МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

Кафедра радиофизики и цифровых медиа технологий

Методы анализа влияния входных признаков при разработке моделей машинного обучения с учителем

Курсовая работа

Раковца Андрея Владимировича

студента 3 курса, специальность

«прикладная информатика»

Научный руководитель:

старший преподаватель

Курочкин А.В.

Минск,2020

Введение

Одна из фундаментальных проблем машинного обучения в том, что обученные модели работают как "черный ящик". Машинное обучение в целом сводится к тому, что мы какую-то очень гибкую и настраиваемую функцию подгоняем под такой вид, который хорошо описывает какие-то имеющиеся данные. Например, мы знаем, как формируется нейронная сеть, знаем, как происходит её обучение, но после того, как она обучена, её поведение очень сложно интерпретировать - она может имеющиеся у нас данные описывать просто идеально, но мы всё равно не будем знать, какие именно принципы лежат в полученном функциональном преобразовании. Т.е. мы знаем выходной результат, но мы не знаем, почему мы получили именно такой результат, а не какой-то другой.

Задача - попытаться хоть как-то объяснить поведение таких моделей. Одна из сторон медали - попытаться для начала понять, какие из входных признаков являются наиболее значимыми по сравнению с другими. Есть модели, в которых эта задача решается "из коробки" просто из-за специфики построения модели - например, деревья принятия решений или случайные леса. Есть другие модели, типа нейронных сетей, в которых эта задача вообще никак не решается.

Рассмотрим бинарное дерево, в котором:

каждой внутренней вершине v приписана функция (или предикат)

βv : X →{0, 1};

каждой листовой вершине v приписан прогноз cv ∈ Y (в случае с классификацией листу также может быть приписан вектор вероятностей).

Рассмотрим теперь алгоритм a(x), который стартует из корневой вершины v0 и вычисляет значение функции βv0. Если оно равно нулю, то алгоритм переходит в левую дочернюю вершину, иначе в правую, вычисляет значение предиката в новой вершине и делает переход или влево, или вправо. Процесс продолжается, пока не будет достигнута листовая вершина; алгоритм возвращает тот класс, который приписан этой вершине. Такой алгоритм называется бинарным решающим деревом.

На практике в большинстве случаев используются одномерные предикаты βv, которые сравнивают значение одного из признаков с порогом:

βv (x; j, t) = [xj < t].

Существуют и многомерные предикаты, например:

• линейные βv(x) = [⟨w, x⟩ < t];

• метрические βv(x) = [ρ(x, xv) < t], где точка xv является одним из объектов выборки любой точкой признакового пространства.

Многомерные предикаты позволяют строить ещё более сложные разделяющие поверхности, но очень редко используются на практике — например, из-за того, что усиливают и без того выдающиеся способности деревьев к переобучению. Далее мы будем говорить только об одномерных предикатах.

Легко убедиться, что для любой выборки можно построить решающее дерево, не допускающее на ней ни одной ошибки — даже с простыми одномерными предикатами можно сформировать дерево, в каждом листе которого находится ровно по одному объекту выборки. Скорее всего, это дерево будет переобученным и не сможет показать хорошее качество на новых данных. Можно было бы поставить задачу поиска дерева, которое является минимальным (с точки зрения количества листьев) среди всех деревьев, не допускающих ошибок на обучении — в этом случае можно было бы надеяться на наличие у дерева обобщающей способности. К сожалению, эта задача является NP-полной, и поэтому приходится ограничиваться жадными алгоритмами построения дерева.

Опишем базовый жадный алгоритм построения бинарного решающего дерева. Начнем со всей обучающей выборки X и найдем наилучшее ее разбиение на две части R1(j, t) = {x | xj < t} и R2(j, t) = {x | xj ≥ t} с точки зрения заранее заданного функционала качества Q(X, j, t). Найдя наилучшие значения j и t, создадим корневую вершину дерева, поставив ей в соответствие предикат [xj < t]. Объекты разобьются на две части — одни попадут в левое поддерево, другие в правое. Для каждой из этих подвыборок рекурсивно повторим процедуру, построив дочерние вершины для корневой, и так далее. В каждой вершине мы проверяем, не выполнилось

ли некоторое условие останова — и если выполнилось, то прекращаем рекурсию и объявляем эту вершину листом. Когда дерево построено, каждому листу ставится в соответствие ответ. В случае с классификацией это может быть класс, к которому относится больше всего объектов в листе, или вектор вероятностей (скажем, вероятность класса может быть равна доле его объектов в листе). Для регрессии это может быть среднее значение, медиана или другая функция от целевых переменных объектов в листе. Выбор конкретной функции зависит от функционала качества в исходной задаче.

Решающие деревья могут обрабатывать пропущенные значения — ситуации, в которых для некоторых объектов неизвестны значения одного или нескольких признаков. Для этого необходимо модифицировать процедуру разбиения выборки в вершине, что можно сделать несколькими способами.

После того, как дерево построено, можно провести его стрижку (pruning) — удаление некоторых вершин с целью понижения сложности и повышения обобщающей способности. Существует несколько подходов к стрижке, о которых мы немного упомянем ниже.

Таким образом, конкретный метод построения решающего дерева определяется:

1. Видом предикатов в вершинах;

2. Функционалом качества Q(X, j, t);

3. Критерием останова;

4. Методом обработки пропущенных значений;

5. Методом стрижки.

Также могут иметь место различные расширения, связанные с учетом весов объектов, работой с категориальными признакам и т.д. Ниже мы обсудим варианты каждого из перечисленных пунктов.

При построении дерева необходимо задать функционал качества, на основе которого осуществляется разбиение выборки на каждом шаге. Обозначим через Rm множество объектов, попавших в вершину, разбиваемую на данном шаге, а через Rℓ и Rr — объекты, попадающие в левое и правое поддерево соответственно при заданном предикате. Мы будем использовать функционалы следующего вида:

Q(Rm, j, s) = H(Rm) − |Rℓ | |Rm| H(Rℓ) − |Rr| |Rm| H(Rr).

