Anotações   
sobre   
Machine Learning

Igor Ruys Cartucho

Sumário

[Capítulo 1: Estimação de Parâmetros 5](#_Toc158475827)

[1.1 Maximum Likelihood Estimation (MLE) 6](#_Toc158475828)

[1.2 Maximum A Posteriori (MAP) Estimation 10](#_Toc158475829)

[Capítulo 2: Regressão Linear 12](#_Toc158475830)

[2.1 Diferentes Interpretações da Regressão Linear 13](#_Toc158475831)

[2.1.1 Ponto de Vista de Otimização 13](#_Toc158475832)

[2.1.2 Ponto de Vista de Álgebra Linear 14](#_Toc158475833)

[2.1.3 Ponto de Vista Probabilístico 16](#_Toc158475834)

[2.2 Regressão Polinomial 17](#_Toc158475835)

[2.3 Forma Geral da Regressão Linear 18](#_Toc158475836)

[Capítulo 3: Regressão Logística 19](#_Toc158475837)

[3.1 Mínimos Quadrados Para Classificação 20](#_Toc158475838)

[3.2 Modelando a Probabilidade A Priori 23](#_Toc158475839)

[3.2.1 Caso 23](#_Toc158475840)

[3.2.2 Caso 24](#_Toc158475841)

[3.2.3 Aplicação para distribuições conhecidas 24](#_Toc158475842)

[3.3 Construção da Regressão Logística 27](#_Toc158475843)

[3.4 Conclusões 30](#_Toc158475844)

[Capítulo 4: Boosting 32](#_Toc158475845)

[4.1 AdaBoost 32](#_Toc158475846)

[Capítulo 5: Support Vector Machine 37](#_Toc158475847)

[5.1 Caso Não Linearmente Separável 41](#_Toc158475848)

[5.2 Máquina de Vetor de Suporte 44](#_Toc158475849)

[5.2.1 SVM como Método de Penalização 45](#_Toc158475850)

[5.2.2 Classificação Multiclasse 46](#_Toc158475851)

[5.3 SVM para Regressão 47](#_Toc158475852)

[5.4 Aspectos Práticos 49](#_Toc158475853)

[Capítulo 6: Rede Neural 51](#_Toc158475854)

[6.1 Estrutura da Rede Neural 51](#_Toc158475855)

[6.2 Algoritmo de Backpropagation 54](#_Toc158475856)

[6.3 Escolhendo a Função Custo e as Não-Linearidades 58](#_Toc158475857)

[6.3.1 Observando a Camada de Saída 58](#_Toc158475858)

[6.3.2 Observando as Camadas Escondidas 59](#_Toc158475859)

[6.4 Regularização 60](#_Toc158475860)

[Capítulo 7: Feature Selection 61](#_Toc158475861)

[Capítulo 8: Principal Component Analysis 63](#_Toc158475862)

[8.1 Formulação da Máxima Variância 64](#_Toc158475863)

[8.2 Detalhes Importantes 65](#_Toc158475864)

[8.3 Relação com a Decomposição SVD 66](#_Toc158475865)

[Capítulo 9: Avaliação de Desempenho e Seleção de Modelo 67](#_Toc158475866)

[9.1 Métricas para Classificação Binária 67](#_Toc158475867)

[9.1.1 Acurácia 67](#_Toc158475868)

[9.1.2 True Positive Rate (TPR) ou Sensibilidade 67](#_Toc158475869)

[9.1.3 False Positive Rate (FPR) 67](#_Toc158475870)

[9.1.4 Precisão 68](#_Toc158475871)

[9.1.5 *Recall* 68](#_Toc158475872)

[*9.1.6* F1*-score* 68](#_Toc158475873)

[9.1.7 F-*score* 69](#_Toc158475874)

[9.1.8 *Receiver Operating Characteristic* (ROC) 69](#_Toc158475875)

[9.2 Métricas para Classificação Multiclasse 70](#_Toc158475876)

[9.2.1 Acurácia 70](#_Toc158475877)

[9.2.2 Acurácia Balanceada 71](#_Toc158475878)

[9.2.3 Métricas Macro 71](#_Toc158475879)

[9.2.4 Métricas Macro Ponderadas (*weighted*) 72](#_Toc158475880)

[9.2.5 Métricas Micro 72](#_Toc158475881)

[9.3 Métricas para Regressão 72](#_Toc158475882)

[9.3.1 *Mean Squared Error* (MSE) 73](#_Toc158475883)

[9.3.2 *Root Mean Squared Error* (RMSE) 73](#_Toc158475884)

[9.3.3 *Mean Absolute Error* (MAE) 73](#_Toc158475885)

[9.3.4 *Mean Absolute Percentage Error* (MAPE) 73](#_Toc158475886)

[9.3.5 Coeficiente de Correlação de Pearson (PCC) 74](#_Toc158475887)

[9.3.6 Coeficiente de Determinação () 74](#_Toc158475888)

[9.4 Métodos de Validação 75](#_Toc158475889)

[Capítulo 10: 76](#_Toc158475890)

[Capítulo 11: Apêndices 77](#_Toc158475891)

[Capítulo 12: Referências 93](#_Toc158475892)

# Introdução

* Tipos de aprendizado (supervisionado, não-supervisionado, semi-supervisionado, federado, por reforço).
* Teoria da decisão.
* Tipos de modelos (paramétrico x não-paramétrico; generativo x discriminativo)
* Estimação de uma função (minimização do valor esperado de uma certa *loss*) [1].
* Função *loss* x função custo.
* Lista de principais *losses?* Ou fica para um apêndice?

# Estimação de Parâmetros

Para entendermos os métodos desta seção, precisamos lembrar do Teorema de Bayes:

em que

: **Probabilidade a priori** de a distribuição que gerou os dados tenham como parâmetro.

Probabilidade de os dados terem sido gerados. O símbolo resume o acontecimento de um conjunto de eventos. Se estivermos considerando um experimento em que uma moeda é lançada N vezes, teremos uma variável aleatória que assume valor 0 (coroa) e 1 (cara). poderia representar, por exemplo, o conjunto de 3 lançamentos, ou seja, . Assim, representaria a probabilidade de acontecer essa sequência de resultados.

: **Probabilidade a posteriori**, ou seja, é a probabilidade de que seja o parâmetro da distribuição que gera os dados, sabendo que os dados foram gerados a partir dessa distribuição.

: **Função de verossimilhança** (*likelihood*), que é a probabilidade de os dados terem sido gerados por uma distribuição com parâmetro dado. Normalmente, em problemas de estimação, temos os dados e tentamos determinar . Dependendo do contexto, ela também costuma ser definida como [2, p. 122]

em que é o número de amostra contidas nos dados. Lembrando que, . Logo, é só uma questão de como interpretar **:** como uma informação a priori ( ou como um parâmetro da lei de probabilidade ().

Em geral, quando falamos de *machine learning*, as probabilidades a priori e a posteriori e a verossimilhança são sempre representadas por essas probabilidades mostradas acima. No entanto, em geral, em qualquer outro problema de estatística, as probabilidades a priori e a posteriori vão depender do ponto de vista. Em dado exemplo, podemos considerar como sendo a probabilidade a priori e a probabilidade posteriori, mas se invertermos o ponto de vista, podemos também considerar que a e a são as probabilidades a priori e a posteriori, respectivamente.

## Maximum Likelihood Estimation (MLE)

Estimamos os parâmetros somente com base nas evidências (dados). Para isso, maximizamos a função de verossimilhança da distribuição, isto é,

Conhecendo-se a expressão de , torna-se fácil resolver esse problema. Isso nem sempre é possível, pois nem sempre conhecemos a distribuição geradora dos dados . No caso de lançamentos de moedas, como veremos no exemplo abaixo, podemos supor que os dados tem distribuição de Bernoulli com parâmetro *.* Mesmo nos casos em que não conhecemos a distribuição dos dados, ainda é possível realizar hipóteses e assumir que eles seguem alguma distribuição conhecida (Benoulli, Gaussiana...).

Lembrar que, usualmente, quando nos referimos à expressão das distribuições usamos uma notação como , sem deixar explícitos os parâmetros. No entanto, é só uma questão de notação e poderíamos escrever , ou . Cada notação interpreta os parâmetros de uma maneira diferente, como já foi discutido no início do capítulo.

É importante perceber que toda probabilidade pode ser interpretada como uma probabilidade condicional, por mais que a informação a posteriori não esteja explicitamente indicada na expressão matemática. Assim, de maneira resumida, quando escrevíamos apenas nas aulas de probabilidade e estatística, era só uma maneira resumida de escrever , em que é algum conhecimento a posteriori (os parâmetros da distribuição, por exemplo, que estavam implícitos). Em [3, p. 59], é feita uma ótima discussão sobre isso.

Para finalizar, é necessário prestar atenção que, quando utilizamos a notação , estamos assumindo que não temos nenhuma outra informação a priori, nem mesmo a distribuição dos dados e, por isso, não podemos utilizar as expressões conhecidas das funções de distribuição de probabilidade.

Exemplo 1

Consideramos uma moeda que foi lançada 5 vezes, dando como resultado . Queremos determinar a distribuição de probabilidades que representa os resultados dessa moeda. Podemos dizer que é uma distribuição de Bernoulli com parâmetro (probabilidade de sucesso, que será representado pelo resultado “Cara”).

Usando o critério de MLE, desejamos que a *likelihood* , seja a maior possível, ou seja, a probabilidade de que os dados tenham vindo de uma distribuição de Bernouilli com parâmetro dado. Se considerarmos que os lançamentos são independentes, temos

Como, e , temos

Para maximizar a expressão acima, fazemos

A única solução coerente para esse problema é a solução para

Com isso, a partir das evidências, chegamos à conclusão de que a moeda é viciada. No entanto, podemos argumentar que os dados não são representativos e que precisaríamos de mais dados para chegar a um resultado mais acurado. De toda forma, o método nos dá um mecanismo para estimar a probabilidade de sair “Cara”.

Se tivéssemos um número genérico n de “Caras” e m de “Coroas”, com , teríamos uma expressão do tipo

Essa expressão é muito difícil de derivar. Um possível artifício que podemos utilizar é aplicar o logaritmo, o que nos daria

ficamos com uma soma em vez de um produto, que é muito mais simples de derivar.

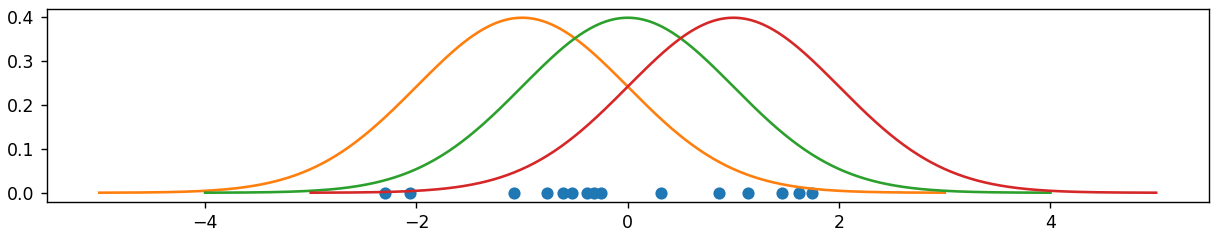
À primeira vista isso pode parecer estranho, mas, se repararmos, o ponto de mínimo de também é o ponto de mínimo de . O termo é chamado de ***log likelihood****.*

Assim, prosseguimos fazendo

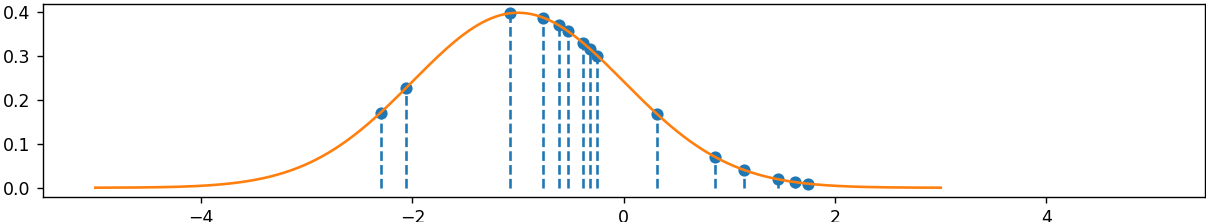
que é justamente a proporção de “Caras” no experimento.

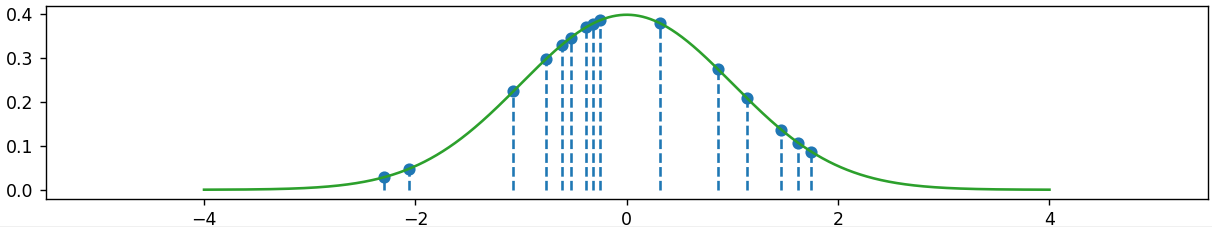
Exemplo 2

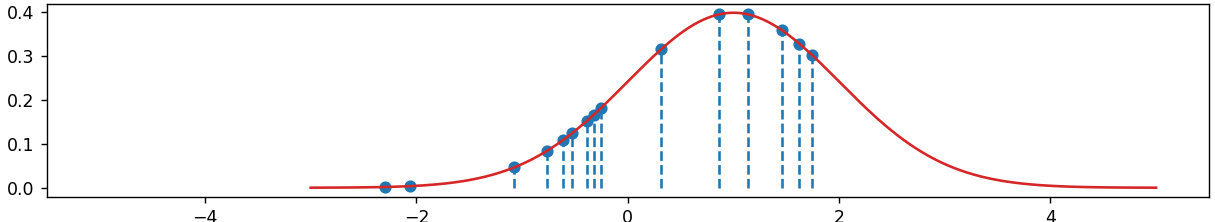
Vamos considerar que agora temos alguns dados e sabemos que eles seguem uma distribuição Gaussiana, mas com parâmetros desconhecidos e . Nosso trabalho, novamente, é encontrar o valor desses parâmetros ao tentar maximizar a *likelihood* , com (aqui estamos usando no lugar de por se tratar de uma distribuição contínua e não mais de uma distribuição discreta). Intuitivamente, estamos tentando encontrar a curva representativa da distribuição Gaussiana que se encaixa melhor nos dados. Na imagem abaixo, observamos os dados em azul e três exemplos de gaussianas que poderiam ter gerado esses dados.



Abaixo, as três Gaussianas são representadas em gráficos separados e os pontos são projetados sobre as curvas para facilitar a análise.







A partir dessa análise visual, podemos ver que as Gaussianas em laranja e verde são as que mais parecem ter gerado os dados em azul.

Intuitivamente, é isso que fazemos: variamos os parâmetros até encontrar a curva que compreende os dados de maneira mais “coerente”, ou seja, encontramos a curva mais provável de ter gerado esses dados. Isso é o equivalente a encontrar os parâmetros que dão o maior valor da *likelihood* .

Como temos dados supostamente gerados independentemente, a *likelihood* pode ser escrita como

Assim, queremos que esse produto seja o maior possível. Falando de maneira simplificada e visual, queremos encontrar tal que os pontos estejam arranjados em sua maioria mais próximos do pico da gaussiana do que das caudas, pois assim, o produto será o maior possível.

Partindo para a análise matemática, teremos um sistema de duas equações: uma considerando a derivada com relação a e outra com relação a , como mostrado abaixo:

O produtório de torna as derivadas um pouco inconvenientes. Por isso, adotamos um procedimento similar ao do exemplo anterior e tentamos minimizar a *log likelihood.*

Com isso, teremos

Por sorte, a primeira equação desse sistema é independente de , o que facilita as contas.

Lembrando que, , a primeira equação fica

Ao desenvolver a segunda equação, encontramos

Portanto, para encontrar o valor dos parâmetros da distribuição gaussiana mais provável de ter gerado os dados, pelo critério MLE, basta substituir os valores de na equação acima.

## Maximum A Posteriori (MAP) Estimation

Estimamos os parâmetros com base nas evidências (dados), mas também em conhecimento a posteriori. Com isso, o que fazemos é calcular

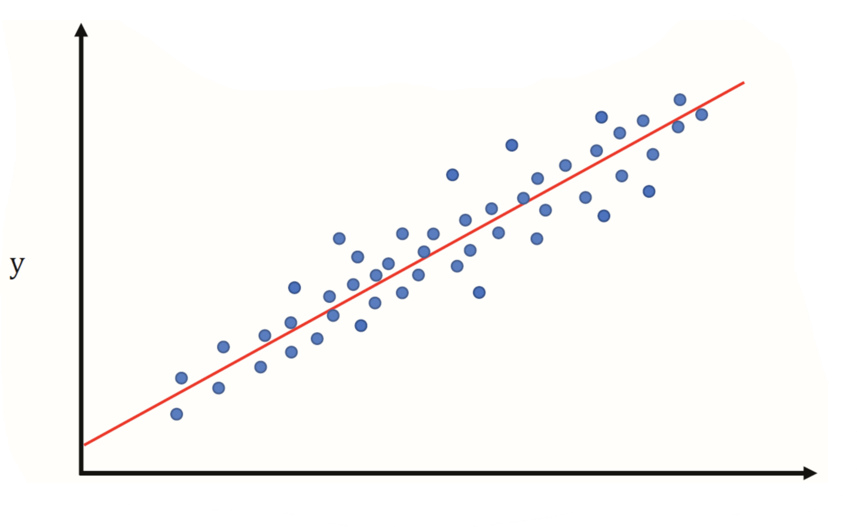
Diferentemente do caso MLE, não temos uma expressão direta para , pois, normalmente, não conhecemos uma expressão para a distribuição de probabilidade do parâmetro . Por isso, nos utilizamos do teorema de Bayes e reescrevemos essa equação como

# Regressão Linear

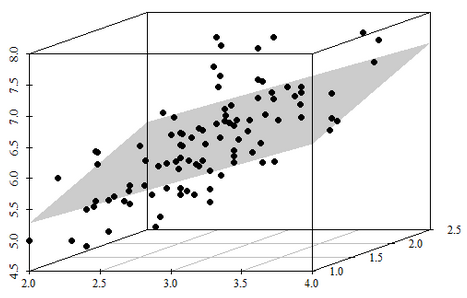
O problema de regressão linear consiste em criar um modelo que consiga relacionar variáveis com uma saída de referência por meio de uma equação linear da seguinte forma:

em que , e . O termo recebe é conhecido como ***bias*** ou ***intercept***.

