

РЕФЕРАТ

Выпускная квалификационная работа содержит _ страниц, _ рисунка, _ использованных источников и _ приложение.

ТЕМЫ_ЧЕРЕЗ_ЗАПЯТУЮ

Постановка_задачи

СОДЕРЖАНИЕ

РЕФЕРАТ	2
СОДЕРЖАНИЕ	3
ВВЕДЕНИЕ.....	4
ОСНОВНАЯ ЧАСТЬ	6
1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ	7
1.1 Задачи машинного обучения.....	7
1.2 Задача классификации	7
1.3 Решение задач классификации.....	9
1.4 Байесовские классификаторы	10
1.5 Наивный байесовский классификатор	10

ВВЕДЕНИЕ

Задача классификации – одна из самых актуальных задач машинного обучения. Она встречается в медицине, экономике, геофизике, социологии, технике, биоинформатике и других отраслях. Классификация может быть разных типов, основные – двухклассовые и многоклассовые. Встречаются также задачи с нечёткими классами, классами с пересечением и без, линейно разделимыми и неразделимыми классами.

В качестве примера прикладной задачи машинного обучения можно привести медицинскую диагностику. Объектом является пациент с определенным набором признаков – пол, рост, вес, симптомы (наличие слабости, тошноты, головной боли), результаты обследований (анализы крови), различные измерения (артериальное давление, пульс). На основе этих признаков можно определить вид заболевания, что является многоклассовой классификацией. Помимо этого, можно назначить способ лечения, оценить риск осложнений, предсказать эффективность терапии.

Другой пример – кредитный скоринг – является примером двухклассовой (бинарной) классификации. На основе признаков банку нужно принять решение, выдавать кредит данному физическому лицу или нет. В качестве признаков могут выступать доход, профессия, состав семьи, задолженности, кредитная история.

Также к задачам машинного обучения относятся распознавание символов, предсказание оттока клиентов, обнаружение спама, распознавание речи, предсказание месторождений полезных ископаемых, различное прогнозирование и т.д.

Таким образом, задачи классификации актуальны и часто встречаются в современном мире, их решение очень востребовано. Машинное обучение предлагает множество различных способов для решения подобных задач. К примеру, существует множество байесовских классификаторов: наивный байесовский классификатор, метод парзеновского окна, линейный дискриминант Фишера. Помимо перечисленных алгоритмов, эти задачи могут

быть решены с помощью персептрона и многослойных нейронных сетей, методом опорных векторов, решающими деревьями, логистической регрессией и множеством других методов.

ОСНОВНАЯ ЧАСТЬ

1 ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

1.1 Задачи машинного обучения

Машинное обучение сейчас является одной из самых востребованных областей знаний. Исторически она развилась из области искусственного интеллекта. При попытке создать разумную машину обнаружилось, что запрограммировать её на решение некоторых задач вполне возможно, к примеру, на нахождение кратчайшего пути между двумя вершинами в графе. Однако решение других задач, таких как распознавание лиц, фильтрация спама, принятие решений и прочих, с которыми человек справляется без труда, запрограммировать не удастся. Было предложено решать эти задачи путем самостоятельного обучения машины, когда алгоритм решения не программируется явно. В настоящее время машинное обучение используется в большом количестве прикладных задач, где присутствует большой объем данных и требуется решать задачи фильтрации, автоматизации принятия решений и т.д. Также оно решает задачи классификации, восстановления регрессии, кластеризации, идентификации, извлечения знаний, ранжирования, составления рекомендаций и многие другие.

1.2 Задача классификации

Одной из задач машинного обучения является задача классификации. Она заключается в том, чтобы разделить заданные объекты на определенные классы. Изначально для обучения алгоритму даётся так называемая обучающая выборка – множество примеров, для объектов которого их классы заранее известны. Необходимо построить алгоритм, который будет определять класс произвольного объекта, основываясь на принадлежности к классам объектов из обучающей выборки.

Задачи классификации делятся на несколько типов. Один из самых простых – двухклассовая классификация. Бывают также многоклассовые классификации, пересекающиеся классы и непересекающиеся, нечёткие

классы. Помимо этого, выделяют линейно разделимые и линейно не разделимые классы.