Здесь H(R) — это критерий информативности (impurity criterion), который оценивает качество распределения целевой переменной среди объектов множества R. Чем меньше разнообразие целевой переменной, тем меньше должно быть значение критерия информативности — и, соответственно, мы будем пытаться минимизировать его значение. Функционал качества Q(Rm, j, s) мы при этом будем максимизировать. Как уже обсуждалось выше, в каждом листе дерево будет выдавать константу — вещественное число, вероятность или класс. Исходя из этого, можно предложить оценивать качество множества объектов R тем, насколько хорошо их целевые переменные предсказываются константой (при оптимальном выборе этой константы):

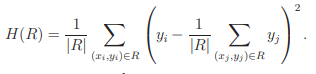


где L (y, c) — некоторая функция потерь. Далее мы обсудим, какие именно критерии информативности часто используют в задачах регрессии и классификации.

Регрессия Как обычно, в регрессии выберем квадрат отклонения в качестве функции потерь. В этом случае критерий информативности будет выглядеть как



Как известно, минимум в этом выражении будет достигаться на среднем значении целевой переменной. Значит, критерий можно переписать в следующем виде:



Мы получили, что информативность вершины измеряется её дисперсией — чем ниже разброс целевой переменной, тем лучше вершина. Разумеется, можно использовать и другие функции ошибки L — например, при выборе абсолютного отклонения мы получим в качестве критерия среднее абсолютное отклонение от медианы.

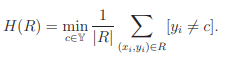
Обозначим через pk долю объектов класса k (k ∈ {1, . . . , K}), попавших в вершину R:



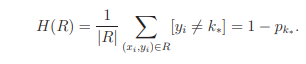
Через k∗ обозначим класс, чьих представителей оказалось больше всего среди объектов, попавших в данную вершину: .

Ошибка классификации

Рассмотрим индикатор ошибки как функцию потерь:

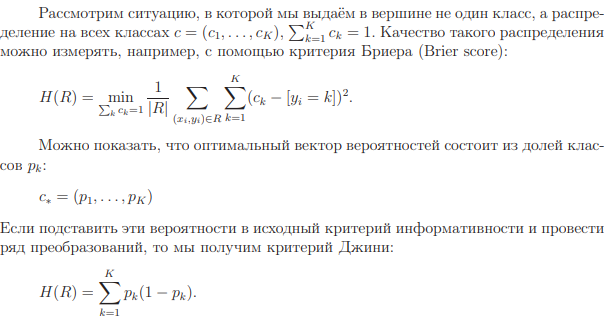


Легко видеть, что оптимальным предсказанием тут будет наиболее популярный класс k∗ — значит, критерий будет равен следующей доле ошибок:

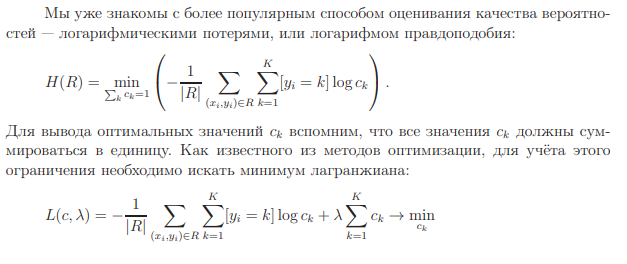


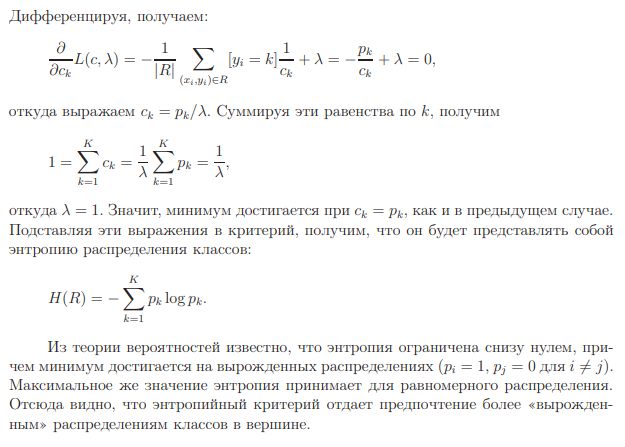
Данный критерий является достаточно грубым, поскольку учитывает частоту pk∗ лишь одного класса.

Критерий Джини



Энтропийный критерий





Критерии останова

Можно придумать большое количестве критериев останова. Перечислим некоторые ограничения и критерии:

• Ограничение максимальной глубины дерева.

• Ограничение минимального числа объектов в листе.

• Ограничение максимального количества листьев в дереве.

• Останов в случае, если все объекты в листе относятся к одному классу.

• Требование, что функционал качества при дроблении улучшался как минимум на s процентов.

С помощью грамотного выбора подобных критериев и их параметров можно существенно повлиять на качество дерева. Тем не менее, такой подбор является трудозатратным и требует проведения кросс-валидации.

Методы стрижки дерева

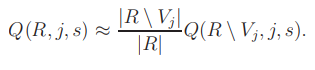
Стрижка дерева является альтернативой критериям останова, описанным выше. При использовании стрижки сначала строится переобученное дерево (например, до тех пор, пока в каждом листе не окажется по одному объекту), а затем производится оптимизация его структуры с целью улучшения обобщающей способности. Существует ряд исследований, показывающих, что стрижка позволяет достичь лучшего качества по сравнению с ранним остановом построения дерева на основе различных критериев. Тем не менее, на данный момент методы стрижки редко используются и не реализованы в большинстве библиотек для анализа данных. Причина заключается в том, что деревья сами по себе являются слабыми алгоритмами и не представляют большого интереса, а при использовании в композициях они либо должны быть переобучены (в случайных лесах), либо должны иметь очень небольшую глубину (в бустинге), из-за чего необходимость в стрижке отпадает. Одним из методов стрижки является cost-complexity pruning. Обозначим дерево, полученное в результате работы жадного алгоритма, через T0. Поскольку в каждом из листьев находятся объекты только одного класса, значение функционала R(T) будет минимально на самом дереве T0 (среди всех поддеревьев). Однако данный функционал характеризует лишь качество дерева на обучающей выборке, и чрезмерная подгонка под нее может привести к переобучению. Чтобы преодолеть эту проблему, введем новый функционал Rα(T), представляющий собой сумму исходного функционала R(T) и штрафа за размер дерева:



где |T| — число листьев в поддереве T, а α > 0 — параметр. Это один из примеров регуляризованных критериев качества, которые ищут баланс между качеством классификации обучающей выборки и сложностью построенной модели. Можно показать, что существует последовательность вложенных деревьев с одинаковыми корнями: TK ⊂ TK−1 ⊂ · · · ⊂ T0, (здесь TK — тривиальное дерево, состоящее из корня дерева T0), в которой каждое дерево Ti минимизирует критерий (5.1) для α из интервала α ∈ [αi , αi+1), причем 0 = α0 < α1 < · · · < αK < ∞. Эту последовательность можно достаточно эффективно найти путем обхода дерева. Далее из нее выбирается оптимальное дерево по отложенной выборке или с помощью кросс-валидации.

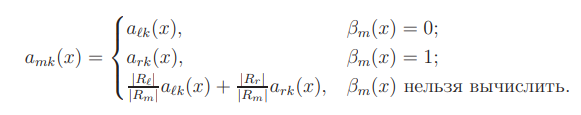
Обработка пропущенных значений

Одним из основных преимуществ решающих деревьев является возможность работы с пропущенными значениями. Рассмотрим некоторые варианты. Пусть нам нужно вычислить функционал качества для предиката β(x) = = [xj < t], но в выборке R для некоторых объектов не известно значение признака j — обозначим их через Vj . В таком случае при вычислении функционала можно просто проигнорировать эти объекты, сделав поправку на потерю информации от этого:



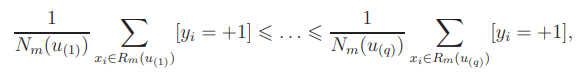
Затем, если данный предикат окажется лучшим, поместим объекты из Vj как в левое, так и в правое поддерево. Также можно присвоить им при этом веса

|Rℓ|/|R| в левом поддереве и |Rr|/|R| в правом. В дальнейшем веса можно учитывать, добавляя их как коэффициенты перед индикаторами [yi = k] во всех формулах. На этапе применения дерева необходимо выполнять похожий трюк. Если объект попал в вершину, предикат которой не может быть вычислен из-за пропуска, то прогнозы для него вычисляются в обоих поддеревьях, и затем усредняются с весами, пропорциональными числу обучающих объектов в этих поддеревьях. Иными словами, если прогноз вероятности для класса k в поддереве Rm обозначается через amk(x), то получаем такую формулу:



Другой подход заключается в построении суррогатных предикатов в каждой вершине. Так называется предикат, который использует другой признак, но при этом дает разбиение, максимально близкое к данному. Отметим, что нередко схожее качество показывают и гораздо более простые способы обработки пропусков — например, можно заменить все пропуски на ноль. Для деревьев также разумно будет заменить пропуски в признаке на числа, которые превосходят любое значение данного признака. В этом случае в дереве можно будет выбрать такое разбиение по этому признаку, что все объекты с известными значениями пойдут в левое поддерево, а все объекты с пропусками — в правое.

Учет категориальных признаков Самый очевидный способ обработки категориальных признаков — разбивать вершину на столько поддеревьев, сколько имеется возможных значений у признака (multi-way splits). Такой подход может показывать хорошие результаты, но при этом есть риск получения дерева с крайне большим числом листьев. Рассмотрим подробнее другой подход. Пусть категориальный признак xj имеет множество значений Q = {u1, . . . , uq}, |Q| = q. Разобьем множество значений на два непересекающихся подмножества: Q = Q1⊔Q2, и определим предикат как индикатор попадания в первое подмножество: β(x) = [xj ∈ Q1]. Таким образом, объект будет попадать в левое поддерево, если признак xj попадает в множество Q1, и в первое поддерево в противном случае. Основная проблема заключается в том, что для построения оптимального предиката нужно перебрать 2q−1 − 1 вариантов разбиения, что может быть не вполне возможным. Оказывается, можно обойтись без полного перебора в случаях с бинарной классификацией и регрессией [1]. Обозначим через Rm(u) множество объектов, которые попали в вершину m и у которых j-й признак имеет значение u; через Nm(u) обозначим количество таких объектов. 9 В случае с бинарной классификацией упорядочим все значения категориального признака на основе того, какая доля объектов с таким значением имеет класс +1:



после чего заменим категорию u(i) на число i, и будем искать разбиение как для вещественного признака. Можно показать, что если искать оптимальное разбиение по критерию Джини или энтропийному критерию, то мы получим такое же разбиение, как и при переборе по всем возможным 2q−1 − 1 вариантам.

***Ансамблевые методы*** — это парадигма машинного обучения, где несколько моделей (часто называемых «слабыми учениками») обучаются для решения одной и той же проблемы и объединяются для получения лучших результатов. Основная гипотеза состоит в том, что при правильном сочетании слабых моделей мы можем получить более точные и/или надежные модели.

Один слабый ученик

В машинном обучении, независимо от того, сталкиваемся ли мы с проблемой классификации или регрессии, выбор модели чрезвычайно важен, чтобы иметь какие-либо шансы получить хорошие результаты. Этот выбор может зависеть от многих переменных задачи: количества данных, размерности пространства, гипотезы распределения…

Слабое ***смещение (bias)*** и ***разброс (variance)*** модели, хотя они чаще всего изменяются в противоположных направлениях, являются двумя наиболее фундаментальными особенностями, ожидаемыми для модели. Действительно, чтобы иметь возможность «решить» проблему, мы хотим, чтобы в нашей модели было достаточно степеней свободы для разрешения базовой сложности данных, с которыми мы работаем, но мы также хотим, чтобы у нее было не слишком много степеней свободы, чтобы избежать ее высокого разброса и быть более устойчивой. Это хорошо известный **компромисс между смещением и разбросом**.