No caso em que temos apenas uma variável , o problema consiste em encontrar a reta descrita pela equação , que aproximar se ajustar aos pontos , em que é o valor de referência da variável . Assim, o objetivo é que, com essa equação, consigamos fazer com que da melhor maneira possível os valores de referência , como ilustra a figura abaixo.



Quando temos um problema em que há duas variáveis de entrada, ou seja, , o problema é parecido, mas, para representa-lo visualmente, precisamos de um espaço de três dimensões, como mostrado na figura abaixo.



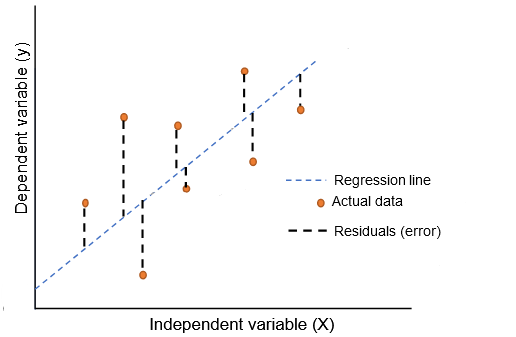
Com isso, podemos perceber que o problema da regressão linear consiste em encontrar o **hiperplano** que melhor descreve a relação entre as variáveis e a saída . O caso da reta e do plano mostrados acima são apenas casos particulares do hiperplano em que os vetores pertencem ao e ao , respectivamente.

Agora, como determinar os valores de que definem esse hiperplano? A seguir, são mostradas diferentes interpretações desse problema que levam a mesma solução.

## Diferentes Interpretações da Regressão Linear

### Ponto de Vista de Otimização

Uma maneira de resolver esse problema é encontrar o tal que a diferença entre os valores preditos e o valores de referência sejam os menores possíveis, levando em consideração todos os pares existentes no conjunto de dados. Essa diferença é comumente chamada de **erro** ou **resíduo**. No caso em que temos algo similar ao mostrado na imagem abaixo:



Assim, queremos que a soma de todos os resíduos em módulo seja a menor possível, ou seja, queremos algo como , em que . No entanto, se levarmos em consideração que para utilizar métodos tradicionais de minimização teríamos que derivar essa expressão, percebemos que talvez a ***loss*** não seja a melhor escolha.

Uma alternativa seria utilizar como *loss* o erro quadrático que é facilmente derivável e não altera o objetivo final, pois minimizar a soma dos erros quadráticos é equivalente a minimizar o módulo dos resíduos (o ponto de ótimo será o mesmo).

Com isso, adotamos como **função custo** a ser minimizada a função descrita abaixo:

O termo , que ainda não tinha sido considerado, surge apenas para simplificar futuras derivações, em que o 2 advindo do expoente cancela com o termo Novamente, isso não altera o resultado final, pois

Para encontrar valor de que minimiza a função custo, derivamos e igualamos a zero:

Com isso, vemos que o ótimo é aquele que satisfaz a equação acima.

Na prática, uma forma de se resolver esse problema é utilizar o algoritmo do gradiente descendente, em que escolhemos um inicial aleatório para ser nosso ponto de partida e, a cada iteração, movemos esse ponto na direção de máxima decida, ou seja, a cada iteração, fazemos

em que é a taxa de aprendizado e controla o tamanho do passo que será dado na direção de maior descida.

Apesar de podermos aplicar o método do gradiente descendente, há um outro método muito mais direto e que resolve o problema da regressão linear em uma iteração apenas, como veremos a seguir.

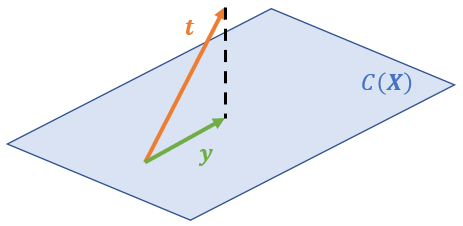
|  |
| --- |
| **Observação: *Loss function x Cost function***  ***Loss function*** Função utilizada para medir o erro entre o valor de referência e o valor predito . Nesta seção, foram vistos dois exemplos: o erro absoluto e o erro quadrático .  ***Cost function***  Função utilizada para medir o custo total por se adotar como parâmetro, considerando todas as observações do conjunto de dados Muitas vezes, algumas pessoas usam de maneira intercambiável os termos *loss function* e *cost function*, apesar de serem diferentes.  Exemplo: |

### Ponto de Vista de Álgebra Linear

O nosso problema de relacionar variáveis a uma saída pode ser representado de maneira vetorial por meio da seguinte equação

em que e

Idealmente, desejaríamos que , em que , porém, normalmente, essa equação não tem solução, pois , ou seja, não pertence ao espaço coluna de . Uma possível solução para esse problema é encontrar um vetor que está mais próximo de do que qualquer outro vetor, ou seja, queremos . Evidentemente, esse vetor precisa ser necessariamente a projeção de em como ilustra a figura abaixo.



Com auxílio dessa figura, reparamos que é ortogonal a , isto é, Como consequência disso, temos que o produto interno de por qualquer vetor da coluna de é nulo, ou seja, . Logo, chegamos à equação

que possui uma solução, diferentemente de . Se for invertível (que normalmente é, a não ser que admita várias soluções, o que não é o caso no nosso problema), podemos escrever

|  |
| --- |
|  |

Assim, conseguimos resolver o problema da regressão linear com uma única equação em um único passo.

**Bônus:**

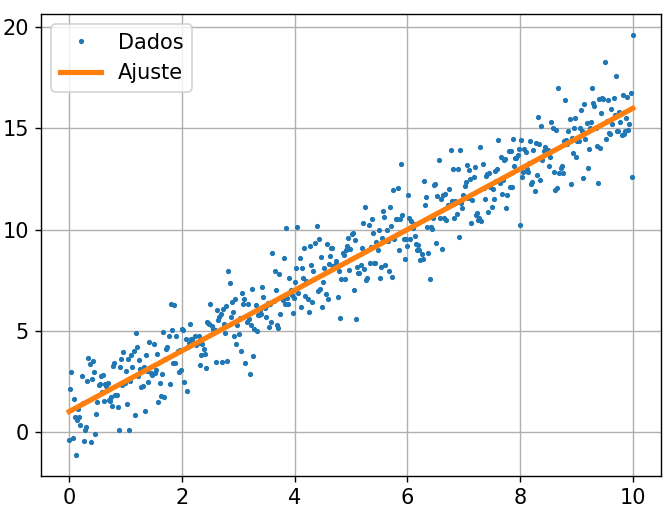
Se repararmos, o que desejamos é , que é equivalente a

em que é a função custo encontrada na Seção 3.1.1.

Além disso, essa equação poderia ter sido resolvida mais facilmente na forma matricial, fazendo

### Ponto de Vista Probabilístico

Também é possível chegar ao mesmo resultado adotando uma abordagem probabilística. Para isso, assumimos que a equação que define a geração dos pontos é dada por , ou seja, é um hiperplano definido por mais uma perturbação . Na imagem abaixo, a reta em laranja representa o hiperplano e o pontos em azuis são gerados por . O que gostaríamos de obter é a curva laranja, que é totalmente definida pelo parâmetro , porém, só conhecemos os dados , não conhecemos os valores de correspondentes a .



Uma possível suposição é de que , o que faz com que .

Assim, podemos aplicar a estimação de máxima verossimilhança (MLE) para determinar o parâmetro .

Para começar, sabemos que

Se considerarmos todos os pares de e considerarmos que eles são gerados de maneira independente, teremos

Seguindo um procedimento similar ao visto na Seção 2.1, aplicamos a função log (base e) para encontrar a log verossimilhança:

Com isso, passamos para a etapa de maximizar a log verossimilhança, o que é equivalente a minimizar o negativo da log verossimilhança. Normalmente, é preferível esse ponto de vista de “minimização” em vez de “maximização”, pois, eventualmente, podemos considerar o negativo da log verossimilhança como uma função custo, que normalmente é uma função que visamos normalizar:

Portanto, ao minimizarmos essa função custo obtemos

que é justamente à conclusão que tínhamos chegado na Seção 3.1.1 e que é equivalente a minimizar a função custo

## Regressão Polinomial

É uma modalidade da regressão linear em que temos uma variável de entrada e a substituímos por variáveis que são potências de . Em geral, funções substituem as variáveis antigas são chamadas de **funções de base**. Além disso, de forma geral, podemos chamar essas novas variáveis formadas pelas funções base de **atributos** ou ***features***. Dependendo da interpretação, também podemos chamar as variáveis de *features*, mas geralmente, o que temos nesse caso, na verdade, são funções base identidade na forma .

Normalmente, escolhemos essa abordagem quando não conseguimos modelar os dados com uma equação na forma

e precisamos recorrer a uma modelagem não linear da relação entre e .;

Assim, utilizamos um modelo na forma

|  |
| --- |
|  |

em que é o grau do polinômio e .

Por mais que existam termos de ordem maior do que 1 e que a relação entre e seja não linear, ainda temos uma regressão linear, pois a relação entre e os termos é linear. Se considerarmos todos os dados, independentemente da relação que cada *feature* mantém entre elas, ainda temos uma equação linear , em que corresponde à matriz de dados , a variável independente corresponde a e

Por mais que essa seja a explicação oficial do porquê de essa regressão ainda ser linear, ainda acho mais lógico ela ser linear pelo fato de ser linear com relação às *features* e podermos escrever uma equação linear . Fazendo uma comparação, nas seções anteriores, tínhamos um vetor de variáveis de entrada e uma equação similar: . A princípio, não sabemos se as variáveis são independentes entre si ou se elas têm algum tipo de relação entre elas. É possível que ( sendo a largura de um terreno quadrado e sendo a área desse terreno, por exemplo), que é o caso em que teríamos algo que lembra uma regressão polinomial e, mesmo assim, ainda temos uma regressão linear.

## Forma Geral da Regressão Linear

Percebemos ao longo deste capítulo que a regressão linear é um problema cujo objetivo é encontrar uma equação que relacione de maneira linear uma variável de saída com variáveis (que podem ser dependentes entre si ou não), por meio de uma equação na forma

|  |
| --- |
|  |

sendo que o parâmetro ótimo é dado por

|  |
| --- |
| . |

O caso da regressão polinomial é apenas um caso particular, em que forçamos a dependência entre as variáveis . No início do capítulo tínhamos outro caso particular, só que não forçamos nenhuma relação entre as variáveis de entrada que nos foram dadas. Tínhamos .

# Regressão Logística

O modelo de regressão logística, apesar do nome, não é um modelo de regressão, mas sim, de classificação. Ele faz parte de um conjunto de **modelos discriminativos**, que associam a cada classe do problema uma **função discriminante** [4, p. 101], de forma que, associamos o exemplo à classe se . Mais especificamente, na regressão logística, essa função discriminante é a probabilidade a posteriori . Alguns exemplos de modelos discriminantes são: regressão logística, SVM, árvore de decisão.

Em oposição, existem os **modelos generativos**, que modelam a probabilidade a priori e a verossimilhança para só depois encontrar a probabilidade a posteriori por meio do teorema de Bayes.

É interessante ressaltar que nos dois grupos de modelos, busca-se determinar justamente porque, pela teoria de decisão, um determinado exemplo deverá ser classificado como classe se , ou seja, atribuímos à classe cuja probabilidade a posteriori for a maior dentre todas as classes.

No modelo da regressão logística, a probabilidade a posteriori é modelada por

em que , é uma função base de e é a função sigmoide logística, dada por

|  |  |
| --- | --- |
|  | Sigmoid function - Wikipedia |

Com isso, atribuímos o exemplo , correspondente às *features* ,à classe com maior .

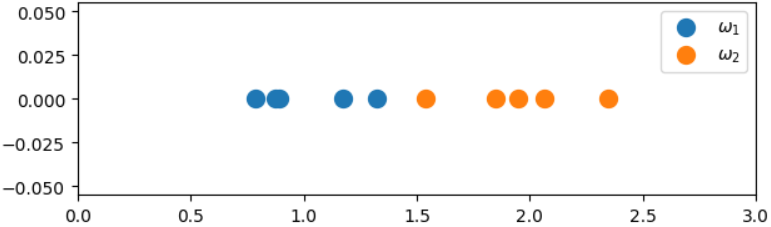
Para chegar a esse modelo, existe todo um desenvolvimento que será abordado a seguir.

Antes de começarmos, é importante ressaltar que, como o problema é de classificação, o *target* não assume mais valores decimais. Caso o problema tenha um número de classes igual a 2, consideramos , em que cada valor de indica uma classe diferente. Caso , adotamos uma codificação *one-hot* para , em que temos um vetor de tamanho cujas entradas são todas nulas, exceto na posição , que vale 1, indicando que o exemplo em questão pertence à classe . Um ponto pertencente à classe , por exemplo, teria um vetor de *target* da seguinte forma:

Passemos, agora, ao desenvolvimento que leva à criação do modelo da regressão logística.

## Mínimos Quadrados Para Classificação

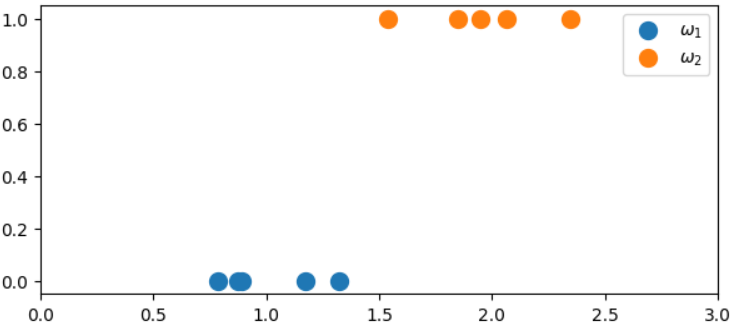
Consideremos um problema de classificação em que temos conjuntos de dados que pertencem a duas classes distintas, como ilustra a imagem abaixo:



Como criar um modelo matemático para, dados novos pontos, conseguir classificá-los em classe ou ? Se conhecêssemos bem as distribuições que geraram esses pontos, poderíamos propor um valor de a partir do qual passaríamos a classificar os pontos como classe . Por exemplo, se soubéssemos que e são as variáveis aleatórias que geram essas duas classes de pontos, poderíamos propor uma fronteira de decisão passando em , na metade do caminho entre as médias das duas Gaussianas.

No entanto, em quase todos os casos, não temos essa informação e precisamos encontrar um modelo para classificar os pontos mesmo sem saber as funções de distribuição geradoras.

Uma possibilidade mais simples seria utilizar o método dos mínimos quadrados. Mas como fazer isso se temos pontos alinhados em uma única dimensão, com mesmo valor de ? Podemos codificar a informação presente nas cores em número, por exemplo, fazendo para a classe (azul) e para a classe (laranja), o que nos daria a seguinte representação:



Com isso, fica um pouco menos obscura a ideia de utilizar mínimos quadrados para encontrar uma função que se ajuste a esses dados. O ideal seria que essa função assumisse o valor zero quando pertencesse a e assumisse o valor caso contrário. No entanto, só conseguiríamos encontrar uma reta desse tipo somente se todos os pontos azuis estivessem concentrados em um mesmo valor e todos os pontos laranjas estivessem concentrados em um mesmo valor de . Claramente isso não acontece e o que temos, na realidade, é um modelo em que pode assumir qualquer valor real, como mostrado na Figura 4‑1.

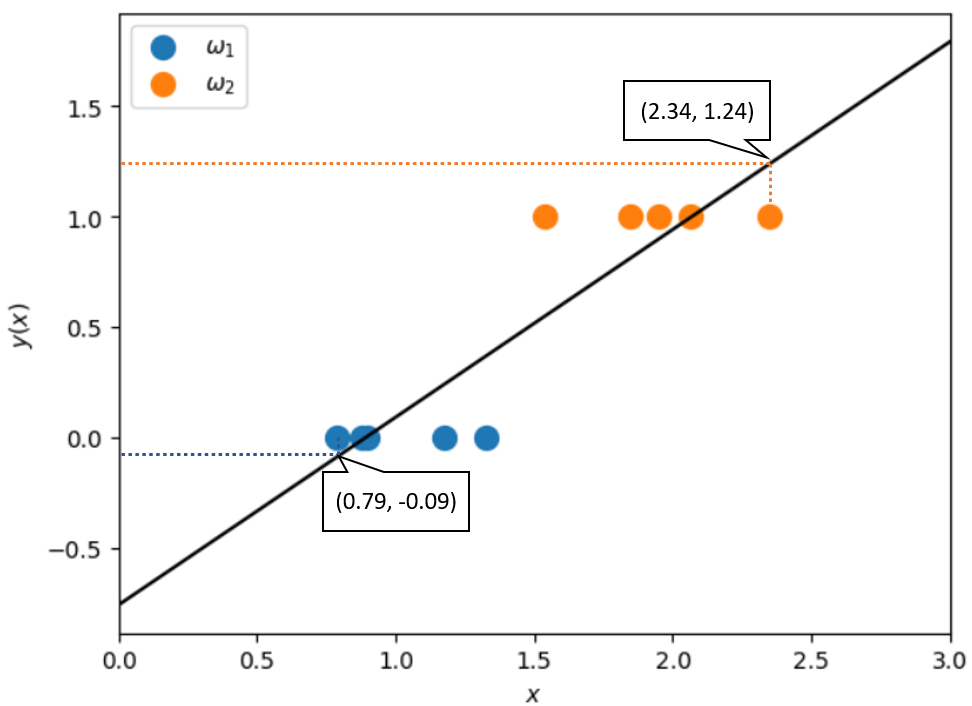


Figura 4‑1: Ajuste de uma reta aos pontos das classes azul e laranja.

Uma solução para isso é adotarmos a regra de que, para , associamos a e associamos a caso contrário. Com essa regra bastante intuitiva, separamos perfeitamente os pontos da imagem acima.

E no caso em que temos 3 classes, por exemplo, como mostra a Figura 4‑2?