Входные данные для классификатора могут быть представлены различными способами. Может быть дано изображение или аудио, матрица расстояний между элементами, временной ряд, текст. Но чаще всего данные представлены признаковым описанием. В этом случае каждому объекту ставятся в соответствие некоторые значения, чаще всего числовые, и признаки f_i выступают в роли такого отображения: $f_i: X \rightarrow D_j, j = 1, \dots, n$; X – множество объектов, D_j – область определения для j -го признака. Объект будет описываться вектором фиксированного размера, каждый элемент которого представляет собой определенный признак. Чаще всего встречаются бинарные признаки (принимающие только значения $+1$ или -1) и количественные (принимающие любое числовое значение). Бывают также номинальные (категориальные) и порядковые признаки, которые принимают значения из какого-то ограниченного множества, в последнем случае в этом множестве введено отношение порядка. Примером бинарного признака может служить пол человека, количественного – его рост, номинального – цвет глаз, порядкового – воинское звание.

Формальное определение задачи классификации: изначально даны множество объектов X и множество наименований классов (меток, ответов) Y . Существует неизвестная зависимость $y: X \rightarrow Y$, значения которой известны на объектах конечной обучающей выборки $X^l = (x_i, y_i)_{i=1}^l, y_i = y(x_i)$. Необходимо найти классификатор $a: X \rightarrow Y$ с минимальной вероятностью ошибки.

Признаковое описание объекта $x \in X$ выглядит следующим образом: $(f_1(x), \dots, f_n(x))$, где f_1, \dots, f_n – множество некоторых признаков. Множество таких описаний для всего множества объектов представляется в виде матрицы «объекты-признаки»:

$$F = \|f_j(x_i)\|_{l \times n} = \begin{pmatrix} f_1(x_1) & \cdots & f_n(x_1) \\ \vdots & \ddots & \vdots \\ f_1(x_l) & \cdots & f_n(x_l) \end{pmatrix}$$

Каждой строке этой матрицы соответствует ответ или метка класса. В случае бинарной классификации ответы могут принимать два возможных значения: $Y = \{+1, -1\}$. Для многоклассовой классификации есть несколько вариантов значений: $Y = \{1, \dots, M\}$.

1.3 Решение задач классификации

Для решения задач классификации существует множество методов: нейронные сети, сокращение размерности, байесовские классификаторы, деревья решений, линейные разделители, алгоритмическая композиция. Какой бы алгоритм не использовался, его работа делится на два этапа: этап обучения и этап применения (тестирования). На первом этапе по обучающей выборке строится функция, которая будет классифицировать новые объекты. На втором этапе даётся выборка из новых объектов, называемая тестовой выборкой, на которой полученная функция выдает ответы – предсказанные классы.

В общем случае существует множество функций $A = \{a_i\}$, способных предсказать класс объекта, которые могут различаться между собой, например, значениями некоторых параметров. Необходимо каким-то образом выбирать из них наилучшую функцию, и для этого вводится функция потерь $L(a, x)$, которая характеризует величину ошибки алгоритма $a \in A$ на элементе $x \in X$. Для задачи классификации функция потерь имеет вид $L(a, x) = [a(x) \neq y(x)]$, и равна 1, если алгоритм классифицировал неверно, или 0, если ответ правильный. Для оценки ошибки алгоритма на всем множестве X вводится функционал $Q(a, X^l) = \frac{1}{l} \sum_{i=1}^l L(a, x_i)$, называемый эмпирическим риском. Необходимо минимизировать этот функционал по параметрам модели, и таким образом получить наилучший алгоритм, который дает наименьшую ошибку.

1.4 Байесовские классификаторы

Рассмотрим байесовские классификаторы - класс методов, который состоит из алгоритмов, основанных на нахождении класса с максимальной апостериорной вероятностью. Для работы байесовских методов необходима полная априорная информация о классах, то есть функция правдоподобия для каждого из классов и вероятности появления классов (априорные вероятности). По этим данным высчитываются апостериорные вероятности согласно формуле Байеса:

$$P(y|x) = \frac{P(x|y)P(y)}{P(x)},$$

где y – предположительный класс, x – объект классификации, $P(y)$ – априорная вероятность класса y , $P(x|y)$ – функция правдоподобия для класса y , $P(y|x)$ – апостериорная вероятность класса y , $P(x)$ – априорная вероятность объекта x . Смысл этой формулы можно воспринимать как перестановку причины и следствия местами.

После расчета вероятностей для каждого класса необходимо найти класс y^* , который даёт наибольшую вероятность для заданного объекта x , т.е:

$$y^* = \arg \max_{y \in Y} \frac{P(x|y)P(y)}{P(x)}, Y - \text{множество классов.}$$

На практике часто сталкиваются с тем, что плотности распределения классов и вероятности их появления неизвестны, поэтому их приходится находить с некоторой погрешностью по обучающей выборке. Для восстановления функции правдоподобия используются разные предположения и методы, которые порождают различные байесовские алгоритмы классификации.