Иллюстрация компромисса между смещением и разбросом

В ансамблевой теории обучения мы вводим понятия ***слабых учеников*** (или ***базовых моделей***), которых можно использовать в качестве строительных блоков для проектирования более сложных моделей путем объединения нескольких из них. В большинстве случаев эти базовые модели работают сами по себе не так хорошо в связи с тем, что они имеют высокое смещение (например, модели с низкой степенью свободы), либо с тем, что имеют слишком большой разброс, чтобы быть устойчивыми (например, модели с высокой степенью свободы). Тогда идея ансамблевых методов состоит в том, чтобы попытаться уменьшить смещение и/или разброс таких слабых учеников, объединяя несколько из них вместе, чтобы создать ***сильного ученика*** (или ***модель ансамбля***), который достигает лучших результатов.

Объединение слабых учеников

Чтобы реализовать ансамблевый метод, нам сначала нужно отобрать наших слабых учеников для агрегирования. В основном (в том числе в хорошо известных методах бэггинга и бустинга) используется единственный базовый алгоритм обучения, так что у нас есть однородные слабые ученики, которые обучаются по-разному. Получаемая нами модель ансамбля называется «***однородной***». Тем не менее, существуют также некоторые методы, которые используют различные типы базовых алгоритмов обучения: некоторые ***разнородные слабые ученики*** затем объединяются в **«*разнородную ансамблевую модель*»**.

* **Бэггинг.**В этом случае часто рассматривают однородных слабых учеников, обучают их параллельно и независимо друг от друга, а затем объединяют их, следуя некоторому детерминированному процессу усреднения.

Слабых учеников можно объединить, чтобы получить модель с лучшими показателями. Способ объединения базовых моделей должен быть адаптирован к их типам. Модели с низким смещением и высоким разбросом следует объединять таким образом, чтобы сделать сильную модель более устойчивой, тогда как модели с низким разбросом и высоким смещением лучше объединять таким образом, чтобы сделать ансамблевую модель менее смещенной.

**Сфокусируем внимание на бэггинге**

В ***параллельных методах*** мы рассматриваем разных учеников независимо друг от друга друга и, таким образом, можно обучать их одновременно. Наиболее известным из таких подходом является «***бэггинг***» (от «*bootstrap aggregation*»), целью которого является создание ансамблевой модели, которая является **более надежной,** чем отдельные модели, ее составляющие.

Бутстрэп

Давайте начнем с определения бутстрэпа. Этот статистический метод заключается в генерации выборок размера B (так называемых бутстрэп выборок) из исходного датасета размера N путем случайного выбора элементов с повторениями в каждом из наблюдений B.



Иллюстрация процесса бустрэпа

При некоторых допущениях эти выборки имеют довольно хорошие статистические свойства: в первом приближении их можно рассматривать как взятые непосредственно из истинного базового (и часто неизвестного) распределения данных, так и независимо друг от друга. Таким образом, их можно рассматривать как репрезентативные и независимые выборки истинного распределения данных (почти идентичные выборки). Гипотеза, которая должна быть проверена, чтобы сделать это приближение действительным, имеет две стороны. Во-первых, размер N исходного датасета должен быть достаточно большим, чтобы охватить большую часть сложности базового распределения, чтобы выборка из датасета была хорошим приближением к выборке из реального распределения **(репрезентативность)**. Во-вторых, размер датасета N должен быть достаточно большим по сравнению с размером бутстрэп выборок B, чтобы выборки не слишком сильно коррелировали **(независимость)**. Обратите внимание, что в дальнейшем мы иногда будем ссылаться на эти свойства (репрезентативность и независимость) бутстрэп выборок: читатель всегда должен помнить, что **это только приближение**.

Бутстрэп выборки часто используются, например, для оценки разброса или доверительных интервалов статистических оценок. По определению статистическая оценка является функцией некоторых наблюдений и, следовательно, случайной величины с разбросом, полученным из этих наблюдений. Чтобы оценить разброс такой оценки, нам нужно оценить его на нескольких независимых выборках, взятых из интересующего распределения. В большинстве случаев рассмотрение действительно независимых выборок потребовало бы слишком большого количества данных по сравнению с реально доступным количеством. Затем мы можем использовать бутстрэп, чтобы сгенерировать несколько бутстрэп выборок, которые можно рассматривать как «почти репрезентативные» и «почти независимые» (почти «независимые одинаково распределенные выборки»). Эти примеры бутстрэп выборок позволят нам аппроксимировать разброс оценки, оценивая его значение для каждой из них.

Бутстрэп часто используется для оценки разброса или доверительного интервала некоторых статистических оценок

**Бэггинг**

При обучении модели, независимо от того, имеем ли мы дело с  
проблемой классификации или регрессии, мы получаем функцию, которая принимает входные данные, возвращает выходные данные и определяется в отношении обучающего датасета. Из-за теоретического разброса обучающего датасета (мы напоминаем, что датасет является наблюдаемой выборкой, исходящей из истинно неизвестного базового распределения), подобранная модель также подвержена изменчивости: **если бы наблюдался другой датасет, мы получили бы другую модель**.

Идея бэггинга в таком случае проста: мы хотим подобрать несколько независимых моделей и «усреднить» их прогнозы, чтобы получить модель с меньшим разбросом. Однако на практике мы не можем подобрать полностью независимые модели, потому что для этого потребуется слишком много данных. Таким образом, мы полагаемся на хорошие «приблизительные свойства» бутстрэп выборок (репрезентативность и независимость) для подбора моделей, которые практически независимы.

Сначала мы генерируем несколько бутстрэп выборок так, чтобы каждая новая бутстрэп выборка выполняла роль (почти) еще одного независимого датасета, взятого из истинного распределения. Затем мы можем **обучить слабого ученика для каждой из этих выборок и, наконец, агрегировать их так, чтобы мы как бы «усреднили» их результаты** и, таким образом, получили модель ансамбля с разбросом меньшим, чем ее отдельные компоненты.