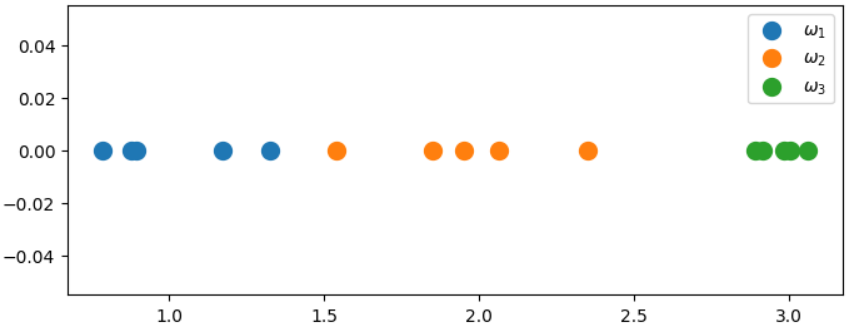


Figura 4‑2: Problema multiclasse.

Nesse caso, existem diferentes abordagens. Em [5, p. 183], Bishop menciona algumas delas:

* Um contra um, em que se adota uma função discriminante na forma para cada par de classes . Se classificamos como e, caso contrário, classificamos como . Essa abordagem gera uma região de indecisão, formada por pontos que são atribuídos a mais de uma classe, ou seja, quando para o mesmo ponto , existe mais de um (Figura 4‑3).  
  Observar que as fronteiras de decisão da figura são curvas de nível do hiperplano , e são encontradas fazendo , que é o limiar entre uma classe e outra. Assim, em um exemplo em que tivéssemos , é a nossa função discriminante, que é um plano no espaço tridimensional (pode ser reescrito como para facilitar a visualização) e é uma reta (que pode ser reescrita como para facilitar a visualização), contida no mesmo plano onde se encontram os pontos .
* Um contra o resto, em que temos funções discriminante e, se , dizemos que pertence à classe . Caso contrário, dizemos que não é da classe . Essa abordagem gera uma região de indecisão, formada por pontos que não foram classificados como nenhuma classe, ou seja, pontos em que (Figura 4‑4). Aqui, as fronteiras de decisão da imagem também são curvas de nível da função discriminante.
* Abordagem em que temos uma função para cada classe e atribuímos à classe que tiver maior valor de Nesse caso, não são criadas regiões de indecisão, pois, excetuando as interseções entre os hiperplanos discriminantes, sempre haverá .

|  |  |
| --- | --- |
| Figura 4‑3: Um contra um. | Figura 4‑4: Um contra o resto. |

Dessa forma, a abordagem que parece mais razoável para nosso problema é a terceira, já que não são criadas regiões de indecisão. Nela, poderíamos utilizar o método dos mínimos quadrados para encontrar as funções discriminantes . No entanto, as fronteiras de decisão são mais difíceis de encontrar, quando comparamos com os dois outros métodos, principalmente no caso multiclasse, pois elas são definidas pelas regiões em que cada curva tem seu valor de maior do que o de todas as outras classes.

Uma propriedade interessante dessa abordagem é que [5, p. 185], o que é muito similar ao que temos em medidas de probabilidade. Apesar disso, não pode ser considerado uma medida de probabilidade, pois não está restrito apenas ao intervalo

Portanto, aplicando a terceira abordagem ao problema multiclasse ilustrado na Figura 4‑2, obtemos uma reta para cada classe, como ilustrado na Figura 4‑5. Observamos que, para modelar cada , precisamos a cada instante considerar a classe com e todas as outras com .

Percebemos que, para , o modelo dos mínimos quadrados para classificação começa a apresentar alguns problemas. A classe , por exemplo, apresenta uma curvaque atribui valores baixos e mais ou menos próximos de para todos os pontos, mesmo que eles pertençam a outras classes. Isso faz com que os pontos de sejam classificados incorretamente como pertencentes às outras classes, cujos são maiores que

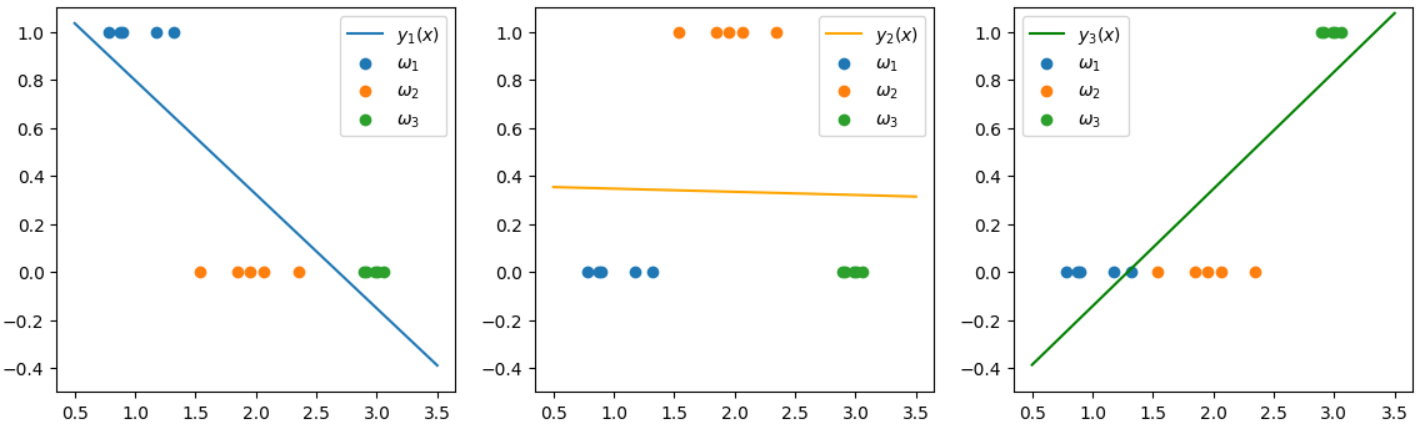


Figura 4‑5: Abordagem em que se tem uma regressão linear para cada classe (terceira abordagem).

Por fim, podemos resumir esse problema em uma única equação vetorial:

em que , , e   
 Lembrando que é o vetor de *target* na codificação *one-hot* e é o vetor aumentado, ou seja, .

## Modelando a Probabilidade A Priori

Na seção anterior, vimos que o modelo dos mínimos quadrados pode ser utilizado em problema de classificação. Por outro lado, vimos também que ele não é muito adequado por alguns fatores: não transmitir uma noção de probabilidade (valor não estão restritos a intervalos ), dificuldades para classificação com .

Por isso, nesta seção, estudamos uma forma de escrever uma equação para probabilidade a posteriori que possa auxiliar na construção de um modelo para classificação.

### Caso

Podemos utilizar o Teorema de Bayes para modelar a probabilidade a posteriori da seguinte maneira:

Com algumas manipulações, podemos reescrever essa equação da seguinte maneira:

que é equivalente a

Por curiosidade, percebemos que pode ser escrita com uma composição de funções dela mesma, ou seja,

Ora, se , então . Assim, notamos que a inversa da função sigmoide é dada por

que é conhecida como **função logit**.

### Caso

Para mais de duas classes, podemos escrever a probabilidade a posteriori da classe como

em que .

A função

com ,é conhecida como **softmax**. Observar que é necessário dar como entrada tanto quanto o índice . Ela é o caso geral da função sigmoide.

### Aplicação para distribuições conhecidas

Se formos aplicar as equações desenvolvidas acima em casos em que conhecemos a *likelihood*, como no caso da distribuição normal, exponencial, discretas binárias, encontramos probabilidades a priori com o seguinte formato

|  |  |
| --- | --- |
|  |  |
|  |  |

A expressão para varia de acordo com a distribuição [5, pp. 198-203].

Com isso, percebemos que, para várias distribuições bastante comuns, temos uma probabilidade a posteriori que é dada pela *softmax* (o que, por generalização, inclui a sigmoide) de uma função linear. Isso faz com que as fronteiras de decisão entre essas classes sejam hiperplanos.

Tomemos por exemplo o caso em que sabemos que os dados pertencem às classes e e que são gerados por distribuições gaussianas com parâmetros específicos para cada classe. Isso quer dizer que conhecemos as *likelihoods* e , com .

Para o caso em que as duas distribuições apresentam a mesma matriz de covariância temos probabilidade a posteriori como mostrado acima: . Para encontrar a fronteira de decisão, segundo a teoria de decisão, precisamos determinar:

que é a equação de uma reta no e de um plano no .

Um erro que poderia ser cometido é achar que o plano que correspondente a essa reta do no é a função No entanto, não podemos afirmar isso, pois a equação dessa reta não surgiu a partir de uma curva de nível de uma função , fazendo , mas sim, da equação .

Então, não é possível fazer o caminho inverso , pois não conhecemos o comportamento da variável em outros valores diferentes de . Por que não poderia ser , ou escrito de maneira equivalente, , que é igual a equação mostrada acima em ?

No , temos sempre 3 variáveis: , e . Nossa equação tem a forma . O também está representado nessa equação, mas de maneira implícita: . Isso nos indica que, e só possuem dependência entre eles e o valor de não influencia nos valores que essas duas variáveis podem assumi. Então, temos um plano paralelo ao eixo , pois, independentemente do valor de escolhido, a relação entre e é sempre a mesma: .

Para encerrar essa discussão, isso é só uma questão de ponto de vista. Se estamos trabalhando com representações 2D desse problema, representaremos a fronteira de decisão como uma reta no . Se estamos trabalhando com representações em 3D, representaremos nossa fronteira de decisão como um plano no .

A Figura 4‑7 e a Figura 4‑7 ilustram as curvas desse exemplo de diferentes pontos de vista. Na curva da probabilidade a posteriori pode parecer que ela representa uma função de densidade de probabilidade (contínua) de . Para que isso fosse verdade, precisaríamos que

o que é um absurdo, já que e, por isso, não converge. Lembrando que, como é linear, tem a mesma forma da sigmoide, porém possivelmente deslocada e distorcida ao longo do eixo , no caso unidimensional, ou ao longo do plano formado por pelas componentes de , no caso multidimensional.

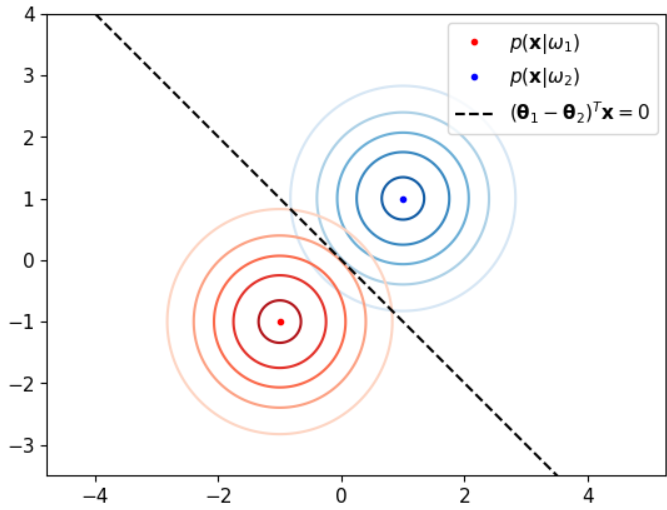


Figura 4‑6: Curvas de nível das likelihoods.

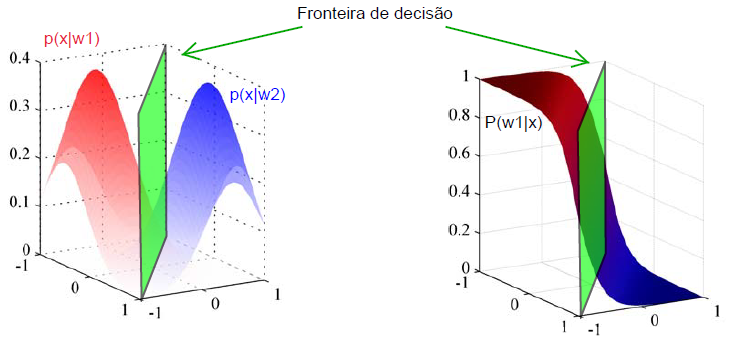


Figura 4‑7: Representação das likelihoods (à esquerda) e da função de probabilidade a posteriori (à direita). Nessas figuras, está representada a fronteira de decisão , só que aqui, representada no .

Em outras palavras, a aba vermelha do gráfico à direita na Figura 4‑7 se estende até o infinito. Isso faz sentido, já que, quanto mais além do plano da fronteira de decisão maior é a chance do ponto pertencer à classe . Logo, esse gráfico não representa o gráfico de uma função de distribuição de probabilidade.

No entanto, isso não quer dizer não seja uma p.d.f. Ela é, mas não em função de e sim de . Mais especificamente, ela é uma função de massa, pois ela é discreta. Repare que .

Uma última observação, é que podemos perceber perfeitamente o formato 3D da sigmoide na figura. Vemos também que a região em que a probabilidade de ser a classe é 0,5 (chances iguais de ser e ) é justamente uma reta ao longo da qual passa o plano representando a fronteira de decisão.

Para finalizar este exemplo, é importante relembrar que a expressão de depende dos parâmetros das duas Gaussianas, ou seja, e . Se por acaso só soubermos que as duas classes geram dados segundo uma distribuição Gaussiana, mas não conhecermos o valor desses parâmetros (o que é comum na realidade), podemos estimá-los por meio da estimação de máxima verossimilhança utilizando os dados . Com isso, determinamos os valores numéricos de caso os parâmetros não sejam conhecidos.

## Construção da Regressão Logística

Na seção anterior, vimos que, para alguns casos de *likelihood,* podemos escrever a probabilidade a posteriori como a função sigmoide/softmax de uma função linear. Assim, conhecendo a *likelihood* dos dados gerados por cada classe, conseguimos escrever uma equação para com auxílio do teorema de Bayes.

No entanto, na grande maioria das vezes, os dados não seguem exatamente as distribuições especiais da seção anterior e, normalmente, não conhecemos a distribuição deles. Com isso, seríamos obrigados a estimar suas distribuições de probabilidade, o que é uma abordagem completamente válida e é a marca dos modelos generativos, mas também pode gerar resultados ruins se a estimação não for adequada.

Uma alternativa seria, em vez de desenvolvermos um método em que precisemos estimar a verossimilhança para só assim calcularmos a posteriori, desenvolver um modelo discriminativo. É daí que surge a ideia da regressão logística.

O modelo da regressão logística consiste em generalizar a probabilidade a posteriori por meio da expressão

o que parece bastante natural, visto que várias distribuições têm expressões analíticas exatas para a posteriori dessa mesma forma.

Assim, mesmo que não conheçamos a distribuição dos dados, aplicamos a mesma expressão que vimos na seção anterior. A diferença é que antes tínhamos uma expressão exata para e, agora, temos algo estimado. Se antes tínhamos expressões analíticas exatas para calculadas a partir da expressão da verossimilhança conhecida/estimada e com auxílio do teorema de Bayes, agora, calcularemos a expressão da probabilidade a posteriori com auxílio da estimação de máxima verossimilhança sem conhecer a *likelihood*.

Observar que, aqui, substituímos o vetor de entradas por um vetor genérico de *features*, formado por funções base não lineares . Essas funções são importantes para separar dados que não podem ser separados linearmente, com fronteiras de decisão lineares. A Figura 4‑8 ilustra um exemplo em que foram utilizadas funções base gaussianas com centros marcados nas cruzes verdes. Com isso percebemos que com a escolha de funções base corretas, conseguimos separar os dados (no espaço original das entradas) usando uma fronteira de decisão circular. Observar também que no espaço das *features*, a fronteira de decisão é linear, da forma como desenvolvemos ao longo desta seção.

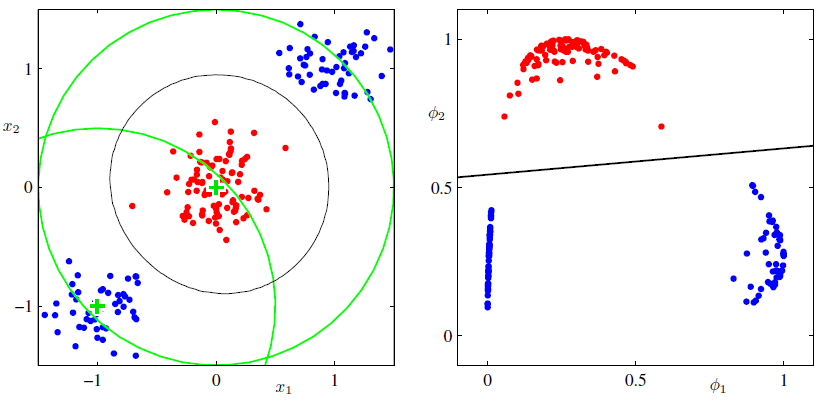


Figura 4‑8: À esquerda, dados no espaço original das entradas .À direita, a transformação desses dados para o espaço das features com funções base .

Dada a expressão da regressão logística, precisamos encontrar o parâmetro . Para isso, nos basearemos no princípio da estimação de máxima verossimilhança.

Precisaremos ficar atentos para não nos confundirmos. No início desta seção, foi sugerido usar a MLE para calcular os parâmetros a distribuição dos dados quando supúnhamos que eles eram gerados por uma distribuição específica conhecida (gaussiana). Nesse caso, tentávamos maximizar para cada classe , pois, no final, por meio do teorema de Bayes, conseguíamos escrever a expressão de em função desses parâmetros () específicos de cada classe.

Aqui, estimaremos o parâmetro diretamente por meio da MLE, sem tentar escrevê-lo em função de outros parâmetros, maximizando . É importante lembrar que , mas omitimos o para simplificar a notação. Se considerarmos que as amostras são independentes, teremos a seguinte expressão para a verossimilhança:

No caso de classificação binária, teremos duas possibilidades:

* ;
* .

Deixamos explícito nas expressões acima que é dado porque senão não ficaria claro que essa probabilidade está associada apenas a esse exemplo de índice . Além disso, reparar que manter o como uma informação dada é apenas uma notação. Poderíamos ter uma variável aleatória que codificasse isso. Por exemplo, poderíamos ter uma variável aleatória que representa o evento “classe a qual pertence o exemplo ” e poderíamos expressar as probabilidades acima como . Nesse último caso, também mostramos que não precisamos deixar o como uma informação dada, mais sim, como um parâmetro, o que é marcado explicitamente pelo ponto e vírgula.