1.5 Наивный байесовский классификатор

Одним из примеров таких алгоритмов является наивный байесовский классификатор. В его основе лежит предположение о том, что все признаки (вероятности) независимы и имеют одинаковый вклад в результат вычислений.

Представим классифицируемый объект в виде набора его признаков: $x = (x_1, x_2, \dots, x_n)$. В общем случае признаки могут быть зависимы друг от друга, и вероятность $P(x|y)$ представляет собой вероятность $P(x|y, x)$. В наивном байесовском классификаторе делается предположение о том, что признаки друг от друга не зависят, и в этом случае условную вероятность вектора признаков можно представить в виде произведения условных вероятностей отдельных признаков:

$$P(x|y) = P(x_1|y)P(x_2|y) \dots P(x_n|y)$$

Тогда формула Байеса принимает следующий вид:

$$P(y|x_1, \dots, x_n) = \frac{P(x_1|y)P(x_2|y) \dots P(x_n|y)P(y)}{P(x_1)P(x_2) \dots P(x_n)}$$

Так как знаменатель при вычислении с разными классами не меняется, а значит, не влияет на получающиеся вероятности, его можно не учитывать. Получаем:

$$P(y|x_1, \dots, x_n) \propto P(y) \prod_{i=1}^n P(x_i|y)$$

После всех перечисленных упрощений задача классификации сводится к нахождению следующего класса y^* :

$$y^* = \arg \max_{y \in Y} P(y) \prod_{i=1}^n P(x_i|y)$$

Таким образом, для классификации нужно знать априорные вероятности $P(y)$ каждого класса, а также условные вероятности $P(x_i|y)$ каждого признака. В первом случае можно взять долю объектов из обучающей выборки, которые принадлежат этому классу. Однако частота определенного класса в выборке может отличаться от реального распределения, так как, к примеру, на этапе составления выборки могло быть взято одинаковое количество объектов каждого класса. Для подсчета $P(x_i = a|y = b)$, (a, b – конкретные значения признака и класса) можно взять отношение количества объектов из класса b с признаком $x_i = a$ к общему количеству объектов,

принадлежащих этому классу: $P(x_i = a|y = b) = \frac{\sum obj(x_i=a,y=b)}{\sum obj(x,y=b)}$ (за $obj(x_i = a, y = b)$ примем объекты обучающей выборки, которые принадлежат классу b и имеют признак x_i равным a ; за $obj(x, y = b)$ примем объекты, принадлежащие классу b).

Рассмотрим пример работы наивного байесовского классификатор. Пусть даны признаки в виде информации о погоде и решение (класс), стоит ли в такую погоду играть в гольф:

Погода, x_1	Ветер, x_2	Гольф, y
Дождливо	Нет	Нет
Дождливо	Есть	Нет
Солнечно	Нет	Да
Солнечно	Нет	Да
Солнечно	Есть	Нет
Дождливо	Нет	Нет
Дождливо	Нет	Да
Солнечно	Нет	Да
Дождливо	Есть	Да

Для каждого из признаков можно составить таблицу частот и правдоподобия:

Погода, $x_1 \setminus$ Гольф, y	Нет	Да	
Солнечно	1	3	$P(x_1) = 4/9$
Дождливо	3	2	$P(x_1) = 5/9$
<i>Всего</i>	<i>4</i>	<i>5</i>	<i>9</i>
	$P(y) = 4/9$	$P(y) = 5/9$	

Ветер, $x_2 \setminus$ Гольф, y	Нет	Да	
Есть	2	1	$P(x_2) = 3/9$
Нет	2	4	$P(x_2) = 6/9$

<i>Всего</i>	4	5	9
	$P(y) = 4/9$	$P(y) = 5/9$	

Предположим, что теперь необходимо посчитать, стоит ли играть в гольф, если погода солнечная и есть ветер. Для каждого класса по формуле Байеса получаем:

$$\begin{aligned}
 &P(y = \text{Да} | x_1 = \text{Солнечно}, x_2 = \text{Есть}) = \\
 &= \frac{P(x_1 = \text{Солнечно} | y = \text{Да})P(x_2 = \text{Есть} | y = \text{Да})P(y = \text{Да})}{P(x_1 = \text{Солнечно})P(x_2 = \text{Есть})} = \\
 &= \frac{3/5 * 1/5 * 5/9}{4/9 * 3/9} = 0.4
 \end{aligned}$$

$$\begin{aligned}
 &P(y = \text{Нет} | x_1 = \text{Солнечно}, x_2 = \text{Есть}) = \\
 &= \frac{P(x_1 = \text{Солнечно} | y = \text{Нет})P(x_2 = \text{Есть} | y = \text{Нет})P(y = \text{Нет})}{P(x_1 = \text{Солнечно})P(x_2 = \text{Есть})} = \\
 &= \frac{1/4 * 2/4 * 4/9}{4/9 * 3/9} = 0.375
 \end{aligned}$$

Получаем, что $P(y = \text{Да} | x) > P(y = \text{Нет} | x)$, поэтому ответом будет класс «Да».