Итак, предположим, что у нас есть L бутстрап выборок (аппроксимации L независимых датасетов) размера B. Это обозначается:



Мы можем обучить L почти независимых слабых учеников (по одному на каждый датасет): 

А затем объединим их некоторым процессом усреднения, чтобы получить модель ансамбля с меньшим разбросом. Например, мы можем определить нашу сильную модель так, чтобы



Существует несколько возможных способов объединить несколько моделей, обученных параллельно. Для задачи регрессии выходные данные отдельных моделей могут быть буквально усреднены для получения выходных данных модели ансамбля. Для задачи классификации класс, предсказываемый каждой моделью, можно рассматривать как голос, а класс, который получает большинство голосов, является ответом модели ансамбля (это называется **мажоритарным голосованием**). Что касается задачи классификации, мы также можем рассмотреть вероятности каждого класса, предсказываемые всеми моделями, усреднить эти вероятности и сохранить класс с самой высокой средней вероятностью (это называется **мягким голосованием**). Средние значения или голоса могут быть простыми или взвешенными, если будут использоваться любые соответствующие им веса.

**Случайные леса**

***Деревья решений*** являются очень популярными базовыми моделями для ансамблевых методов. Сильные ученики, состоящие из нескольких деревьев решений, можно назвать «лесами». Деревья, составляющие лес, могут быть выбраны либо неглубокими (глубиной в несколько узлов), либо глубокими (глубиной в множество узлов, если не в полную глубину со всеми листьями). Неглубокие деревья имеют меньший разброс, но более высокое смещение, и тогда для них лучшим выбором станут **последовательные методы**, которые мы опишем позже. Глубокие деревья, с другой стороны, имеют низкое смещение, но высокий разброс и, таким образом, являются подходящим выбором для бэггинга, который в основном направлен на уменьшение разброса.

**Случайный лес**представляет собой метод бэггинга, где глубокие деревья, обученные на бутстрап выборках, объединяются для получения результата с более низким разбросом. Тем не менее, случайные леса также используют другой прием, чтобы несколько обученных деревьев были менее коррелированными друг с другом: при построении каждого дерева вместо выбора всех признаков из датасета для генерации бутстрэпа мы выбираем и сохраняем только случайное их подмножество для построения дерева (обычно одинаковое для всех бутстрэп выборок).

Выборка по признакам действительно приводит к тому, что все деревья не смотрят на одну и ту же информацию для принятия своих решений и, таким образом, уменьшают корреляцию между различными возвращаемыми выходными данными. Другое преимущество выборки по признакам заключается в том, что **она делает процесс принятия решений более устойчивым к отсутствующим данным**: значения наблюдения (из обучающего датасета или нет) с отсутствующими данными можно восстанавливать с помощью регрессии или классификации на основе деревьев, которые учитывают только те признаки, где данные не отсутствуют. Таким образом, алгоритм случайного леса сочетает в себе концепции бэггинга и выбора подпространства случайных объектов для создания более устойчивых моделей.

Задача отбора признаков

**Методы отбора признаков при моделировании**

Целевые признаки (feature), используемые для обучения модели, оказывают большое влияние на качество результатов. Неинформативные или слабо информативные признаки могут существенно понизить эффективность и точность многих моделей, особенно линейных, таких как линейная и логистическая регрессия. После устранения или преобразования неинформативных/слабо информативных признаков модель упрощается, и соответственно уменьшается размер набора данных в памяти и ускоряется работа алгоритмов ML на нем.

Можно выделить 3 задачи:

* **feature selection** – отсечение ненужных признаков (избыточных, слабо информативных) и выбор признаков, имеющих наиболее тесные взаимосвязи с целевой переменной.
* **feature extraction and feature engineering** – превращение данных, специфических для предметной области, в понятные для модели векторы;
* **feature transformation** – трансформация данных для повышения точности алгоритма (например, нормализация данных).

Каждая из этих задач направлена на обеспечение следующих преимуществ:

* **Уменьшение переобучения.** Чем меньше избыточных данных, тем меньше возможностей для модели принимать решения на основе «шума».
* **Повышение точности предсказания модели.** Чем меньше противоречивых данных, тем выше точность.
* **Сокращение времени обучения.** Чем меньше данных, тем быстрее обучается модель.
* **Увеличивается семантическое понимание модели.**

 Выделяют методы ручного и автоматизированного отбора признаков.

Методы ручного отбора признаков основаны на содержательном анализе каждого признака и их совокупности, когда решение о включении/исключении признака из модели принимает исследователь.

В данном разделе рассмотрены различные методы автоматизированного отбора признаков (feature selection), применяемые для подготовки данных. Они могут быть реализованы с помощью Python и библиотеки scikit-learn. Подробное руководство по отбору признаков с помощью scikit-learn вы можете найти в документации к этой библиотеке в разделе Feature selection.

Методы отбора признаков делятся на три группы:

1) методы-фильтры (filters) - они оценивают признаки только на основе информации, полученной из обучающей выборки. Применяются на этапе предобработки, до запуска алгоритма обучения;

2) методы-обертки (wrappers) - классификатор запускается на конкретных подмножествах обучающей выборки, а затем выбирается подмножество наиболее информативных для обучения признаков;



Рисунок 1 - Процесс работы оберточных методов

3) встроенные методы (embedded) - позволяют не отделять отбор признаков и обучение классификатора. Данный тип методов также обладает рядом других преимуществ: они хорошо приспособлены к конкретной модели; не требуется выделять специальное подмножество для тестирования, как в предыдущих методах, и, как следствие из этого, меньше риск переобучения.



Рисунок 2 - Процесс работы встроенных методов

Рассмотрим подробнее каждую группу.

**1 Методы – Фильтры**(filters)

**Фильтры** (англ. *filter methods*) измеряют релевантность признаков на основе функции μμ, и затем решают по определенному правилу, какие признаки оставить в результирующем множестве.