Por mais que possa parecer confuso, a expressão que estabelecemos inicialmente para a posteriori, (no caso binário), é equivalente a Isso porque na expressão , temos o termo explicitamente. Logo, ele tem que ser um parâmetro dado, por mais que não apareça explicitamente na notação Lembrando que, dizer que é dado, não significa dizer que conhecemos os valores de suas componentes, pois ele pode ser “dado” e ainda assim ser uma variável desconhecida. O problema está na nomenclatura “dado”, que nesse caso, é o equivalente a dizer que estamos calculando a probabilidade do exemplo pertencer à classe condicionado a . Assim, fica mais claro que não se trata de probabilidades em que se tem valores conhecidos dados, mas sim, de probabilidades condicionadas a uma variável. Portanto, se temos , obviamente essa expressão está condicionada a , por mais que o vetor de parâmetros não se encontre explícito na expressão da probabilidade.

Depois dessa discussão, vamos voltar ao nosso problema de encontrar o valor de para o caso da classificação binária. Lembremos que, no caso binário, temos que . Nosso objetivo é maximizar com respeito a :

em que .

Por simplicidade, como de costume, minimizamos o negativo da log verossimilhança:

|  |  |  |
| --- | --- | --- |
| ­ |  | (4.1) |

A expressão dentro desse somatório é uma *loss* conhecida como **entropia cruzada** e é amplamente utilizada em problemas de classificação. Para o caso em que temos classes e o ponto sendo avaliado pertence a uma classe com , a expressão da entropia cruzada pode ser escrita como

|  |
| --- |
|  |

em que é a probabilidade de o ponto pertencer à classe e é a probabilidade de o ponto pertencer à classe sabendo qual a classe a qual ele realmente pertence, ou seja, Lembrando que essa expressão (considerando e da forma como definimos) é um caso específico do problema de classificação e foi derivada a partir da eq. (4.1). Na expressão geral da entropia cruzada (para problemas que não são necessariamente relacionados a *machine learning* ou a classificação) e são funções de densidade de probabilidade quaisquer (consultar Apêndice A:).

**Reparar que terá apenas uma parcela do somatório não nula.**

A função custo genérica para um problema de classificação com classes teria a seguinte forma:

|  |
| --- |
|  |

Ela poderia ter sido derivada da mesma maneira como fizemos para o caso binário.

Reparar que, apesar de termos derivado a expressão da entropia cruzada à medida que derivávamos a expressão da regressão logística, elas não são dependentes uma da outra. A entropia cruzada não surgiu do modelo de regressão logística. Ela poderia ter sido derivada de qualquer outro problema de classificação.

Tentando ver esse problema de uma forma mais intuitiva, o que estamos fazendo é minimizar a entropia cruzada, que quantifica a dissimilaridade entre as distribuições e (lembrando que minimizar a entropia cruzada é equivalente a minimizar a divergência KL, conforme Apêndice A:). Então, como , queremos fazer com que a probabilidade se aproxime o máximo possível de .

Por fim, para encontrar os parâmetros aplicamos o método *Iterative Reweighted Least Squares (IRLS),* que é baseado no método do Newton e consiste em atualizar o valor de a cada iteração da seguinte maneira:

em que [5, p. 207].

## Conclusões

Ao final de todo o desenvolvimento para se chegar ao modelo da regressão logística, percebemos que existe uma relação entre ele e o modelo dos mínimos quadrados para classificação.

No método dos mínimos quadrados para classificação, um dos pontos negativos era o fato de não termos funções que possam ser interprestadas como probabilidades, pois seus valores não se limitavam ao intervalo . Na regressão logística, é como se pegássemos o modelo dos mínimos quadrados que tínhamos desenvolvido e o empacotássemos na função logística sigmoide, obrigando, assim, que os valores fiquem limitados ao intervalo .

Obviamente, não é possível encontrar com a equação dos mínimos quadrados e substituir esse valor em , pois, só foi possível chegar a essa equação porque não havia incialmente a não linearidade da função sigmoide.

Por fim, é interessante reparar que, mesmo para os casos em que a distribuição dos dados pertence a uma daquelas distribuições especiais descritas na Seção 4.2.3, ainda é preferível usar o modelo da regressão logística em vez de usar as expressões analíticas para cada um desses casos particulares. Isso porque, na regressão logística, precisamos estimar consideravelmente menos parâmetros comparado com os métodos que se baseiam no teorema de Bayes. Por exemplo, se, num problema de classificação binária, tivermos vetores de *features* de dimensão e nossos dados seguirem uma distribuição Gaussiana, então, na regressão logística, teremos apenas parâmetros para estimar. Já utilizando o modelo baseado no teorema de Bayes teríamos que estimar parâmetros para as médias e parâmetros para a matriz de covariância [5, p. 205][6, p. 319].

# Boosting

O *Boosting* é um esquema iterativo, em que a cada iteração um *base learner* (também chamado de *weak learner* [5]) é treinado utilizando um conjunto de treinamento diferente. A geração desses conjuntos é feita ao atribuir pesos às amostras de treinamento, que são mudados à cada iteração. O resultado é um modelo de *boosting* obtido por meio da média ponderada de todos os modelos base (*base learners*) [6].

A seguir, são mostrados alguns dos principais modelos de *boosting*.

## AdaBoost

### Descrição do Algoritmo

Para definir o AdaBoost (*adaptive boosting*), focamos na tarefa de classificação binária. O objetivo é construir um classificador do tipo

|  |  |  |
| --- | --- | --- |
|  |  | (5.1) |

em queé uma amostra genérica de um conjunto de dados e representa o modelo final de *boosting*, dado por

O termo permite atribuir importâncias diferentes a modelos diferentes e representa o modelo base (binário) da iteração , definido em termos de um conjunto de parâmetros . A cada iteração, esses parâmetros são otimizados de maneira gulosa, ou seja, encontramos os seus valores ótimos para essa iteração, considerando fixo os valores dos parâmetros de outras iterações.

Para começarmos a detalhar a construção desse modelo, em uma certa iteração , podemos escrever a soma parcial dos termos, de maneira iterativa, como

ou, de maneira recursiva, como

Em , temos .

Como o algoritmo é executado de maneira gulosa, os termos das iterações anteriores, como , são considerados conhecidos.

Para encontrar os valores de e , é realizado uma otimização empregando a **loss exponencial**, dada por que é justamente um dos elementos que caracteriza o AdaBoost.

Se repararmos na Figura 5‑1, tanto nos casos em que a classificação foi correta (), quanto nos casos em que ela foi incorreta (), a função *loss* tem valor positivo, diferentemente da *loss* 0-1, que vale 1 quando a classificação é incorreta e 0 quando for correta. Mesmo assim, na *loss* exponencial, as classificações erradas levam a uma *loss* maior do que as certas. Além disso, a *loss* é exponencial é diferenciável, enquanto a *loss* 0-1 não é.

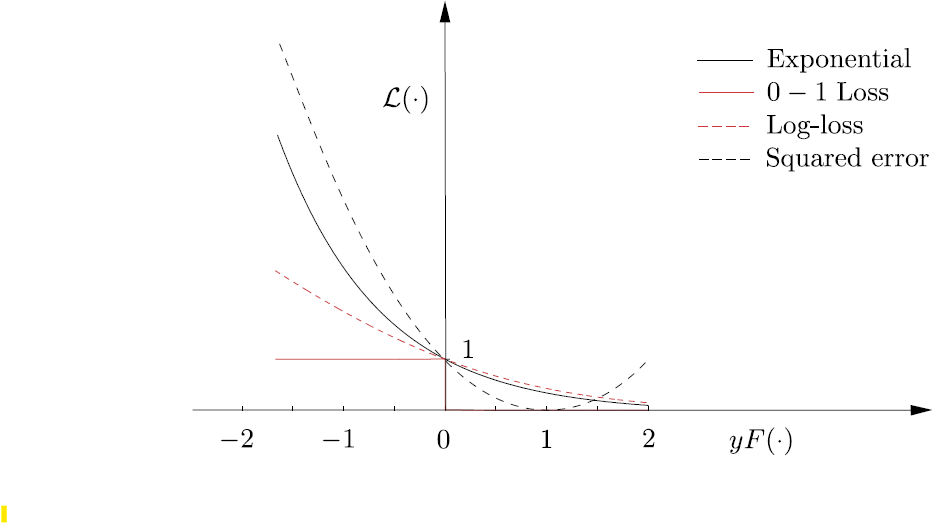


Figura 5‑1: Comparação de diferentes funções de loss.

O problema de minimizar a função custo com a *loss* exponencial é dado por

|  |  |  |
| --- | --- | --- |
|  |  | (5.2) |

|  |  |  |
| --- | --- | --- |
|  |  | (5.3) |

em que

|  |  |  |
| --- | --- | --- |
|  |  | (5.4) |

com sendo um fator de normalização para garantir e

|  |  |  |
| --- | --- | --- |
|  | . | (5.5) |

Como só depende da amostra de índice e , ele pode ser considerado o peso associado à amostra . Além disso, como na iteração não temos um modelo anterior , inicializamos os valores de em , pois assim, garantimos que inicialmente todas as amostras tenham o mesmo peso e que a eq. (5.5) é válida.

Reparar que , pois é constante em cada iteração.

Realizamos a otimização da eq. (5.3), primeiramente, com relação à , mantendo constante:

|  |  |  |
| --- | --- | --- |
|  |  | (5.6) |

em que

|  |  |  |
| --- | --- | --- |
|  |  | (5.7) |

Como é constante e , então:

* , ;
* , .

Portanto, fica claro que, de fato, o valor de que minimiza a eq. (5.6) também minimiza a eq. (5.7). Com isso, vemos que, apenas os pontos classificados incorretamente contribuem para o cálculo de . Portanto,

|  |  |  |
| --- | --- | --- |
|  |  | (5.8) |

Reparar que , pois, os pesos são normalizados.

Passamos para a otimização de :

A partir das equações (5.5) e (5.8), podemos escrever

Ao derivarmos com relação a e igualar a zero, obtemos

|  |  |  |
| --- | --- | --- |
|  |  | (5.9) |

Notar que, quando , , o que é esperado na prática.

Conhecendo os valores de e , podemos determinar e passar para a próxima iteração.

Com isso, podemos fazer algumas observações importantes:

1. Percebemos que os pesos assumem valores maiores nas iterações seguintes para as amostras classificadas incorretamente e valores menores caso contrário, pois, , já que as constantes e desaparecem dentro do argmin da eq. (5.3).
2. Vemos também que o termo representa a taxa de erro ponderada do modelo base da iteração (o que é mais facilmente visto pela eq. (5.7)). Quando aumenta, diminui. Logo, modelos que têm menor taxa de erro ponderada recebem maior peso durante a predição conjunta dos diferentes *base learners*.

A Figura 5‑2 resume o processo de treinamento e predição do algoritmo AdaBoost.

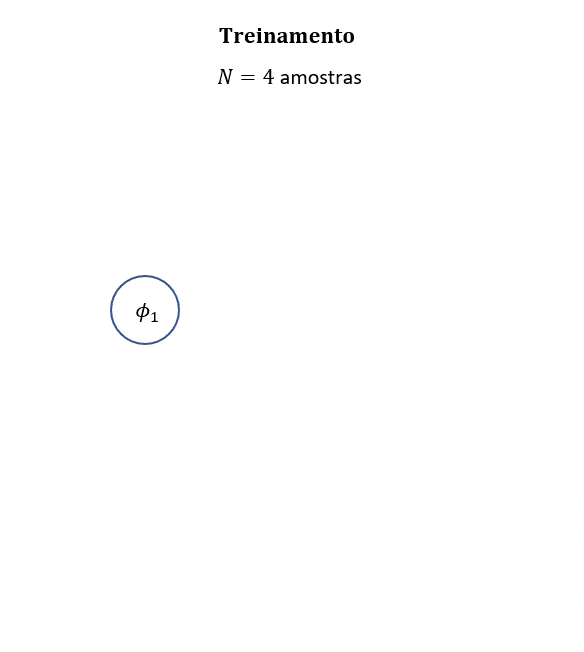


Figura 5‑2: Diagrama ilustrativo do AdaBoost. Cada círculo representa um weak learner.

### Discussão sobre a *loss function*

A escolha da *loss* exponencial para o modelo *AdaBoost*, descrito na Subseção 5.1.1, e a forma como a função de classificação da eq. (5.1) é definida não são arbitrárias. Para entender isso, olhemos para o valor esperado da *loss* exponencial com relação à variável aleatória que representa a classe de um determinado ponto

|  |  |  |
| --- | --- | --- |
|  |  | (5.10) |

A ideia transmitida por esse cálculo é que, se considerarmos os diferentes pontos do conjunto de dados, com uma distribuição qualquer de classes, é esperado que o valor da função *loss* assuma o valor . Com isso, se quisermos saber qual deve a forma da função que minimiza esse valor devemos calcular:

Aqui, foi omitido o parâmetro que caracteriza a função , apenas por simplicidade. Com isso, vemos que, ao utilizar a *loss* exponencial, o valor esperado dessa *loss* é minimizado quando a função é proporcional a uma função logit. Isso quer dizer que, quando , e, caso contrário, (Figura 5‑3). Portanto, ao adotar função de classificação , estamos classificando o ponto com base na classe que tem maior probabilidade a posteriori, o que está de acordo com a teoria da decisão.

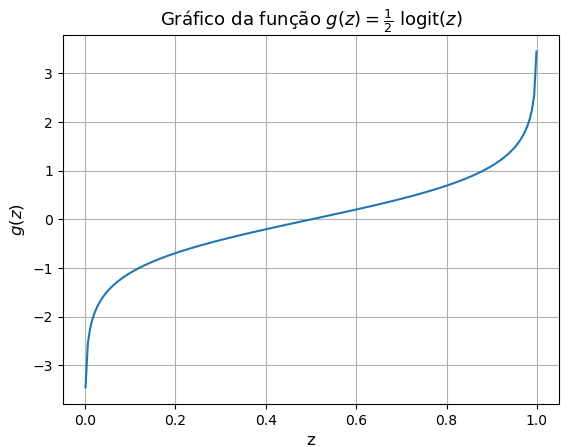


Figura 5‑3: Curva da função logit.

Como isso se relaciona com o desenvolvimento da Subseção 5.1.1? Repare que, a função custo minimizada na eq. (5.2), é justamente a média amostral da *loss* exponencial, que é um estimador natural para ela:

Logo, o desenvolvimento feito na Subseção 5.1.1 está de acordo com a teoria da decisão.

No entanto, foi visto anteriormente, a *loss* exponencial penaliza demais pontos errados, principalmente aqueles cuja margem está muito distante da superfície de decisão, localizada em Por isso, *outliers* tendem a receber um peso muito maior quando comparados com outros pontos, o que impacta o processo de otimização. Assim, na presença de *outliers* a *loss* exponencial não é a mais adequada.

Por outro lado, nesses casos, podemos utilizar como alternativa a *loss* logística (que aparentemente, é equivalente à log *loss*), definida como

Como pode ser visto na Figura 5‑1, essa *loss* apresenta valores mais balanceados para diferentes valores de , diminuindo a atribuição de pesos excessivamente grandes para *outliers*. Um detalhe importante é que, ao se utilizar essa função, a otimização fica muito complicado e, por isso, é recomendado utilizar métodos como gradiente descendente ou baseados no método de Newton [1].

# Support Vector Machine

Um conceito importante para entender o modelo SVM é o **hiperplano de separação ótimo**, que separa duas classes linearmente separáveis e maximiza a distância entre os pontos mais próximos de cada classe [4]. Esse conceito é ilustrado na Figura 6‑1. A distância do hiperplano de separação para o ponto mais próximo de cada classe é chamada de **margem** e é representado pela letra .

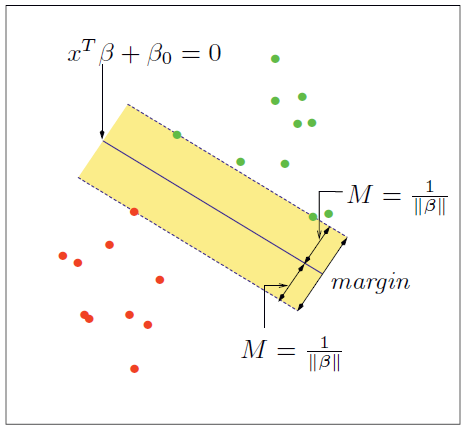


Figura 6‑1: Exemplo de classificador de vetor suporte.

Um hiperplano de separação pode ser definido como , como mostra a Figura 6‑2. Ele consegue separar duas classes de dados: os dados que estão acima do hiperplano, para os quais , e os dados que estão abaixo do hiperplano, para os quais . Assim, podemos usar o sinal de para classificar os dados.

Uma métrica importante de se conhecer é a distância de um ponto qualquer para esse hiperplano. Primeiramente, façamos algumas considerações.

Se , então . Como , concluímos que .

Seja . A distância de um ponto para é dada por

Como , temos que

|  |  |  |
| --- | --- | --- |
|  |  | (6.1) |

Observar que pode ser positivo ou negativo, dependendo do sinal de .

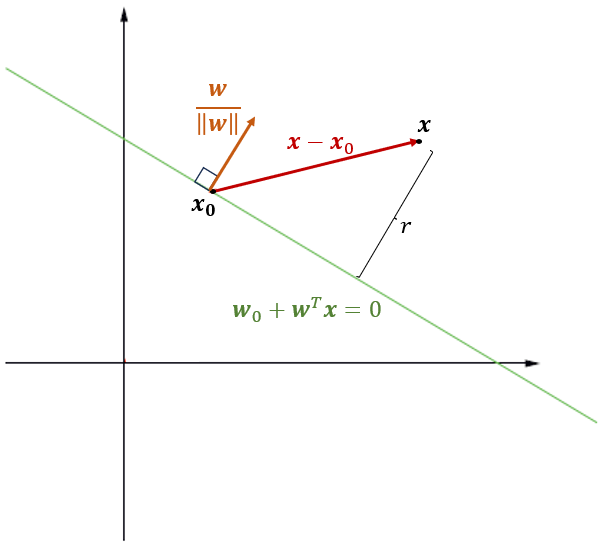


Figura 6‑2: Distância de um hiperplano para um ponto.

Tendo uma expressão para a distância entre um hiperplano e um ponto qualquer, podemos passar ao problema do hiperplano de separação ótimo.