На этапе классификации может возникнуть так называемая проблема нулевой частоты. Это происходит, когда на этапе тестирования какой-нибудь категориальный признак принимает значение, которого не было в обучающей выборке. Например, для приведенной выше задачи в качестве признака x_1 может попасться значение Облачно. В таком случае все условные вероятности будут равны нулю, что даст ноль при их перемножении, а значит и все классы будут иметь нулевую вероятность. Для решения этой проблемы применяют сглаживание Лапласа. Его идея заключается в том, что каждое слово считается встреченным на один раз больше, то есть к частотам слов прибавляется единица:

$$P(x_i = a | y = b) = \frac{\sum \text{obj}(x_i = a, y = b) + 1}{\sum [\text{obj}(y = b) + 1]}$$

В итоге условные вероятности для признаков, которые ранее не встречались, никогда не будут нулевыми.

В случае, когда объект выражается большим количеством признаков, приходится перемножать большое количество чисел, которые могут быть близки к нулю. Это может привести к исчезновению порядка, в результате чего все вероятности окажутся нулевыми. Чтобы этого избежать, можно использовать свойство логарифма произведения: $\log(a * b) = \log(a) + \log(b)$. Логарифм является монотонной функцией, поэтому переход к нему не изменит максимум функции, а значит, и искомый класс y^* . В результате все полученные слагаемые по модулю будут больше нуля, а значит их сумма скорее всего не будет давать настолько маленькое число, чтобы можно было столкнуться с исчезновением порядка.

После перехода к логарифму получается следующая формула:

$$y^* = \arg \max_{y \in Y} \left[\log P(y) + \sum_{i=1}^n \log P(x_i|y) \right]$$

Бывает несколько типов моделей наивных байесовских классификаторов, которые различаются предположениями относительно условных вероятностей $P(x|y)$ – распределений признаков. Один из них – мультиномиальный. Он используется для случаев, когда признаки принимают дискретные значения, и считается, что каждый признак имеет мультиномиальное распределение. Чаще всего используется для классификации документов, в этом случае подсчитывается частота появления слова в документе.

Следующий тип использует распределение Бернулли. Он похож на мультиномиальную модель, но признаки могут принимать только значения 0 или 1. Для классификации документов это может означать проверку факта, появляется слово в тексте или нет. Мотивация такого подхода в том, что наличие или отсутствие слова в тексте важнее частоты его появления, поэтому количество появлений слова можно не учитывать.

Еще одна модель основывается на распределении Гаусса. Она используется в случае, когда признаки принимают непрерывные значения, и предполагается, что они имеют нормальное распределение. На основе этого условная вероятность считается по формуле:

$$P(x_i|y) = \frac{1}{\sqrt{2\pi\sigma_y^2}} \exp\left(-\frac{(x_i-\mu_y)^2}{2\sigma_y^2}\right),$$

где μ_y – математическое ожидание признака x_i в классе y , σ_y^2 – дисперсия.

Если непрерывный признак не имеет нормального распределения, можно попробовать различными методами и преобразованиями привести его к такому. Другим вариантом является разбиение значений по интервалам, в которых содержится примерно одинаковое количество различных значений признака, например, на квартили или децили. Каждое значение признака помечается номером соответствующего интервала, и признак считается категориальным. Во время классификации признаки также относят к определенному интервалу, и исходя из этого рассчитывают необходимые вероятности. Также для улучшения работы наивного байесовского классификатора можно убрать зависимые признаки, чтобы они не перевешивали другие признаки по значимости. В задаче классификации документов (текстов) можно убрать так называемые стоп-слова, которые могут встречаться в любом тексте и не имеют отношения к каким-то определенным классам.

Дерево решений

Еще одним методом решения задач классификации является дерево решений. Этот метод приближен к той схеме, по которой человек оценивает, какое решение нужно принять. Уточняя различную информацию, получается постепенно прийти к какому-то ответу. Этот метод также можно сравнить с инструкциями, которые описывают, какие действия предпринимать в различных ситуациях.