Фильтры могут быть:

* Одномерные (англ. *univariate*) — функция μμ определяет релевантность одного признака по отношению к целевой переменной. В таком случае обычно измеряют "качество" каждого признака с помощью, например, статистических критериев (коэффициент ранговой корреляции Спирмена, Information gain и др.) и удаляют худшие. Например, библиотека scikit-learn содержит класс SelectKBest, реализующий одномерный отбор признаков (univariate feature selection). Этот класс можно применять совместно с различными статистическими критериями для отбора заданного количества признаков.
* Многомерные (англ. *multivariate*) — функция μμ определяет релевантность некоторого подмножества исходного множества признаков относительно выходных меток.

Преимуществом группы фильтров является простота вычисления релевантности признаков в наборе данных, но недостатком в таком подходе является игнорирование возможных зависимостей между признаками.

Принцип методов обертки состоит в следующем:

• выполняется поиск по пространству подмножеств исходного множества признаков;

• для каждого шага поиска используется информация о качестве обучения на текущем подмножестве признаков (в качестве функции оценки качества обучения на текущем подмножестве признаков часто используется точность классификатора).

Этот процесс является циклическим и продолжается до тех пор, пока не будут достигнуты заданные условия останова. Оберточные методы учитывают зависимости между признаками, что является преимуществом по сравнению с фильтрами, к тому же показывают большую точность, но вычисления занимают длительное время, и повышается риск переобучения.

2.Методы-обертки (Wrapper methods)

Существует несколько типов оберточных методов: детерминированные, которые изменяют множество признаков по определенному правилу, а также рандомизированные, которые используют генетические алгоритмы для выбора искомого подмножества признаков. Среди детерминированных алгоритмов самыми простыми являются алгоритмы последовательного поиска:

* SFS (Sequential Forward Selection) — жадный алгоритм, который начинает с пустого множества признаков, на каждом шаге добавляя лучший из еще не выбранных признаков в результирующее множество. На первом этапе производительность классификатора оценивается по отношению к каждому признаку. Выбирается признак, который работает лучше всего. На втором этапе первый признак пробуется в сочетании со всеми другими функциями. Выбирается комбинация двух функций, обеспечивающих наилучшую производительность алгоритма. Процесс продолжается до тех пор, пока не будет выбрано указанное количество признаков.
* SBS (Sequential Backward Selection) — алгоритм обратный SFS, который начинает с изначального множества признаков, и удаляет по одному или несколько худших признаков на каждом шаге; следует отметить, что эмпирически обратный жадный алгоритм даёт обычно лучшие результаты по сравнению с прямым жадным алгоритмом. Это связано с тем, что обратный жадный алгоритм учитывает признаки, информативные в совокупности, но неинформативные, если рассматривать их по отдельности.
* SSS (Sequential Stepwise Selection) – вунаправленное исключение/отбор - комбинация вышеперечисленных алгоритмов: тестирование на каждом шаге после включения/исключения признаков.

 На каждом шаге описанных алгоритмов для оценки качества обычно используются такие критерии, как F-тест (статистика Фишера), t-тест (статистика Стъюдента), скорректированный коэффициент детерминации R2 и прочие. Сам алгоритм при этом принимает форму последовательности F-тестов, t-тестов, скорр R2.

Популярным оберточным методом также является SVM-RFE (SVM-based Recursive Feature Elimination, рекурсивное исключение признаков), который иногда также относят к встроенным методам отбора. Этот метод использует как классификатор SVM и работает итеративно: начиная с полного множества признаков обучает классификатор, ранжирует признаки по весам, которые им присвоил классификатор, убирает какое-то число признаков и повторяет процесс с оставшегося подмножества признаков, если не было достигнуто их требуемое количество. Таким образом, этот метод очень похож на встроенный, потому что непосредственно использует знание того, как устроен классификатор.

3.Встроенные методы (embedded)

Встроенные алгоритмы требуют меньше вычислений, чем wrapper methods (хотя и больше, чем методы фильтрации).

Очень похожи на оберточные методы, но для выбора признаков используется непосредственно структура некоторого классификатора. В оберточных методах классификатор служит только для оценки работы на данном множестве признаков, тогда как встроенные методы используют какую-то информацию о признаках, которую классификаторы присваивают во время обучения.

Основным методом из этой категории является регуляризация.

Регуляризация — это своеобразный штраф за излишнюю сложность модели, который позволяет защитить себя от перетренировки в случае наличия среди признаков неинформативных. Не стоит думать, что регуляризация бывает только в линейных моделях, и для бустинга и для нейросетей существуют свои методы регуляризации.  
Существуют различные ее разновидности, но основной принцип общий. Если рассмотреть работу классификатора без регуляризации, то она состоит в построении такой модели, которая наилучшим образом настроилась бы на предсказание всех точек тренировочного сета.  
Например, если алгоритм классификации линейная регрессия, то подбираются коэффициенты полинома, который аппроксимирует зависимость между признаками и целевой переменной. В качестве оценки качества подобранных коэффициентов выступает среднеквадратичная ошибка (RMSE). Т.е. параметры подбираются так, чтобы суммарное отклонение (точнее суммарный квадрат отклонений) у точек предсказанных классификатором от реальных точек было минимальным.  
Идея регуляризации в том, чтобы построить алгоритм, минимизирующий не только ошибку, но и количество используемых переменных.

**Лассо-регрессия / Ридж-регрессия**(метод регуляризации Тихонова, ridge regression)

Эти методы часто применяются для борьбы с переизбыточностью данных, когда независимые переменные коррелируют друг с другом (т.е. имеет место мультиколлинеарность). Следствием этого является плохая обусловленность матрицы  и неустойчивость оценок коэффициентов регрессии. Оценки, например, могут иметь неправильный знак или значения, которые намного превосходят те, которые приемлемы из физических или практических соображений.