Consideremos o conjunto de dados com e . Consideremos também que é possível usar um hiperplano de separação para separar os dados, de forma que quando e quando . Assim, podemos resumir o problema de encontrar o hiperplano de separação ótimo ao problema de maximizar a margem , para a qual ainda não temos uma expressão definida, mas com a restrição de que todos os pontos devem estar acima dessa margem. No entanto, só estamos interessados nos pontos que foram corretamente classificados, para os quais e cuja distância absoluta para é dada por .

Matematicamente, escrevemos esse problema como

Como , todos os pontos incorretamente classificados são automaticamente deixados de fora.

Observar que multiplicar e (os únicos termos que temos a liberdade de variar nesse problema de otimização) por um fator , ou seja, e , não altera em nada o problema acima:

Assim, se e maximizam o problema acima, então e também maximizam. Temos essa liberdade para variar essas variáveis porque temos uma única restrição, mas duas variáveis.

Com isso, podemos escolher um tal que . Portanto, fazemos e , com e encontramos:

Por simplicidade, podemos definir e . Além disso, como , o problema de otimização pode ser escrito como:

Para manter a notação anterior, e . Além disso, maximizar é equivalente a minimizar , que é equivalente a minimizar . Portanto, o problema de otimização se resume a

|  |  |  |
| --- | --- | --- |
|  |  | (6.2) |

A escolha de minimizar em vez de ficará mais evidente adiante.

A função de Lagrange e a função de Lagrange dual desse problema são, respectivamente:

Para encontrar fazemos

|  |  |  |
| --- | --- | --- |
|  |  | (6.3) |
|  |  | (6.4) |

Lembrando que . Assim vemos que, anteriormente, foi escolhido minimizar porque o quadrado torna a derivação mais simples.

O passo anterior só é possível quando há dualidade forte, ou seja, quando o gap de dualidade é zero e temos , em que e são os parâmetros ótimos, que minimizam a função objetivo. Como o problema primal é convexo (função objetivo quadrática e restrição linear), basta que a as condições de KKT sejam satisfeitas para que possamos afirmar que há dualidade forte. As condições de KKT são as seguintes:

Se garantirmos que todas elas sejam satisfeitas, o que é trivial, podemos seguir assumindo dualidade forte.

A expressão da função de Lagrange dual fica:

|  |  |  |
| --- | --- | --- |
|  |  | (6.5) |

Para , em que é o símbolo de maior ou igual elemento a elemento.

Com isso, o problema de otimização se resume a maximizar a função de Lagrange dual acima (comumente resolvida pelo computador) respeitando as condições de KKT.

Tendo encontrados os valores ótimos de e , o hiperplano de separação ótimo produz uma função , que pode ser usada para classificar novos dados. Se for positiva, temos uma classe e, se for negativa, temos outra.

É interessante observar uma das condições KKT, dada pela *complementary slackness,* mostrada a seguir:

Para essa condição ser respeitada, precisamos ter ou . Isso nos deixa com dois cenários interessantes:

* , o que implica , isto é, está exatamente na margem (reparar que, em (6.2), havendo igualdade somente quando está na margem).
* , isto é, não está na margem e , o que zera o somatório da eq. (6.5) fazendo com que esse ponto não contribua para a solução do problema.

Portanto, reparamos que apenas os pontos que estão na margem contribuem para a determinação do plano de separação ótimo, já que é uma combinação linear desses pontos (eq. (6.3)). Esses pontos são chamados de **vetores de suporte**.

## Caso Não Linearmente Separável

Quando temos dados que não são linearmente separáveis, ou seja, que estão sobrepostos, o desenvolvimento acima não é válido. Por isso, refaremos todo esse desenvolvimento, mas de maneira mais geral.

No caso em questão, não conseguimos separar completamente todos os pontos com um hiperplano. É necessário aceitar que, em cada lado do hiperplano, haverá pontos das duas classes, em geral (observar a Figura 6‑3). Além disso, haverá ainda pontos que estão do lado certo, mas que estão dentro da margem, ou seja, estão a uma distância do hiperplano menor que . Essa abordagem, muitas vezes, é chamada de soft margin classification, em oposição ao método apresentado anteriormente, que não permitia que pontos estivessem dentro da margem ou do lado errado do hiperplano, chamado muitas vezes de de hard margin classification [7].

|  |  |
| --- | --- |
| 1. *Caso linearmente separável.* | 1. *Caso não linearmente separável.* |

Figura 6‑3: Possíveis casos para o classificador de vetor de suporte.

Para considerar esses casos, usaremos variáveis , para indicar uma noção de distância que um ponto está da margem da classe a qual ela pertence, na direção contrária ao lado ao qual ela pertence (observando a Figura 6‑3b isso fica mais claro). Assim, escreveremos a restrição do nosso problema como

|  |  |  |
| --- | --- | --- |
|  |  | (6.6) |

em que e . Isso nos deixa com alguns casos diferentes:

* , indica que o ponto está do lado correto do hiperplano, mas dentro da margem;
* , indica que o ponto está do lado certo do hiperplano e está fora da margem, independentemente de sua distância para a margem;
* indica que o ponto está do lado errado do hiperplano (ou exatamente em cima do hiperplano, no caso em que ).

Com isso, vemos que indica a distância de um ponto para a margem certa de maneira relativa. Talvez uma forma mais natural de escrever essa restrição fosse , pois, nesse caso, está de fato indicando a distância absoluta para a margem. No entanto, essa forma de escrever a restrição não facilita o resto do desenvolvimento e, por isso, a restrição adotada será na forma da eq. (6.6).

Logo, seguindo a lógica adotada no problema linearmente separável, o problema pode ser escrito como

Uma forma mais conveniente de reescrever esse problema é a seguinte:

|  |  |  |
| --- | --- | --- |
|  |  | (6.7) |

Dessa forma, temos um parâmetro “custo” na função objetivo que assume um papel similar ao da constante que limita . Quando , temos o caso separável.

Como o problema de otimização é convexo, podemos seguir passos análogos aos que foram adotados anteriormente para resolver esse problema. A função de Lagrange é dada por:

Como a função de Lagrange dual é derivamos e igualamos a zero:

|  |  |  |
| --- | --- | --- |
|  |  | (6.8) |

|  |  |  |
| --- | --- | --- |
|  |  | (6.9) |

Usando as equações acima, encontramos a seguinte expressão para função de Lagrange dual:

Lembrando que é preciso considerar as condições de KKT para podermos resolver esse problema, que são dadas por:

|  |  |  |
| --- | --- | --- |
| 1. | Restrição 1: ou | (6.10) |
| 2. | Restrição 2: | (6.11) |
| 3. | Condição do Lagrangiano 1: | (6.12) |
| 4. | Condição do Lagrangiano 2: | (6.13) |
| 5. | *Complementary slackness* 1*:* | (6.14) |
| 6. | *Complementary slackness* 2: | (6.15) |
| 7. | Gradiente nulo 1: | (6.16) |
| 8. | Gradiente nulo 2 : | (6.17) |
| 9. | Gradiente nulo 3: | (6.18) |

A condição dada pela eq. (6.14), pode ser escrita como . A partir dessa equação e condição dada pela eq.(6.16), vemos que, assim como no caso linearmente separável, é uma combinação linear de apenas alguns pontos , que são chamados de **vetores de suporte**. Nesse caso, os únicos pontos que não são vetores de suporte são aqueles que estão do lado certo do hiperplano e fora da margem (sem estar em cima da borda da margem). Isso pode ser percebido ao observarmos as diferentes possibilidades para :

* Quando (pontos do lado correto do hiperplano em cima da borda da margem ou fora da margem), temos uma situação parecida com o caso linearmente separável:
  + Quando , ou seja, está do lado certo do hiperplano, mas fora da margem, e, portanto, esse ponto não é contabilizado na eq. (6.16).
  + Quando , temos ou seja, o ponto está exatamente em cima da borda da margem. Como , o ponto é contabilizado.
  + Lembrar que uma das condições de KKT é que , então, não haverá o caso .

É interessante reparar que, nesse caso, pela eq. (6.18), .

* Quando (pontos do lado correto do hiperplano dentro da margem ou pontos do lado incorreto do hiperplano), . Logo, e todos os pontos são contabilizados na eq. (6.16).  
  Isso acontece porque representa a distância normalizada de um ponto para o hiperplano, sendo que ela será positiva quando o ponto estiver do lado certo do hiperplano e negativa caso contrário. Quando , isso não é necessariamente verdade, pois, esse caso inclui tanto os pontos que estão em cima da borda da margem, em que de fato , mas também inclui os pontos corretamente classificados que estão fora da margem, em que .  
  Dois exemplos ajudam a entender isso:
  + Se , o ponto está do lado correto do hiperplano, mas dentro da margem, e . Se, por exemplo, , sua distância normalizada da margem é dada por e sua distância normalizada para o hiperplano é dada por
  + Se , o ponto está do lado errado do hiperplano e . Se, por exemplo, , sua distância normalizada da margem é dada por e sua distância normalizada para o hiperplano é . Lembrando que o sinal de menos em é usado porque é negativo quando o ponto está do lado errado do hiperplano.

É interessante reparar que, nesse caso, pelas eqs. (6.15) e (6.18), .

Depois de e terem sido determinados, para classificar novos pontos, basta analisar o sinal de .

é um parâmetro de *tunning*. Quanto maior o valor de , menores deverão ser os valores de para poder minimizar o problema (6.7). Logo, menor será a margem. De forma análoga, quanto menor for , maiores serão os valores de . A Figura 6‑4 ilustra essas situações.

|  |  |
| --- | --- |
|  |  |

Figura 6‑4: Margens do classificador de vetor de suporte para diferentes valores de C.

## Máquina de Vetor de Suporte

Como vimos acima, o classificador de vetor de suporte encontra fronteiras lineares de decisão no espaço das entradas . No entanto, é possível tornar esse procedimento mais flexível aumentando esse espaço usando funções base, criando assim, um espaço de *features*. Quando aplicamos o método dessa maneira, encontramos uma fronteira de decisão linear no espaço das *features*, porém não-linear no espaço das entradas.

Essa utilização do método do classificador de vetor de suporte com a possibilidade de trabalhar em um outro espaço de dimensão maior (possivelmente infinito) dá origem ao modelo suport vector machine (SVM).

O procedimento para encontrar a fronteira de decisão desse modelo é, basicamente, o mesmo que foi desenvolvido na Seção 6.1, bastando apenas substituir as entradas pelas suas funções correspondentes . Então, com base na eq. (6.16), podemos escrever

|  |  |  |
| --- | --- | --- |
|  |  | (6.19) |

É importante dizer que é uma aplicação definida como

em quem é a dimensão dos dados e é um *reproducing kernel Hilbert Space* (RKHS) de funções reais. é chamada de *feature map* e pode ter dimensão finita ou infinita. Para mais detalhes sobre o RKHS, consultar Apêndice D:.

Observar que, na eq. (6.19), o produto interno que existia originalmente na eq. (6.16), , produto interno do espaço Euclidiano, foi substituído pelo produto interno dos *features maps* . O subscrito serve para indicar que o produto interno entre essas duas aplicações não é mais um produto interno do espaço Euclidiano, pois essa aplicação pertence ao espaço de Hilbert, que é um espaço de produto interno .

Todo RKHS apresenta uma função kernel que o define. Além disso, nesse espaço, temos que . Logo, podemos reescrever a eq. (6.19) como

|  |  |  |
| --- | --- | --- |
|  |  | (6.20) |

Com isso, vemos que não é necessário conhecer as *features* definidas por para determinar a fronteira de decisão. Basta conhecer a função kernel, que normalmente, é uma escolha de *design* do modelo SVM. Escolhas populares para o kernel são:

* Kernel polinomial:
* Kernel Gaussiano:
* Sigmoid kernel:

em que é o produto interno do espaço Euclidiano, pois e representam entradas.

### SVM como Método de Penalização

O problema de minimização do modelo SVM é similar ao do classificador de vetor de suporte, definido na eq. (6.7), porém substituindo por quando necessário. Assim, omitindo as restrições, o problema de minimização consiste em

Podemos reescrever esse problema da seguinte forma:

em que , e .

Com isso, vemos que o problema de minimização do modelo SVM tem a forma *loss* + penalidade, típica de um problema de otimização com regularização.

A função de *loss* é chamada de *hinge loss* (*loss* articulação), devido ao seu formato, como mostrado na Figura 6‑5. Nessa imagem, outras funções de *loss* são mostradas para efeito de comparação. Para mais detalhes, consultar [4].

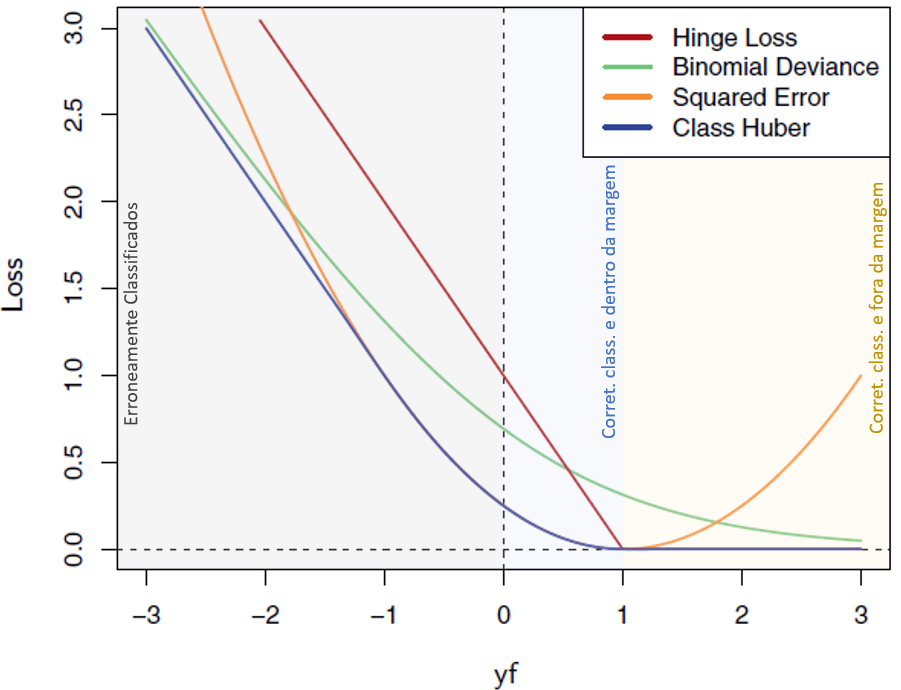


Figura 6‑5: Comparação de diferentes funções de loss.

Com isso, vemos que a *hinge loss* atribui uma perda nula para os termos para os quais , ou seja, para todos os pontos que tenham sido classificados corretamente e que estejam fora da margem. Além disso, atribuiu uma perda linear para os pontos dentro da margem ou classificados erroneamente.

Um detalhe importante para se atentar é que, só encontramos a expressão da *hinge loss* na modelagem do SVM por causa de algumas suposições feitas, como e . Se outras escolhas tivessem sido feitas, obteríamos outra *loss*.

### Classificação Multiclasse

O mais comum é adotar a abordagem *one-vs-the-rest*. Para corrigir o problema das regiões de ambiguidade, diferentes técnicas podem ser adotadas, como mostrado em [5, pp. 338-339].

Notar que, no modelo da regressão logística, esse problema era facilmente resolvido ao atribuir uma função discriminante para cada uma das funções e estabelecer a regra de que se . Lembrando que a variável aleatória nesse caso é , que é o conjunto dos pontos pertencentes à classe . Nesse caso, não existirá regiões de ambiguidade.

No entanto, no SVM, isso não é possível, pois não temos uma função discriminante que representa a probabilidade a posteriori de o dado pertencer à classe .

## SVM para Regressão

Nas seções anteriores, tínhamos dados que pertenciam a duas classes diferentes e utilizávamos um hiperplano para separá-los, considerando que existe uma margem ao redor desse hiperplano.

Para o caso da regressão, é necessário adaptar o método, já que o nosso problema não é mais de separação dos dados. A adaptação que pode ser feita é considerar que, agora, representará uma curva de regressão que tentará aproximar a função geradora dos dados . Para isso, consideraremos que os dados podem estar exatamente em cima da curva ou dentro de uma margem de espessura ao redor da curva, como mostra a Figura 6‑6.

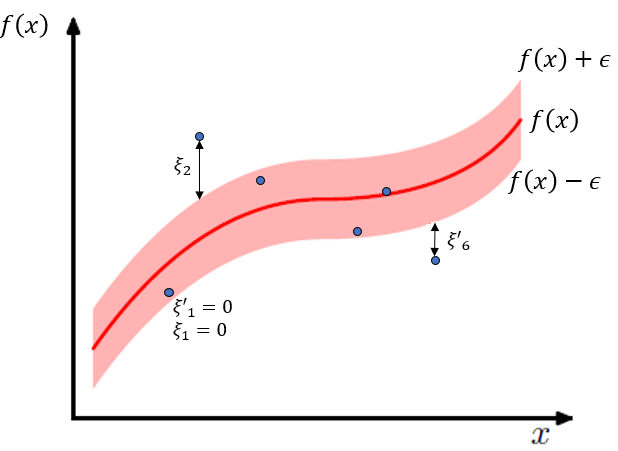


Figura 6‑6: Modelo de SVM para regressão.

Podemos escrever esse problema no formato , sujeito à condição de que os pontos devem estar dentro do “tubo-” que envolve . Com isso, o método acima se resume a

em que é a função de erro -insensível, dada por

ou seja, desprezamos todo erro abaixo de .

No entanto, nem sempre vamos conseguir fazer com que todos os pontos se encontrem dentro do tubo-. Por isso, assim como no caso da classificação, introduzimos variáveis para permitir a contabilização de pontos que não estejam dentro do tubo-. No entanto, na regressão, precisaremos de variáveis para os pontos acima da curva e variáveis para pontos abaixo da curva . Essas variáveis são definidas como e .

Incluindo essas variáveis no problema, temos um novo problema de otimização, dado por

Se repararmos, temos algo muito parecido com o que tínhamos no problema (6.7). Com isso, vemos que é preferível ter e menores possíveis, pois e grandes levam a um custo maior.

Com isso, o Lagrangiano pode ser escrito como

em que , , e são os multiplicadores de Lagrange.

