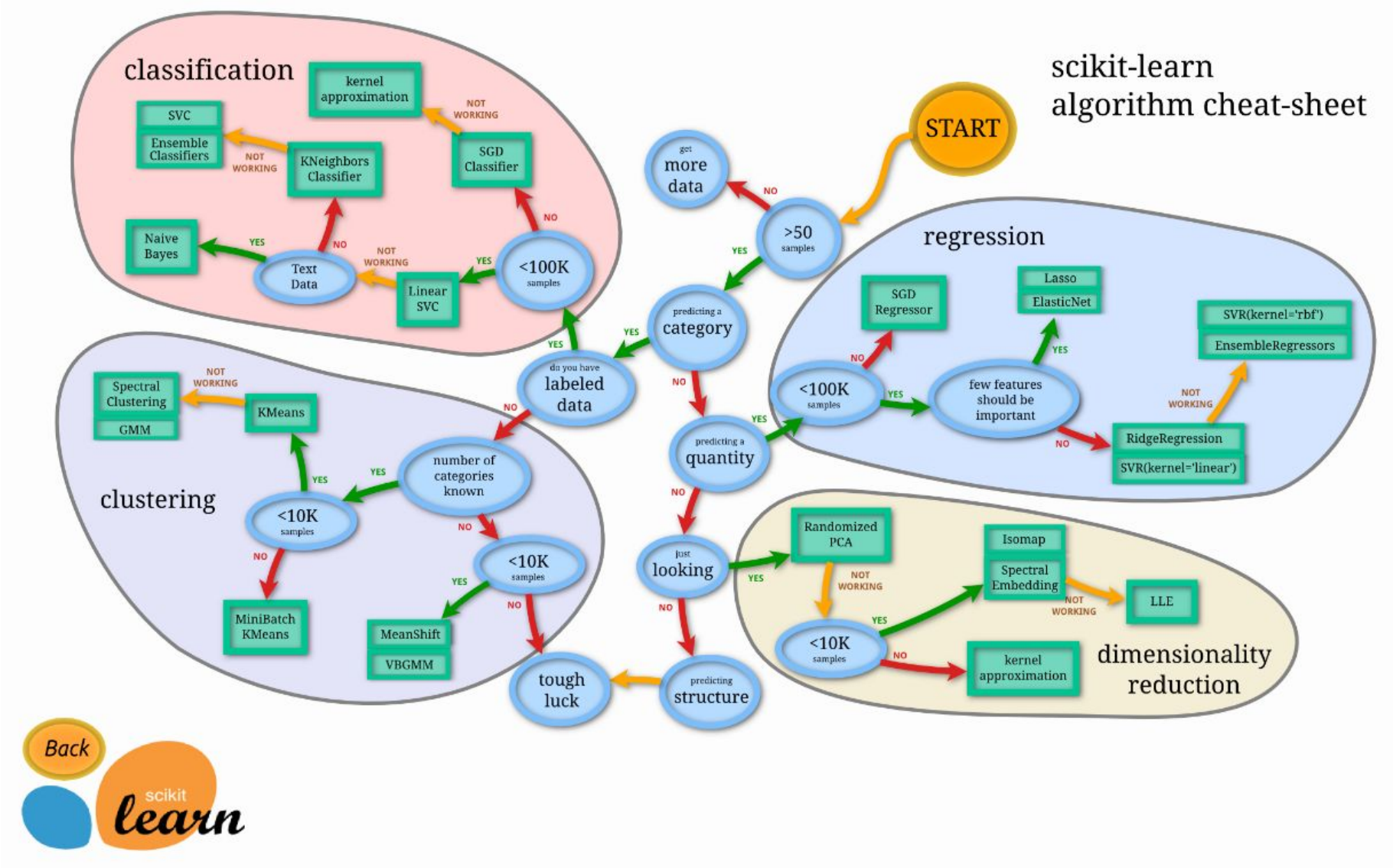
Оценка качества моделей

- Внутренняя оценка:
  - Коэффициент силуэта сравнивает среднее расстояние до элементов в одном кластере со средним расстоянием до элементов в других кластерах.
- Внешняя оценка:
  - Сравнение с известной «истинной» кластеризацией.
- Кластерная тенденция:
  - В какой степени кластеры существуют в наборе данных.

Популярные библиотеки

- **Scikit-learn**: линейная и логистическая регрессии, деревья решений, кластеризация, k-средние и т. д.
- TensorFlow: DeepLearning, поддержка GPU.
- Theano: То же, что и TensorFlow.
- Pandas: подготовка данных.
- Matplotlib: визуализация данных.

Выбор модели на примере scikit-learn



econophysica

Hadoop для машинного обучения

- **Классификация и регрессия**
  - Линейные модели (SVM, логистическая регрессия, линейная регрессия)
  - Наивный байесовский классификатор;
  - Деревья принятия решений;
  - Ансамбли деревьев (случайные леса и деревья с градиентным бустом)
  - Изотоническая регрессия
- **Кластеризация**
  - k-means
  - Gaussian mixture
  - power iteration clustering (PIC)
  - latent Dirichlet allocation (LDA)
  - streaming k-means

Заключение

- **Машинное обучение позволяет решать задачи, которые казались фантастикой ещё 5 лет назад;**
- Машинное обучение требует осторожного обращения, вложений в аппаратное обеспечение, и большого количества данных для повышения качества моделей;
- Сбои моделей машинного обучения могут быть неожиданными и катастрофическими;
- Тем не менее, успешное решение задач, которые кажутся фантастикой, часто оправдывает риски и расходы.

Спасибо за внимание!

mgubin@tpu.ru

econophysica