Обе техники позволяют уменьшить размерность данных и устранить/смягчить проблему переобучения. Для этого применяются два способа:

* L1-регуляризация — добавляет штраф к сумме абсолютных значений коэффициентов. Этот метод используется в **Лассо-регрессии**. В процессе работы алгоритма величина приписанных алгоритмом коэффициентов будет пропорциональна важности соответствующих переменных для классификации, а для переменных, которые дают наименьший вклад в устранение ошибки, коэффициенты станут нулевыми. Таким образом, более значимые признаки сохранят свои коэффициенты ненулевыми, а менее значимые – обнулятся. Стоит также отметить, что большие по модулю отрицательные значения коэффициентов тоже говорят о сильном влиянии.
* L2-регуляризация — добавляет штраф к сумме квадратов коэффициентов. Этот метод используется в ридж-регрессии.

В большинстве случаев исследователи и разработчики предпочитают L2-функцию — она эффективнее с точки зрения вычислительных функций. С другой стороны, лассо-регрессия позволяет уменьшить значения некоторых коэффициентов до 0, то есть вывести из поля исследования лишние переменные. Это полезно, если на какое-либо явление влияют тысячи факторов и рассматривать все их оказывается бессмысленно.

Ридж-регрессия - усовершенствование линейной регрессии с повышенной устойчивостью к ошибкам, налагающая ограничения на коэффициенты регрессии для получения более приближенного к реальности результата.

Применение гребневой регрессии нередко оправдывают тем, что это практический приём, с помощью которого при желании можно получить меньшее значение среднего квадрата ошибки.

Пара слов о параметре альфа. Он позволяет настраивать вклад регуляризирующего оператора в общую сумму. С его помощью мы можем указать приоритет — точность модели или минимальное количество используемых переменных.  
В LASSO – всё аналогично, за исключением регуляризирующего оператора. Он представляет собой не сумму квадратов, а сумму модулей коэффициентов. Несмотря на незначительность различия, свойства отличаются. Если в ridge по мере роста альфа все коэффициенты получают значения все ближе к нулевым, но обычно при этом все-таки не зануляются. То в LASSO с ростом альфа все больше коэффициентов становятся нулевыми и совсем перестают вносить вклад в модель. Таким образом, мы получаем действительно отбор признаков. Более значимые признаки сохранят свои коэффициенты ненулевыми, менее значимые — обнулятся.

Методы выделения признаков. Эти методы каким-то образом составляют из уже исходных признаков новые, все также полностью описывающие пространство набора данных, но уменьшая его размерность и теряя в репрезентативности данных, т.к. становится непонятно, за что отвечают новые признаки. Все методы feature extraction можно разделить на **линейные** и **нелинейные**.

Одним из самых известных методов **линейного** выделения признаков является PCA (Principal Component Analysis, рус. *метод главных компонент*). Основной идеей этого метода является поиск такой гиперплоскости, на которую при ортогональной проекции всех признаков максимизируется дисперсия. Данное преобразование может быть произведено с помощью сингулярного разложения матриц и создает проекцию только на линейные многомерные плоскости, поэтому и метод находится в категории линейных.

Рассмотрим применение описанных выше методов в реальной задаче – предсказать, зарабатывает ли человек больше $50 тыс. Загрузим библиотеки и данные, для удобства оставив только численные признаки:

* age – возраст
* fnlwgt (final weight) – примерная оценка количества людей, которое представляет каждая строка данных
* educational-num – длительность обучения
* capital-gain – прирост капитала
* capital-loss – потеря капитала
* hours-per-week – количество рабочих часов в неделю

Посмотрим точность на кросс-валидации и важность признаков для случайного леса:

scores = [0.82427915 0.82290796 0.83106668 0.8192637 0.83155106]

mean score = 0.82581 +/- 0.00478

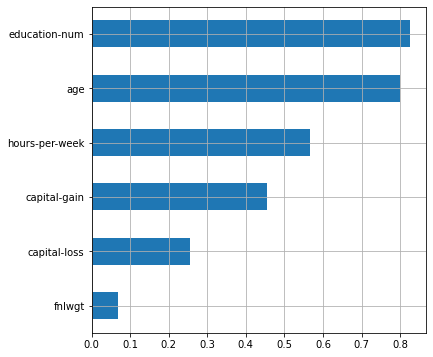


Самым важным признаком для случайного леса является fnlwgt. Это можно интерпретировать как то, что главным фактором того, что человек зарабатывает больше $50 тыс. является количество людей с такими же характеристиками. Такая интерпретация выглядит нелогичной, и происходит это потому, что модели с деревьями могут выдавать сильно смещённую оценку признаков. Притом, чем хуже настроена модель, тем сильнее может быть смещение, поэтому доверять оценкам таких моделей надо с осторожностью.

Повторим процедуру для линейной модели (с L1-регуляризацией). Для нормализации данных будем использовать метод PowerTransformer.

scores = [0.82034993 0.83000963 0.8348707 0.81787667 0.83548066]

mean score = 0.82772 +/- 0.00732



Создадим 12 шумовых признаков, элементами которых будут некоррелируемые случайные числа из выборок с нормальным, равномерным и Лапласовым распределениями. Параметры каждого распределения подбираются случайным образом независимо друг от друга.



Проведём кросс-валидацию на зашумлённых данных и посмотрим важность признаков:

scores = [0.8522425 0.85382173 0.86249657 0.84897581 0.85443027]

mean score = 0.85439 +/- 0.00447

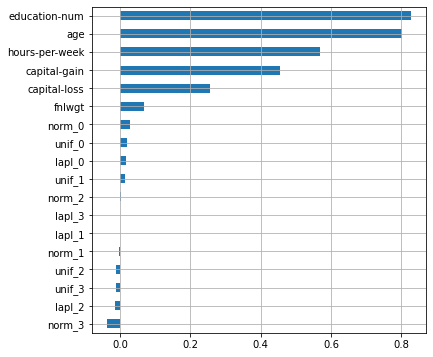


Несмотря на большое количество добавленных шумовых признаков, точность модели на кросс-валидации значительно возросла как на каждом фолде, так и в среднем! Кроме этого, все шумовые признаки имеют высокую важность, сравнимую с двумя оригинальными. Очевидно, что наша модель переобучена, однако в реальных задачах такие ситуации бывает очень сложно распознать, особенно когда при удалении некоторых признаков (про которые неизвестно – шумовые они, или нет) падает валидационная точность. Кроме того, часто бывает сложно подобрать пороговое значение важности признаков для исключения их из модели.