A função dual de Lagrange é dada por

com

Para terminar de resolver o problema de otimização, basta maximizar sujeito às condições de KKT. Duas dessas condições, advindas da propriedade *complementary slackness*, são interessantes para serem analisadas, como mostradas abaixo:

|  |  |  |
| --- | --- | --- |
|  |  | (6.21) |

|  |  |  |
| --- | --- | --- |
|  |  | (6.22) |

A partir da eq. (6.21), vemos que somente se , ou seja, se o ponto estiver fora do tubo- ou exatamente em sua borda. Isso porque

* se o ponto está fora do tubo-, então e ;
* se o ponto está na borda do tubo-, então , e .

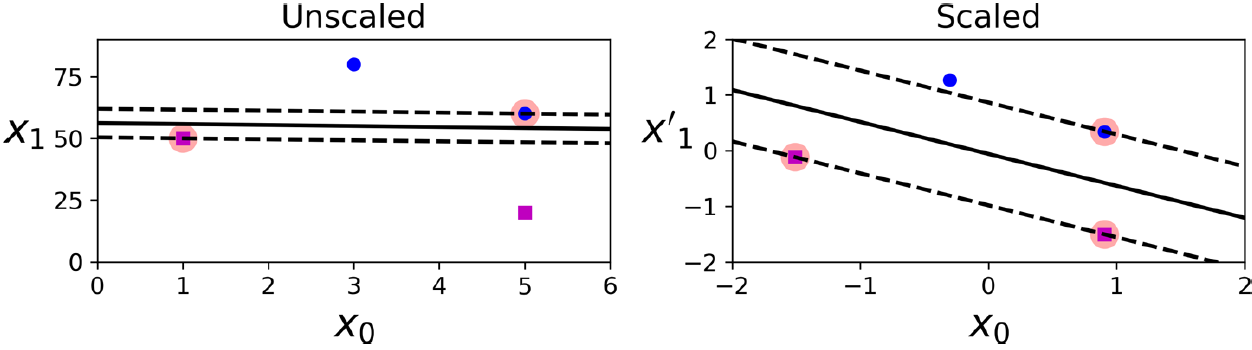
No caso em que o ponto está entro da margem , pois .

O raciocínio é análogo para na eq. (6.22). Com isso, vemos que os únicos pontos que contribuem para são aqueles que estão fora do tubo- ou exatamente em cima de sua borda.

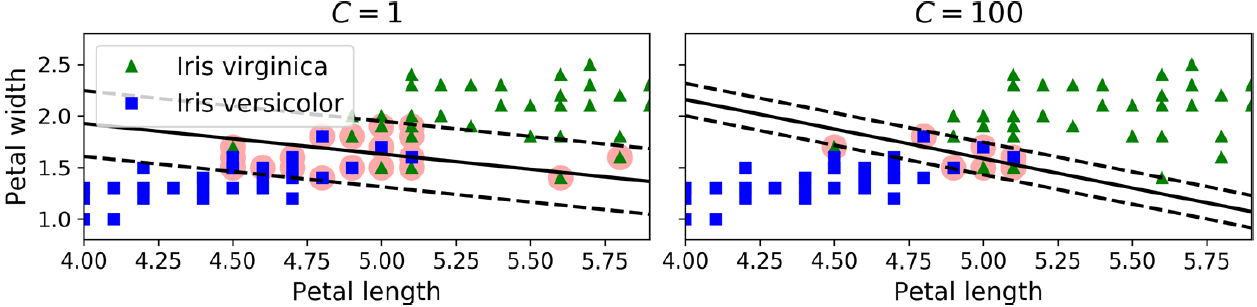
Assim, como foi feito no caso da classificação, todo esse desenvolvimento pode ser generalizado para o caso em que estamos trabalhando no espaço das *features*. Basta substituir as entradas pelas *features* e o produto interno Euclidiano pela função kernel **.**

## Aspectos Práticos

* O modelo SVM é mais adequado para *datasets* de tamanho pequeno/médio, pois ele não escala bem com o número de dados, tendo complexidade entre e para a classe SVC do scikit-learn, em que é o número de exemplos e o número de *features* [7]. Para kernel linear, dar preferência para a classe LinearSVC do scikit-learn, pois o algoritmo tem complexidade .
* É sensível à escala.



* Baixos valores de C aumentam a regularização do modelo, deixando a margem menos estreita.



* Poderíamos aplicar um classificador de vetor de suporte *soft* para separar dados não-linearmente separáveis. No entanto, precisaríamos criar novas *features* a partir das variáveis de entrada, de forma a encontrar uma fronteira de decisão adequada (e não linear). Criar *features* polinomiais geralmente é uma boa opção. Para polinômios de grau pequeno, isso pode até ser viável, mas para polinômios de grau elevado, isso se torna inviável. A partir disso, podemos ver a vantagem do SVM sobre métodos lineares que utilizam transformações para gerar novas *features*: não é preciso criar novas *features*, apenas escolher a função *kernel* adequada.
* As funções *kernel* mais comumente usadas são a linear e a *Gaussian Radial Basis Function* (RBF). Como regra de ouro para escolher a função *kernel* na prática, pode-se começar com a linear (dando preferência para o LinearSVC, em vez do SVC do scikit-learn, pela eficiência computacional), especialmente se o conjunto de dados for muito grande. Caso o conjunto de dados não seja tão grande, pode-se testar em seguida a *Gaussian* RBF.

# Rede Neural

Nas seções sobre regressão linear e regressão logística, vimos que os modelos tinham a forma

com e . Na regressão linear, tínhamos e, na regressão logística, tínhamos uma função não-linear (mais especificamente uma sigmoide).

Na rede neural, teremos um modelo muito parecido, mas as funções base , agora, também dependerão de parâmetros ajustáveis e terão a forma abaixo:

em que e são funções não lineares. Como a rede neural pode ter saídas, usamos o índice para indicar a qual saída estamos nos referindo. Além disso, percebemos que a função base é uma composição de várias outras funções que dependem dos parâmetros ajustáveis. Utilizamos um sobrescrito nos parâmetros para indicar a qual das **camadas** da rede neural eles estão vinculados.

Assim, vemos que a rede neural é uma versão mais complexa de uma regressão logística (no caso da classificação), em que a função base depende dos parâmetros ajustáveis e de uma estrutura recursiva de funções não lineares. Isso nos permite criar fronteiras de decisão não lineares (no espaço das entradas ) muito mais complexas do que as da regressão logística, graças à existência de uma função base bastante adaptável.

## Estrutura da Rede Neural

O elemento básico de uma rede neural é chamado de **neurônio**, como pode ser visto na Figura 7‑1.

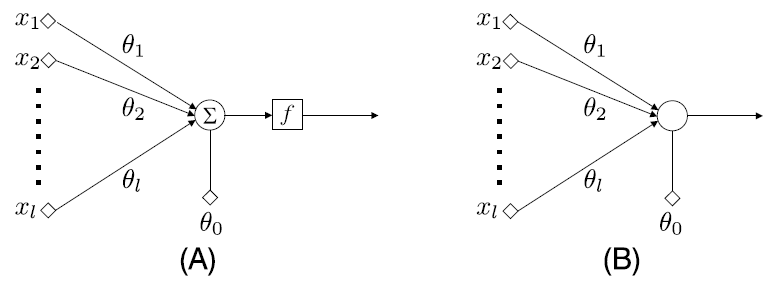


Figura 7‑1: Ilustração do neurônio de uma rede neural.

Nessa imagem, podemos ver os elementos já mencionados anteriormente, nomeadamente as entras , os pesos e a função não linear , que recebe o nome especial de **função de ativação**. Além disso, o termo , que não está associado a nenhuma entrada recebe o nome de bias(ou *threshold*). A parte B dessa figura mostra que, usualmente, agrupamos o bloco de combinação linear com o da função de ativação para formar o que é chamado de **nó**. Muitas vezes, o termo nó será utilizado para se referir ao neurônio inteiro.

Juntando vários neurônios, podemos formar o que é chamado de ***feed-forward network*** ou ***fully connected network***(FCN), como é mostrado na Figura 7‑2. O nome *feed-forward network* se dá pelo fato de a informação ser unidirecional, indo das entradas até camada de saída. Já o nome *fully connected network* enfatiza o fato de que cada neurônio desse tipo de rede está conectado a todos os neurônios da camada anterior.

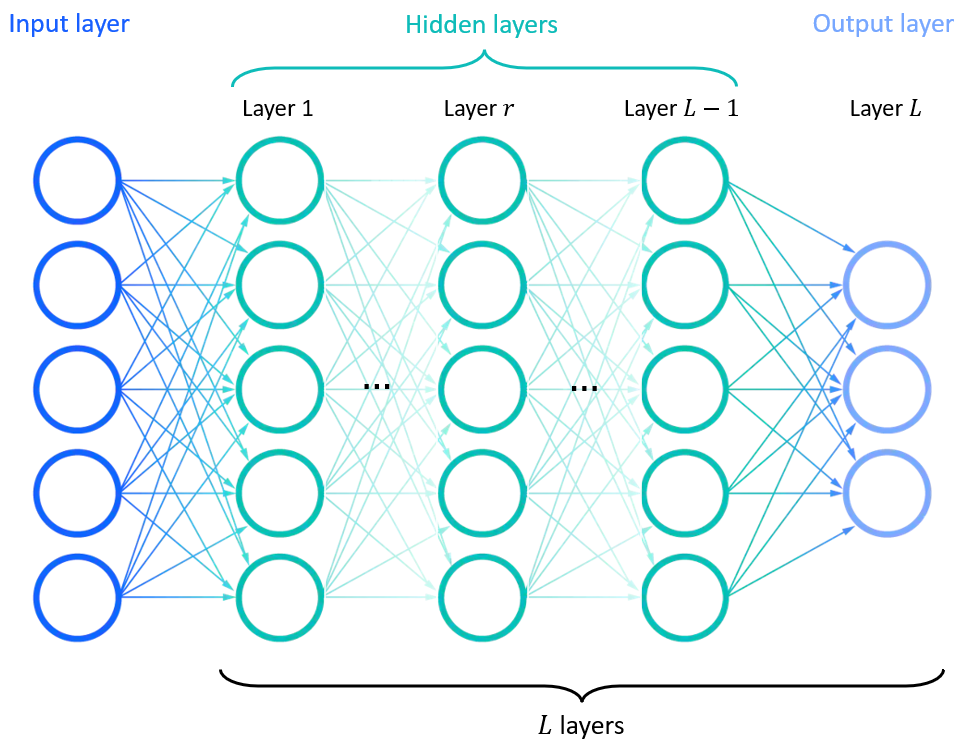
****

Figura 7‑2: Rede neural totalmente conectada com camadas.

Atentando-se para a questão de nomenclatura, damos os nomes de **neurônio de saída** e **neurônios escondidos** aos neurônios pertencentes às camadas de saída e camadas escondidas, respectivamente. Os nós pertencentes à camada de entrada não são neurônios, ou seja, não realizam nenhum tipo de processamento. Por causa disso, dizemos que a rede da Figura 7‑2 é uma rede de camadas, excluindo a camada de entrada da contagem. Redes com até 3 camadas (até duas camadas escondidas) são chamadas de **rasas** e redes com mais camadas são chamadas **profundas**.

Muitas pessoas também chamam essa rede de ***multilayer perceptron*** (MLP), por causa da origem desse modelo, que era baseado em um modelo de neurônio chamado de perceptron.

Em cada neurônio da rede neural, estamos realizando a seguinte operação:

|  |
| --- |
|  |

O sobrescrito indica a qual das camadas o neurônio pertence.  
O subscrito identifica o número do neurônio nessa camada, considerando um total de neurônios.  
Assim, a expressão diz que a saída do neurônio da camada é igual ao produto do vetor com as saídas dos neurônios da camada anterior pelo vetor de parâmetros ,vinculado ao neurônio em questão, passado por uma função não linear .

O vetor das saídas de todos os neurônios de uma camada é dado por

|  |
| --- |
|  |

em que e é o número de neurônios na camada .

Lembrando que o elemento 1 em leva em consideração o *bias* , contido no vetor.

A Figura 7‑3 mostra um diagrama que resume essas equações para uma camada .

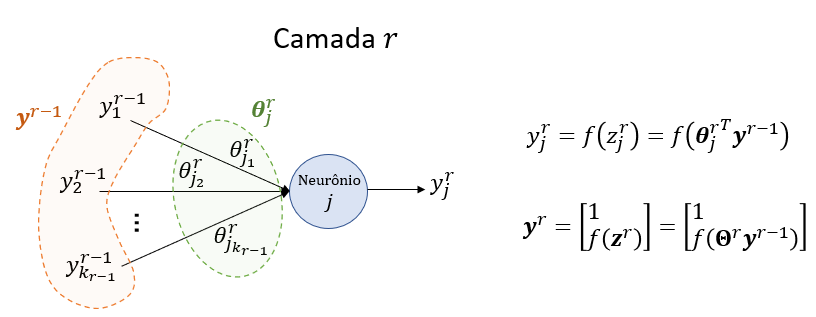


Figura 7‑3: Equações da FCN.

Para a função não linear , é comum utilizarmos funções como a sigmoide ou a tangente hiperbólica, por alguns motivos específicos, mas principalmente por elas serem diferenciáveis. Seus gráficos são mostrados na Figura 7‑4.

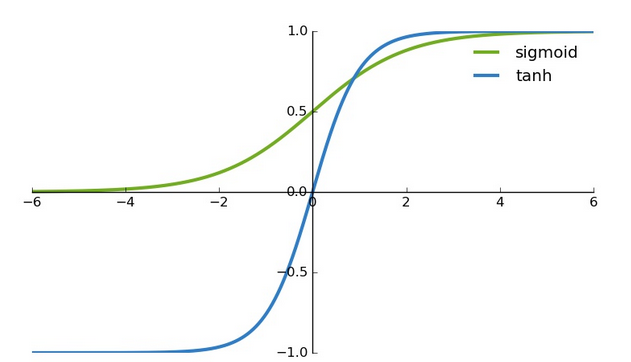


Figura 7‑4: Funções sigmoide e tangente hiperbólica.

## Algoritmo de Backpropagation

É o algoritmo utilizado pelas redes neurais para otimizar os parâmetros . Assim como em outros modelos de *machine learning*, nosso objetivo é otimizar uma função objetivo/custo com o seguinte formato:

em que é o número total de amostras de treinamento , e é a função *loss*.

Uma das grandes dificuldades de otimizar uma função como essa está na estrutura multicamadas da rede neural, em que cada neurônio possui um vetor de parâmetros único associado a cada um deles e as saídas de cada neurônio depende das saídas dos neurônios mais **rasos** (pertencentes a camadas de índice menor). Assim, temos uma estrutura em que a saída de um neurônio é uma composição de várias funções não lineares

Outra dificuldade é que, devido à natureza altamente não linear da rede neural, a função custo tende a apresentar diversos mínimos locais, o que dificulta encontrarmos a solução ótima, principalmente quando aplicamos técnicas de otimização como o gradiente descendente. Muitas vezes, o mínimo local é tão fundo que se aproxima do valor de ótimo. Nesses casos, podemos adotar esse mínimo local como solução, se o resultado final for satisfatório.

Feitas essas considerações, entraremos nos detalhes do algoritmo de *backpropagation*. Primeiramente, precisamos escolher uma função de perda. Nesse momento, adotaremos a função de erro quadrático para assumir esse papel. Assim, a função custo fica da seguinte forma:

|  |  |  |
| --- | --- | --- |
|  |  | (7.1) |

com

Com isso, estamos avaliando o erro quadrático entre o valor estimado da saída no neurônio para a amostra de índice e o valor real que deveria estar na saída, sendo o índice o indicador da posição no vetor .

O próximo passo é escolher um algoritmo de otimização para nos auxiliar a encontrar os melhores valores de Normalmente, são utilizados algoritmos baseados no cálculo do gradiente, devido à sua simplicidade. O método do gradiente descendente é um exemplo e será empregado na derivação do algoritmo do *backpropagation* por simplicidade, apesar de existirem variações desse método que são até mais utilizadas na prática (Adagrad, Adam...) [6, pp. 924-934]. De toda forma, no método do gradiente descendente básico, o valor de é atualizado a cada iteração da seguinte maneira:

|  |  |  |
| --- | --- | --- |
|  |  | (7.2) |

Assim, vemos que é necessário determinar o termo da derivada. Antes de desenvolver a expressão dessa derivada, lembremos que

**Observação:** não confundir , com sobrescrito, que é a saída do neurônio da camada , com , sem sobrescrito, que é o valor do *target* na posição correspondente à entrada .

Como é uma soma de , basta encontramos uma expressão para . É interessante notar também que, apesar de estarmos explicitando como dependente de , também poderíamos escrever , já que depende de , que, por sua vez, depende de

Com isso, usando a regra da cadeia, podemos escrever

Devido ao fato de o termo aparecer com frequência no desenvolvimento do algoritmo de *backpropagation*, utilizamos a seguinte definição:

|  |
| --- |
|  |

Portanto, nosso objetivo é encontrar

|  |  |  |
| --- | --- | --- |
|  |  | (7.3) |

Dessa forma, partindo da eq. (7.2) podemos encontrar a expressão que resume a atualização dos pesos da rede neural:

|  |  |  |
| --- | --- | --- |
|  |  | (7.4) |

O valor é observável, então não precisamos calcular esse termo. Basta determinarmos o valor de para cada camada e para cada neurônio nessa camada. Para a camada , determinar é simples, pois , o que faz com que a derivada com relação a seja simples. Estamos calculando a derivada da função custo, que está sendo avaliada na última camada, com relação a de um neurônio que também está na última camada. Logo, não temos composições de funções por causa da passagem de uma camada à outra.

Por outro lado, quando avaliamos para neurônios que não estão na última camada, os cálculos se tornam um pouco mais complicados por causa da composição de funções. Por isso, abaixo, vamos derivar expressões gerais para para os dois possíveis casos de .

**Detalhes dos cálculos do algoritmo de *backpropagation***

**:**

No caso mais simples, em que o neurônio está na última camada, temos

|  |
| --- |
|  |

com sendo o erro da rede neural no neurônio da camada de saída.

Quando analisamos para as camadas anteriores à camada de saída, verificamos que existe uma distância entre , que está sendo avaliado na saída, e a variável , com relação a qual estamos derivando e que está associada à camada . Logo, é natural que surjam regras da cadeia.

Da mesma maneira como foi feito anteriormente, podemos explicitar a dependência de com relação às variáveis da rede neural como

Com isso, podemos escrever,

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (7.5) |

com . Esse termo é só para criar uma uniformidade na notação.