Самым простым видом решающего дерева является бинарное дерево. Все его вершины делятся на два типа. Первый – внутренние вершины, из которых идут рёбра к двум дочерним вершинам. Второй тип – листья – конечные вершины, у которых нет потомков. С каждой внутренней вершиной связано решающее правило, которое разделяет случаи. Это функции (или предикаты), которые определяют, в какое поддерево необходимо отправить рассматриваемый объект. Решающие правила связаны с признаками объектов, и если признаки являются бинарными, то разделение на дочерние вершины происходит согласно значениям признака. Например, если признак принимает значение 1, то объект определяют в правое поддерево, если значение 0, то в левое. Если же признаки могут принимать несколько различных значений, то разделение происходит по какому-нибудь из порогов, отделяющие эти значения. Например, если множество допустимых значений какого-нибудь признака f_i равно целым числам от двух до семи, то есть смысл рассматривать решающие правила « $f_i \geq 2$ », « $f_i \geq 3$ » и т.д. Для выбора лучшего порога используются различные методы, которые оценивают эффективность разделения при выборе порога.

С каждым листом связана метка класса, к которому пришли в результате разбиений с помощью решающих правил, либо плотность вероятности, если класс определяется неоднозначно.

На первом этапе метода по обучающей выборке строится само дерево, выбирая наиболее полезные признаки в качестве решающих правил. Построение продолжается до тех пор, пока в листе не останутся элементы одного класса. Допускаются также другие различные критерии остановки, например, минимальное допустимое количество элементов в листе, глубина дерева и т.д. При завершении построения каждой ветки в листе ставится вектор вероятности либо метка того класса, который имеют объекты, оказавшиеся в этом листе.

На этапе классификации объект пропускается по построенному решающему дереву, в каждой внутренней вершине переходя в правое или

левое поддереву в зависимости от значения проверяемого признака. В итоге объект доходит до листа, и ему присваивается класс, который соответствует этому листу, либо класс с максимальной вероятностью, если листу соответствует плотность вероятности.

После выполнения классификации необходим способ оценивания, насколько хорошо алгоритм справился с задачей. Для этого необходимо сравнить получившееся решение на тестовой выборке с известными результатами. При этом, чтобы оценить качество классификатора, нужно выбрать подходящую метрику.

В самом простом случае можно считать отношение правильно классифицированных объектов к общему их количеству. Недостатками этого метода является плохая работа в случае несбалансированных классов, когда одному классу принадлежит в несколько раз больше объектов, чем к другому. Полученная корректность может быть высокой за счет правильной классификации внутри большого класса, так как в нем содержится больше данных для анализа. Внутри же маленького класса алгоритм может работать неправильно, но из-за небольшого количества таких примеров это почти не испортит оценку точности классификатора.

В качестве меры также можно использовать полноту (recall) и точность (precision). Их можно использовать отдельно или как основу для других метрик. При сравнении результатов работы алгоритма с правильными ответами, можно выделить четыре варианта их соотношений:

- TP (true positive) – истинно-положительный результат;
- TN (true negative) – истинно-отрицательный результат;
- FP (false positive) – ложно-положительный результат;
- FN (false negative) – ложно-отрицательный результат.

Это можно представить в виде таблицы следующим образом:

		Правильный ответ	
		Положительный	Отрицательный
Ответ алгоритма	Положительный	TP	FP
	Отрицательный	FN	TN

То есть истинно-положительный результат получается, когда алгоритм отнес объект к правильному классу, ложно-отрицательный – когда алгоритм не отнес объект к правильному классу и т.д.

Полнота и точность высчитываются по следующим формулам:

$$Recall = \frac{TP}{TP + FN};$$

$$Precision = \frac{TP}{TP + FP}.$$

Таким образом, полнота означает долю тех объектов, которые классификатор отнес к классу, относительно реального числу объектов этого класса. Она характеризует способность алгоритма выявлять положительные ответы, то есть какая доля правильных ответов была найдена. Точность внутри класса означает долю правильно классифицированных объектов относительно объектов, отнесенных алгоритмом к этому классу. Она характеризует, сколько положительных ответов классификатора являются правильными.

Так как невозможно одновременно достичь максимальные полноту и точность, вводится мера, которая объединяет эту информацию, выражает баланс. Она называется F1-мерой и высчитывается следующим образом:

$$F1 = \frac{2 * Recall * Precision}{Recall + Precision}$$