Посмотрим результаты для регрессии.

scores = [0.81993058 0.83005516 0.83446553 0.81763029 0.83543145]

mean score = 0.82750 +/- 0.00738



После добавления шумовых признаков модель не преобучилась, к тому же эти признки имеют значительно меньшие коэффициенты, чем оригинальные. Отметим, что распределение коэффициентов в линейных моделях часто зависит от способа нормализации или масштабирования признаков.

Проведём отбор признаков статистическими методами, для чего будем использовать обобщённый вариант SelectKBest и SelectPercentile, который называется [GenericUnivariateSelect](https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.GenericUnivariateSelect.html#sklearn.feature_selection.GenericUnivariateSelect). Он принимает на вход 3 параметра – функцию оценки, режим отбора и его характеристики. В качестве функции оценки будем использовать взаимную информацию.

|  |  |  |
| --- | --- | --- |
|  | **score** | **support** |
| **capital-gain** | 0.080221 | True |
| **age** | 0.065703 | True |
| **education-num** | 0.064743 | True |
| **hours-per-week** | 0.043655 | True |
| **capital-loss** | 0.033617 | True |
| **fnlwgt** | 0.033390 | True |
| **norm\_3** | 0.003217 | False |
| **unif\_3** | 0.002696 | False |
| **norm\_0** | 0.002506 | False |
| **norm\_2** | 0.002052 | False |
| **lapl\_3** | 0.001201 | False |
| **unif\_1** | 0.001144 | False |
| **lapl\_1** | 0.000000 | False |
| **unif\_2** | 0.000000 | False |
| **lapl\_2** | 0.000000 | False |
| **lapl\_0** | 0.000000 | False |
| **unif\_0** | 0.000000 | False |
| **norm\_1** | 0.000000 | False |

Сгенерированные нами признаки имеют низкое значение оценочной функции (scores\_), поэтому в дальнейшем селектор не будет их использовать (get\_support()=False).

В реальной задаче (когда количество шумовых признаков неизвестно) параметры GenericUnivariateSelect можно находить на кросс-валидации вместе с другими гиперпараметрами модели. Посмотрим, как изменится точность классификаторов после подбора их гиперпараметров, а также количества признаков селектора:

scores = [0.8632776968200635, 0.8683443340928604, 0.8710308000627435, 0.8615748939138762, 0.8693334091828478],

mean score = 0.86671 +/- 0.00364

best params = {'rf\_\_max\_depth': 12, 'rf\_\_max\_features': 0.3, 'selector\_\_param': 5}

Для случайного леса средняя точность на кросс-валидации значительно выросла, а лучший результат получился всего для 5 признаков:



Этот результат был получен после удаления шумовых признаков и признака fnlwgt, который при первоначальной оценке был самым значимым для модели. Однако из всех оригинальных признаков он имел наименьшее значение оценочной функции в GenericUnivariateSelect. Результаты оценки важности признаков после их отбора и настройки модели имеют более логичную интерпретацию – на заработок человека влияют именно характеристики человека, а не параметры самой выборки. Таким образом, статистический отбор признаков бывает полезен для увеличения точности некоторых типов моделей и получения менее смещённой оценки при интерпретации их результатов.

Посмотрим, как изменятся коэффиценты у признаков после подбора коэффициента регуляризации у логистической регрессии.

scores = [0.820445329307105, 0.829874053687009, 0.8346493482101578, 0.8177211039148669, 0.8354590546776963],

mean score = 0.82763 +/- 0.00729

best params = {'lr\_\_C': 0.01}

Средняя точность на кросс-валидации почти не изменилась, но скорректировались коэффициенты у шумовых признаков. Отметим, что сильная регуляризация (L1) может занулить излишнее количество признаков.

Отобранные линейной моделью признаки можно подать на вход другой модели. Для этого воспользуемся методом [SelectFromModel](https://scikit-learn.org/stable/modules/generated/sklearn.feature_selection.SelectFromModel.html#sklearn.feature_selection.SelectFromModel), дадим ему на вход нашу настроенную линейную модель и обозначим граничное значение для отбора коэффициентов.

Заключение:

В работе были рассмотрено использование фильтров и встроенных методов в задаче отбора признаков. К достоинствам фильтров можно отнести низкую стоимость вычислений (линейно зависит от количества признаков) и интерпретируемость. К недостаткам – то, что они рассматривают каждый признак изолировано, поэтому не могут выявить более сложные зависимости в данных, например, зависимость от нескольких предикторов. Эти методы хорошо подойдут, если в данных большое количество признаков, но малое количество объектов (что встречается, например, в медицинских, или биологических исследованиях).

Также в работе были рассмотрены модель решающего дерева и случайного леса. К достоинствам решающего дерева можно отнести порождение четких правил классификации и быстрые процессы обучения и прогнозирования, а к достоинствам случайного леса - существование методов оценивания значимости отдельных признаков в модели и способность эффективно обрабатывать данные с большим числом признаков и классов. К недостаткам деревьев относят чувствительность к шумам во входных данных и необходимость отсекать ветви дерева (pruning) или устанавливать минимальное число элементов в листьях дерева или максимальную глубину дерева для борьбы с переобучением. К недостаткам случайного леса – увеличенную сложность интерпретации по сравнению с решающим деревом.

Список используемых источников:

1. https://medium.com/open-machine-learning-course
2. https://www.hse.ru/mirror/pubs/share/215285956
3. https://neurohive.io/ru/osnovy-data-science/ansamblevye-metody-begging-busting-i-steking/
4. https://nagornyy.me/courses/data-science/feature\_engineering/
5. https://explained.ai/rf-importance/
6. https://habr.com/ru/post/550978/
7. https://archive.ics.uci.edu/ml/datasets/Adult