Lembrando que poderíamos ter escrito uma expressão para explicitamente, mas daria no mesmo. Só teríamos que substituir o termo na equação acima por . Da forma como está a equação acima é mais conveniente.

Depois de todo esse desenvolvimento, vemos que para determinar , dependemos do valor de , da camada seguinte (uma profundidade abaixo). Por isso, para encontrarmos todos os valores de , precisamos fazer os cálculos de trás para frente (*backwards*), começando na camada de saída indo em direção à primeira camada.

O algoritmo de *backpropagation* consiste em

|  |
| --- |
| 1. Inicializar os pesos aleatoriamente; 2. Iterar variando de 1 a N:    1. Realizar o *forward propagation* (calcular as saídas da rede para a entrada );    2. Realizar o *backpropagation*, determinando os valores de para todos os valores de , começando na camada de saída e indo em direção à primeira camada. 3. Atualizar os valores de a partir da eq. (7.4); 4. Se o critério de parada não for satisfeito, retornar ao passo 2. |

O algoritmo acima pode ser executado várias vezes no mesmo conjunto de treinamento, repetindo os pares . Toda vez que completamos um ciclo passando por todas as amostras de treinamento , dizemos que uma **época** foi completada.

Alguns critérios de parada que podem ser adotados são: valor da função custo baixo o suficiente; os valores dos pesos de uma iteração para outra mudam muito pouco; número máximo de épocas foi atingido.

O algoritmo de *backpropagation* descrito acima utiliza uma abordagem do tipo batch, em que todas as amostras de treinamento são utilizadas de uma vez para o cálculo da função custo (observar que o somatório vai de 1 até ). Outra abordagem possível é a stochastic gradient descent (SGD). Nesse caso, usamos um método de otimização similar ao gradiente descendente, mas, para o cálculo da função custo, consideramos uma amostra por vez. Assim, em vem de calcular os valores para todos os valores de para somente no final atualizar os pesos com a eq. (7.1), atualizamos os pesos em cada iteração de , de forma que, em uma época, atualizamos vezes os pesos.

Finalmente, existe uma abordagem intermediária, chamada de minibatch, em que não atualizamos os pesos a cada iteração de , mas também não deixamos para atualizá-los depois de iterarmos ao longo das amostras. Atualizamo-nos de em amostras de treinamento, com , usando uma função custo da forma

em que é o tamanho do *minibatch*.

## Escolhendo a Função Custo e as Não-Linearidades

### Observando a Camada de Saída

Ao observarmos os neurônios da saída, podemos ter uma noção dos efeitos da combinação de determinadas funções não-lineares com determinadas funções custo. Por simplicidade, vamos considerar uma rede com um único neurônio na camada de saída. Consideraremos os casos da função custo de erro quadrático e de entropia cruzada.

#### Função Custo de Erro Quadrático

Nesse caso, temos

em que é o total de exemplos de treinamento, é o valor do *target* e é a saída do neurônio da última camada.

Se adotarmos a função sigmoide como não-linearidade, teremos

Reparar que isso é exatamente o que encontraríamos se aplicássemos a eq. (7.3) diretamente.

Com isso, vemos que o gradiente da função custo depende do erro , o que é justo, pois, à medida que o erro diminui, o gradiente também diminui, assim como o tamanho do passo do gradiente descendente. Por outro lado, a dependência de é incômoda, pois, se for muito distante do valor zero, tende a zero, assim como o valor do gradiente.

Portanto, vemos que quando usamos a função sigmoide como não-linearidade do neurônio de saída, a função custo de erro quadrático não é muito adequada.

#### Função Custo de Entropia Cruzada

Nesse caso, temos

Desenvolvendo a expressão para o gradiente da função custo, obtemos

Verificamos que, diferentemente do caso da função de custo de erro quadrático, o gradiente não depende da derivada da função não-linear, eliminando o problema do gradiente que “desaparece” quando for muito distante do valor zero. Portanto, a função custo de entropia cruzada é mais adequada quando utilizamos a função sigmoide como não-linearidade.

Em geral, quando queremos garantir que as saídas da rede neural sejam probabilidades e somem 1, utilizamos a função softmax na saída. Pode ser mostrado que, utilizar a softmax em vez da função sigmoide gera um gradiente que também é independente da derivada da função não-linear.

### Observando as Camadas Escondidas

Para as camadas anteriores à camada de saída, a expressão que rege o algoritmo de *backpropagation* é a eq. (7.5):

Como podemos perceber, temos uma lógica recursiva, em que o da camada anterior depende do da camada seguinte. Podemos deixar isso mais explícito ao substituirmos o termo na equação acima da seguinte forma:

|  |  |  |
| --- | --- | --- |
|  |  | (7.6) |

Com isso, percebemos que existe um produto dos pesos e das derivadas da função não-linear. À medida que continuamos substituindo recursivamente, mais termos referentes às outras camadas vão sendo adicionados a esse produto.

A derivada da função não-linear pode assumir valores menores do que 1. Com isso, dependendo do caso, pode acontecer de o gradiente da função custo com respeito aos parâmetros das camadas mais superficiais assumam valores muito pequenos e sofram desvanecimento à medida que caminhamos para a parte mais rasa da rede. Esse fenômeno é conhecido como **desvanecimento do gradiente**. O maior problema associado a esse fenômeno é que ele torna o aprendizado mais lento.

Outro fenômeno associado a esse produto recursivo é o **gradiente explosivo**, que acontece quando o valor do gradiente assume valores mais elevados à medida que caminhamos na direção das camadas mais rasas. Isso afeta o aprendizado, pois faz com que a atualização dos parâmetros dê um salto muito elevado, podendo desviar os parâmetros do valor correto. Além disso, o gradiente explosivo pode levar a problema relacionados à overflow das variáveis que armazenam os parâmetros.

Por fim, em redes neurais com muitas camadas, os parâmetros de cada camada podem assumir valores de escalas muito diferentes, o que faz com que a velocidade do aprendizado de cada uma delas seja muito diferente, causando instabilidade.

Uma maneira de lidar com esse problema é utilizar função de ativação ReLU (Rectified Linear Unit) nos neurônios das camadas escondidas. Ela é dada por

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (7.7) |

Seu gráfico é mostrado na Figura 7‑5.

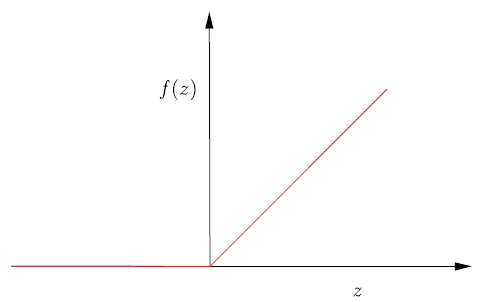


Figura 7‑5: Gráfico da ReLU.

Ela ajuda a resolver os problemas do gradiente desvanecente e explosivo e, consequentemente, acelerando o treinamento porque sua derivada é sempre uma constante. Para , a derivada é um e os termos na (7.6) desaparecem. Para , podemos escolher o valor 0 ou 1 para a derivada.

Como é possível perceber, para , a derivada se anula e o treinamento tende a ficar mais lento e a empacar. Por essa razão, ao inicializar os pesos da rede, no início do treinamento, é importante escolher pequenos valores positivos para os pesos.

## Regularização

Como as redes neurais apresentam uma quantidade muito grande parâmetros, elas ficam sujeitas ao problema de *overfitting.* Uma forma prática de lidar com esse problema é utilizar regularização. As principais técnicas de regularização que podem ser aplicadas a redes neurais são mostradas abaixo:

* **Decaimento de peso:** consiste em alterar a função custo adicionando um termo de regularização, como por exemplo
* ***Early stopping*:** no início do treinamento, há uma tendência de as curvas de erro de treinamento e de teste decaírem. A partir de determinado momento, a curva de erro de teste deixa de decair e começa a subir. A técnica de *early stopping* consiste em interromper o treinamento assim que a curva de erro de teste começa a subir. Esse é um dos métodos de regularização mais utilizados e pode ser combinado com outros métodos.
* ***Dropout:*** consiste em remover da rede neural, durante o treinamento, uma certa porção de nós. Quando um nó é removido, todas as suas conexões com os nós da camada anterior e da camada seguinte também são removidas. A cada iteração, cada nó tem probabilidade de ser removido. Quando um nó é removido em uma iteração, os parâmetros associados a ele não são atualizados. Na iteração seguinte, todos os nós removidos retornam com os seus pesos conservados da iteração anterior a que eles foram removidas e é feito um novo sorteio para decidir quais são os nós que serão removidos novamente. Depois de a rede neural estar treinada e é utilizada para inferências, os pesos de cada neurônio são multiplicados por . Esse é um dos métodos de regularização mais utilizados e pode ser combinado com outros métodos.

# Feature Selection

*Feature selection* é uma técnica de redução de dimensionalidade que consiste em selecionar algumas *features* do conjunto total sem modificá-las ou criar novas *features*.

Um procedimento que tem um nome parecido e pode criar confusão é *feature extraction*, que também faz parte do conjunto de técnicas de redução de dimensionalidade. No entanto, nesse caso, realizamos a projeção de todas as *features* em um novo espaço com dimensão menor. Não selecionamos um subconjunto das *features*, como é o caso da *feature selection.*

As principais vantagens da *feature selection* (e da *feature extraction* também) são [8]:

* Aumento de eficiência computacional, pois são utilizadas menos variáveis durante o aprendizado do modelo.
* Modelo com maior capacidade de generalização, já que, mantendo-se a quantidade de dados constante, diminuir o número de *features* diminui o risco de *overfitting*.

O último ponto está ligado à maldição da dimensionalidade, que diz que, à medida que a dimensão do problema aumenta, os dados tornam-se mais esparsos. Uma forma de visualizar isso é imaginando o exemplo em que temos dois pontos e o posicionamos o mais distante possível dentro de um hipercubo de aresta . Quando o número de dimensões é , a maior distância é . Quando , a maior distância é .

As técnicas de *feature selection* podem ser **supervisionadas**, que é o caso em que utilizamos os *targets* para selecionar o subconjunto de *features*, ou **não-supervisionados**, que é o caso em que não são utilizados os *targets*.

Além disso, as técnicas de *features selection*, sejam elas supervisionadas ou não-supervisionadas, podem ser divididas em:

* ***Wrapper methods*:** o critério utilizado para avaliar as *features* selecionadas é baseado no desempenho do modelo de *machine learning*. Assim, primeiramente, selecionamos um grupo de *features* e as utilizamos para treinar o modelo. Utilizamos os resultados do teste desse modelo para comparar essa seleção com as próximas seleções. A principal desvantagem desse método é a demora relacionada aos diversos treinamentos e testes do modelo que deverão ser executadas. Por isso, essa abordagem é raramente usada na prática.
* ***Filter methods*:** são métodos independentes de algoritmos de aprendizado. Eles avaliam a importância de cada *feature* com base apenas nas características dos dados. Alguns critérios que podem ser utilizados são correlação entre *features*, informação mútua.
* ***Embedded (*ou *intrinsic) methods*:** são métodos em que o processo de seleção das *features* já é executada automaticamente dentro do algoritmo de aprendizado, como é o caso das árvores de decisão.

# Principal Component Analysis

O PCA é uma técnica comumente utilizada em aplicações como redução de dimensionalidade, compressão com perda de dados, extração de *features* e visualização de dados [5].

Essa técnica funciona encontrando a projeção linear que minimiza a distância quadrática média entre os pontos e suas projeções. Ao minimizar essa distância quadrática média também estamos maximizando a variância das projeções dos pontos no hiperplano de projeção. Isso pode ser visto de maneira intuitiva à medida que escolhemos diferentes hiperplanos de projeção, como mostrado na Figura 9‑1 e na Figura 9‑2.

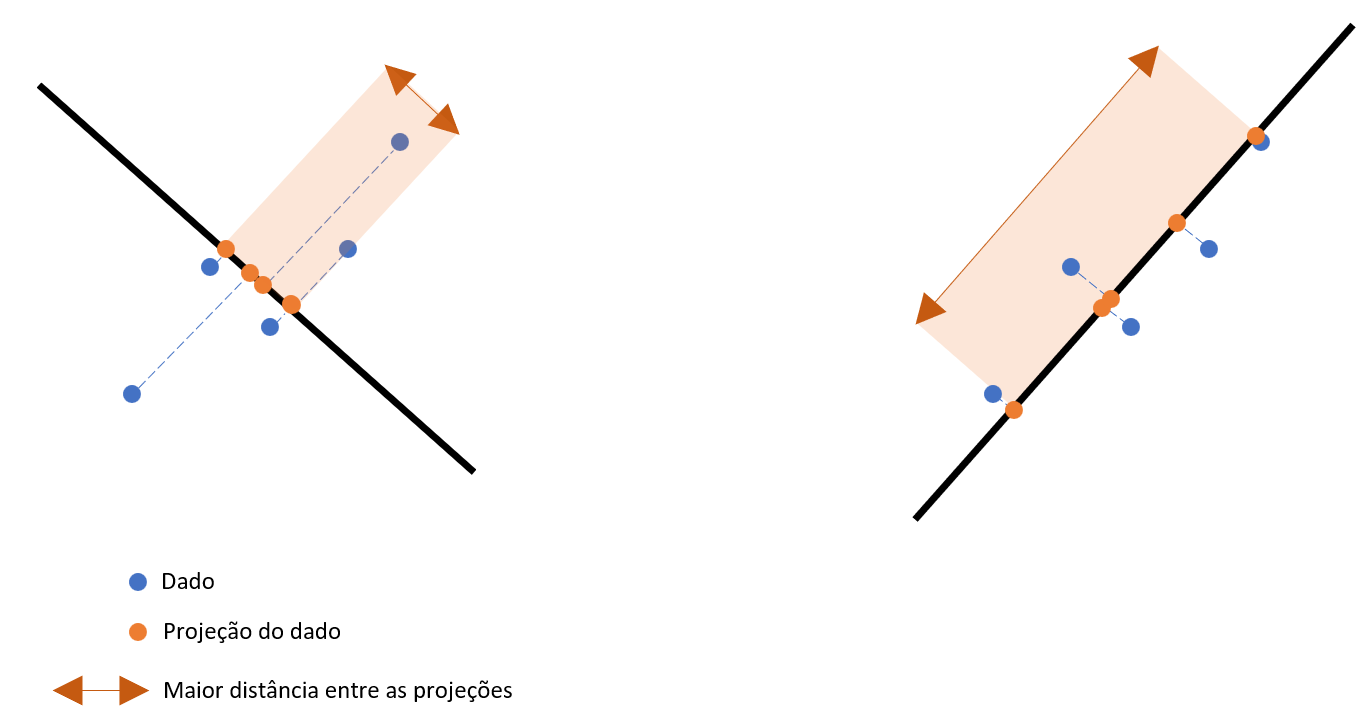


Figura 9‑1: Pontos sendo ajustados por dois hiperplanos de projeção diferentes (e perpendiculares). O ajuste da direita é o ajuste que minimiza a distância quadrática média entre os pontos e o hiperplano de projeção, resultando, assim, em uma maior variância das projeções sobre o hiperplano em questão (como pode ser visto pela seta laranja, que mostra a extensão do espalhamento dos dados). No ajuste da esquerda, feita por um hiperplano ortogonal ao da direita, vemos que as projeções dos dados têm uma variância menor.

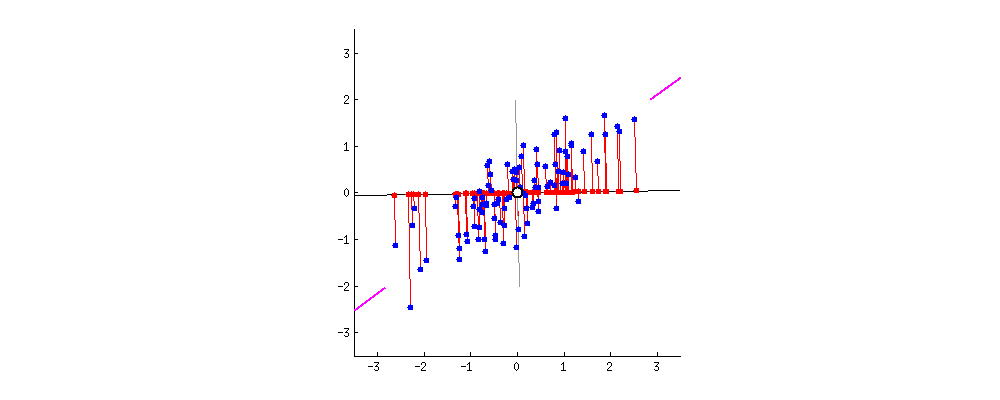


Figura 9‑2: Figura animada mostrando as projeções (pontos vermelhos) dos dados (pontos azuis) à medida que giramos o hiperplano de projeção.

Ao reduzirmos a dimensionalidade maximizando a variância nessa projeção, estamos garantindo a menor perda de representatividade dos dados possível. A Figura 9‑3 ilustra essa relação entre a maximização da variância e a representatividade da projeção.

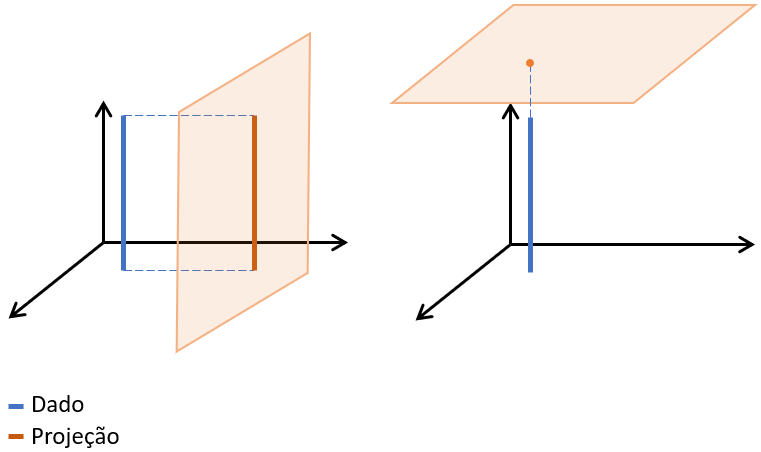


Figura 9‑3: Do lado esquerdo, temos uma projeção bastante representativa dos dados, pois o plano foi escolhido de forma a maximizar a variância da projeção. Por outro lado, do lado direito, o plano escolhido minimiza a variância da projeção, resultado em uma projeção pouco representativa dos dados.

A seguir, são mostrados os cálculos envolvidos no método de PCA.

## Formulação da Máxima Variância

Consideremos um espaço de dimensão . Nosso objetivo é projetar os dados em um espaço de dimensão de forma que a variância dos dados projetados seja máxima.

Por simplicidade, vamos considerar, inicialmente, que . Podemos representar a direção desse espaço usando o vetor unitário de dimensões. Assim, a média das projeções dos dados é dada por

em que e é a quantidade total de dados.

A variância dos dados projetados é dada por

em que é a matriz de covariância dos dados.

Tendo o vetor onde os dados serão projetados e a expressão da variância , basta fazermos

O Lagrangiano desse problema é

em que é um multiplicador de Lagrange.

Para maximizarmos essa expressão, derivamo-la com relação a e a igualamos a zero, encontrando como resultado a seguinte equação

Da equação acima, notamos que é um autovetor de , cujo autovalor é . Além disso, vemos que a variância dos dados projetados é igual ao autovalor . Como está sendo maximizada, então é o maior autovalor de . O vetor recebe o nome de **primeira componente principal**.

Se considerarmos o caso genérico em que o espaço onde os dados estão sendo projetados tem dimensão , então em que são os autovetores correspondentes aos maiores autovalores da matriz de covariância dos dados. Além disso, como é simétrica, assim como toda matriz de covariância, seus autovetores são todos ortogonais entre si [9]. Lembrando que a variância da projeção dos dados associada a cada autovetor é igual ao seu autovalor correspondente.

Por fim, para encontrar as coordenadas dos novos pontos projetados no espaço , basta projetar os pontos originais nos autovetores . De forma geral,

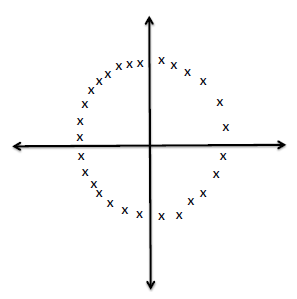
em que apresenta em cada linha uma instância/ um ponto , é a matriz contendo os autovetores nas colunas e é a matriz contendo em suas linhas os pontos projetados na base .

## Detalhes Importantes

Como foi visto na Seção 9.1, projetamos os dados em vetores que geram o espaço de projeção . O problema consiste basicamente em encontrar esses vetores cujas retas geradas minimizem a distância média quadrática aos pontos. No entanto, para fazer isso, precisamos que os dados estejam centralizados em zero, ou seja, precisamos subtrair dos dados a média deles. Observar na Figura 9‑2 como os dados estão centralizados. Se, nessa figura, por exemplo, os dados estivessem centrados em , a melhor reta seria diferente, assim como o vetor que a gerou. Não seria apenas diferente, como também geraria uma projeção com variância menor. Portanto, é possível ver a importância de centralizar os dados antes de aplicar o PCA.

Outros detalhes que podem estar associados a maus resultados do método PCA são listados abaixo**:**

* Centralização/escalamento mal realizados. A importância da centralização dos dados já foi discutida acima. O escalamento, por sua vez, também é importante, pois o resultado do PCA pode variar bruscamente com as unidades adotadas nas coordenadas dos dados [10]. Normalmente, realiza-se o escalamento utilizando o desvio padrão. Além disso, podem ser utilizadas outras técnicas de pré-processamento, como remoção de *outliers*.
* Não linearidade dos dados. Se os dados possuírem uma estrutura não linear, é bem possível que essa relação não-linear entre os dados seja perdida ao realizar a projeção no plano . Na imagem abaixo, a projeção dos dados em qualquer vetor resultaria numa perda da estrutura não linear.

****

## Relação com a Decomposição SVD

Se considerarmos a matriz dos dados com dimensões , em que é o número de dados e é a dimensão desses dados, podemos escrever a matriz de covariância dos dados como [11]

Ao realizar a decomposição SVD de , encontramos , em que é a matriz cujas linhas são os autovetores de e formam uma base ortonormal (conforme Apêndice B:). Além disso, na diagonal de estão os valores singulares de , que correspondem a , com os autovalores de .

Conhecer esses fatos é mais interessante numericamente para fazer os cálculos da PCA, pois, normalmente, é mais fácil determinar os autovalores e autovetores de por meio da decomposição SVD do que por meio da multiplicação , que costuma ser mais custosa.

Avaliação de Desempenho e Seleção de Modelo

## Métricas para Classificação Binária

As principais métricas usadas para classificação binária são apresentadas a seguir.

### Acurácia

É a taxa de acertos do modelo.

Desvantagens:

* Pode levar a conclusões errôneas caso as taxas de acertos de diferentes classes tiverem importâncias diferentes.
* Pouco adequada quando há um desbalanceamento nos dados que favorece muito uma única classe. A taxa de acerto da classe favorecida domina o resultado da acurácia, mascarando a contribuição das taxas de acerto das outras classes. Em um conjunto de dados em que apenas 1% das amostras são da classe 0 e 99% da classe 1, caso o modelo sempre dê uma predição de 1, sua acurácia será de 99%, apesar de ter errado a classificação de todos os dados da classe 0.

### True Positive Rate (TPR) ou Sensibilidade

Mede quão bom o modelo é com relação não deixar de “detectar” amostras positivas (FN). O nome “sensibilidade” vem de um contexto médico [12, p. 95], em que essa métrica é utilizada para medir a capacidade do modelo de detectar a presença de uma doença (sem deixar ela passar).

Uma tática para lembrar rápido da expressão é perceber que a TPR é 100% quando acertamos a classificação de todas amostras positivas. Com isso, o denominador tem que ser o número total de exemplos positivos.

### False Positive Rate (FPR)

Mede a taxa de falsos positivos, ou seja, quantas das amostras negativas são classificadas como positivas do total de amostras negativas. Uma forma de lembrar amostras negativas. Uma forma de lembrar dessa expressão, é só pensar que o caso em que o modelo sempre dá uma predição positiva, teremos FPR igual a 100%, pois todas as amostras negativas serão FP e o numerador se igualará ao denominador. Se o numerador fosse a soma das amostras positivas, não teríamos FPR igual a 100% nesse caso.

A TPR e a FPR, geralmente, são reportadas em pares. Outro par equivalente, seria a FNR e a TNR, que são os complementares da TPR e FPR, respectivamente.

### Precisão

Mnemônico: Precisão = TP / Preditas Positivas.

Mede quão preciso é o modelo na sua seleção de amostras positivas, ou seja, quantas das amostras preditas como positivas são de fato positivas. Está relacionada à capacidade do modelo de evitar falsos positivos.

A precisão e a FPR fornecem informação sobre a capacidade do modelo de evitar falsos positivos. No entanto, quando o número de negativos é muito maior do que o de positivos (o que é muito comum em problemas de diagnóstico de uma doença rara), é preferível utilizar a precisão. Isso porque, nesse caso, o denominador da FPR tende a ficar muito grande e a minimizar o valor de FPR. Por outro lado, a precisão não é afetada por isso, já que o denominador leva em conta apenas as amostras classificadas como positivas.

### *Recall*

Mnemônico: *Recall* =TP / Real Positive.

É equivalente a TPR. Logo, mede a capacidade do modelo de identificar amostras positivas do total de amostras positivas, ou seja, a capacidade do modelo de evitar falsos negativos.

### F1*-score*

Mede o equilíbrio entre precisão e *recall* ou, de forma equivalente, o equilíbrio entre falsos positivos e falsos negativos. Varia de 0 a 1. Se o valor for baixo, a métrica indica que pelo menos ou são baixos. Sendo e altos, também será alto.

É interessante notar que o F1-*score* é a média harmônica de precisão e do *recall*. Reparar que . O motivo para se escolher a média harmônica e não a média aritmética, por exemplo, é que a primeira penaliza os casos em que há desequilíbrio entre e , ou seja, elevado e baixo e vice-versa. Isso pode ser visto por meio dos gráficos das médias aritmética e harmônica para diferentes combinações de e , como mostrado na Figura 9‑4. Isso penaliza casos como o do exemplo da Seção 10.1.1, em que o modelo sempre prevê a mesma classe. Nesse caso, a média harmônica penaliza mais o modelo do que a aritmética, o que é razoável, já que ele é muito ruim.

|  |  |
| --- | --- |
|  |  |
| 1. Média harmônica. | 1. Média aritmética. |
| Figura 9‑4: Comparação entre a média harmônica e aritmética da precisão e do recall. | |

### F-*score*

É a forma geral do F1-score, que permite atribuir graus de importância diferentes para e Para , estamos dando mais importância para e, para , estamos dando mais importância para (apesar de isso não ser muito intuitivo, olhando apenas para a expressão). indica que estamos dando um peso duas vezes maior para . Isso fica mais fácil de compreender quando percebemos que essa expressão corresponde à média harmônica ponderada de e , pois temos

Com a primeira igualdade, fica mais simples de ver que isso se trata de uma média harmônica ponderada. Com a segunda igualdade, vemos que o termo tem mais importância quando maior que 1, pois nesse caso, . No caso limite em que , e e o termo associado a tem nenhuma importância. Portanto, não importa se é grande ou pequeno, pois ele terá uma porcentagem menor de participação no resultado final quando comparado com . Se por exemplo, tivéssemos então .

### *Receiver Operating Characteristic* (ROC)

É o gráfico da TPR pela FPR, como mostrado na Figura 9‑5. Em problemas em que temos que decidir um limiar de probabilidade para classificar uma amostra como positiva, essa curva é útil, pois ela resume a relação da TPR e da FRP para diferentes valores de limiar. Se as duas métricas tiverem importâncias iguais, o melhor ponto dessa curva é na parte superior esquerda, já que quanto menor a FPR, melhor.

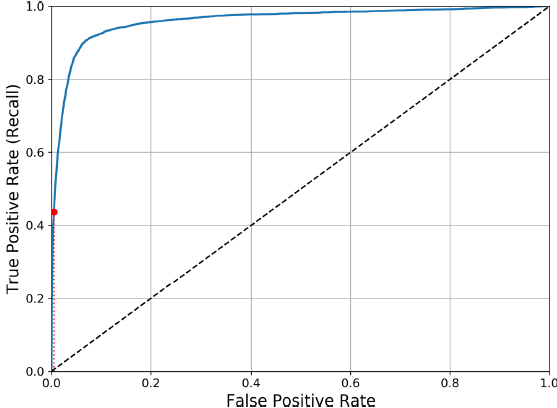


Figura 9‑5: Curva ROC.

Para diferentes valores de hiperparâmetros, teremos diferentes curvas ROC. Uma forma de comparar diferentes curvas, é observar a forma de cada uma delas e determinar a que fornece a melhor combinação de TPR e FPR. Usualmente, quanto mais perto do extremo superior esquerdo estiver o ponto melhor. No entanto, isso não é muito conveniente. Uma forma mais prática de comparar essas curvas é usas a métrica AUC (*Area Under the Curve*). Quanto maior o AUC, melhor é o modelo. Um modelo perfeito terá AUC igual a 1.

Uma alternativa à curva ROC é a curva Precisão x *Recall*, que normalmente é utilizada quando temos um número de amostras negativas muito maior do que o de amostras positivas.

## Métricas para Classificação Multiclasse

Em u problema de classificação multiclasse, ainda podemos utilizar as métricas para o problema binário, mas para cada classe. Por exemplo, se tivermos 3 classes, A, B e C, poderíamos analisar cada classe individualmente, calculando as métricas da Seção 10.1 para cada uma das classes. Para isso usamos uma estratégia *one-vs-the-rest*, ou seja, consideramos a classe em questão como positiva e todas as outras como negativa. Por exemplo, para calcular a precisão para a classe A, consideramos a classe A como positiva e as classes B e C como negativas.

Apesar de podermos usar essa estratégia, isso faz com que tenhamos vários métricas, o que torna a análise complicada, principalmente quando o número de classes é grande. Por isso, é importante definir métricas que resumam a performance global do modelo. Essas métricas são apresentadas a seguir. Na definição dessas métricas, consideraremos um conjunto de classes , com cardinalidade , e utilizaremos o termo para representar a contagem de casos pertencentes à classe (‘real’) que foram classificados como classe (‘predito’).

### Acurácia

É o total de acertos sobre o total de casos.

Quando o número de exemplos de cada classe é desbalanceado, essa métrica pode mascarar o desempenho de classes com baixa contagem de exemplos. Assim, se uma classe minoritária tiver uma taxa de erros muito elevada, mas todas as outras classes tiverem bom desempenho, a acurácia terá a assumir valores mais altos, mascarando o mau desempenho da classe minoritária.

### Acurácia Balanceada

em que é o *recall/*TPR de uma classe .

Logo, a acurácia balanceada é a média das dos valores de TPR para as diferentes classes.

Essa métrica atribui importâncias iguais para cada classe, em vez de atribuir importâncias iguais para cada amostra independentemente da classe, como é o caso da acurácia. Portanto, se considerarmos um exemplo em que há uma classe com poucas amostras e muitos erros de classificação e outras classes com várias amostras e boa performance, teremos . Isso porque a classe minoritária terá um papel para o cálculo da acurácia balanceada tão importante quanto as outras.

Para conjuntos de dados balanceados, não faz sentido usar essa métrica, pois ela tende a se igual à acurácia. Além disso, mesmo que o conjunto de dados seja desbalanceado, se a taxa de acertos global for mais importante do que controlar a taxa de acertos em cada classe, talvez a acurácia seja uma métrica mais recomendada do que a acurácia balanceada.

### Métricas Macro

Macro é uma maneira de calcular métricas que considera cada classe como a unidade básica para o cálculo, ou seja, é a média das métricas calculadas para cada classe no esquema *one-vs-all* (uma classe é considerada positiva e as outras negativas).

Consideremos que , e são, respectivamente, a precisão, o *recall* e o f1-score para uma certa classe , considerando que essa classe é a positiva e todas as outras negativas.

Dessa forma, a precisão, o *recall* e o f1-*score* macro são dados, respectivamente, por:

|  |  |  |
| --- | --- | --- |
|  |  | (9.1) |

É interessante mencionar que em [13], é dada uma definição diferente para o f1-*score* macro, em que essa métrica é calculada a partir da média harmônica de e , ou seja, . No entanto, a definição usada na biblioteca *sklearn* do Python não é a que foi apresentada na eq. (9.1).

Além disso, é interessante observar que a acurácia balanceada é igual ao *recall* macro. No entanto, a acurácia macro não é igual à acurácia balanceada.

### Métricas Macro Ponderadas (*weighted*)

São métricas calculadas de maneira similar às macro, porém ponderando as métricas de cada classe usando o número de amostras de cada uma delas. Dessa forma, a precisão, o *recall* e o f1-*score* macro ponderados são dados por

é o total de amostras pertencentes à classe .

Essas métricas devem ser utilizadas se for desejável ter métricas que resumam o desempenho global do modelo levando em consideração a quantidade de amostras em cada classes. As classes com poucas amostras receberão menos importância e as classes com mais amostras receberam mais importância no resultado final. Caso se queira dar a mesma importância para todas as classes, mas ainda assim ter métricas globais, é melhor utilizar as métricas macro.

### Métricas Micro

Essas métricas são calculadas de maneira global, sem diferenciar amostras individuais pela classe a qual elas pertencem, considerando o número total de TP, FP e FN. Dessa forma, a precisão micro e o *recall* são dados por

Reparar que . Portanto, o F1-*score* é dado por

Por fim, reparar que são iguais à acurácia, pois essas métricas consistem na razão entre os acertos e o total de amostras.

## Métricas para Regressão

As principais métricas usadas para regressão são apresentadas abaixo.

### *Mean Squared Error* (MSE)

Vantagem:

* É diferenciável.

Desvantagem:

* Não é medido nas mesmas unidades que e .
* Como os resíduos são elevados ao quadrado, é dado um peso maior para *outliers.*

### *Root Mean Squared Error* (RMSE)

Vantagem:

* É diferenciável.
* É medido nas mesmas unidades que e .

Desvantagem:

* Como os resíduos são elevados ao quadrado, é dado um peso maior para *outliers.*
* Apesar de ser medido nas mesmas unidades que , o RMSE não representa a diferença média entre o *target* e o valor predito. Um RMSE igual a 10 não significa que o modelo erra em 10 na média.

### *Mean Absolute Error* (MAE)

Vantagem:

* Como os resíduos não são elevados ao quadrado, todos os erros são pesados de maneira igual.
* É medido nas mesmas unidades que os resíduos, e .

Desvantagem:

* Não é facilmente diferenciável.

### *Mean Absolute Percentage Error* (MAPE)

Vantagem:

* É uma porcentagem. Logo, é independente de escala e pode ser comparado com MAE de modelos de diferentes conjuntos de dados.

Desvantagem:

* Não é facilmente diferenciável.

### Coeficiente de Correlação de Pearson (PCC)

e são as variâncias amostrais de e , respectivamente, e é a covariância amostral entre e .

### Coeficiente de Determinação ()

#### Modelos lineares

O coeficiente de determinação surge naturalmente para avaliação de modelos de regressão lineares. Considerando que e são, respectivamente, a média e a variância amostrais dos *targets,* a seguinte expressão é valida para o coeficiente de determinação para modelos de regressão linear [14, p. 68]

|  |  |  |
| --- | --- | --- |
|  |  | (9.2) |

em que [14, p. 44]

|  |  |
| --- | --- |
|  | :*Sum of Squared Residuals* (também chamada de variância não explicada pelo modelo) |
|  | :*Total Sum of Squared Deviations* |
|  | :*Sum of Squared residuals when considering Regression* (também chamada de variiância explicada pelo modelo) |

O que esse coeficiente indica é a proporção de desvio quadrático quando consideramos que os valores da regressão são verdadeiros (mas mantendo a média verdadeira ) com relação ao desvio quadrático real (mantendo os valores reais ). Apesar de compor (observar que ), essa interpretação dificulta um pouco o entendimento. Podemos enxergar essa divisão apenas como uma forma de reportar o de maneira proporcional. Sozinho, o não tem muito valor interpretativo. No entanto, quando o dividimos por , estamos comparando-o a uma referência.

Outra forma de interpretar essa métrica é olhando para a primeira igualdade. O termo pode ter uma interpretação análoga a que criamos no parágrafo anterior: é uma forma de reportar o MSE, porém, comparado a uma grandeza de referência, como a variância amostral . O portanto, é o complementar disso.

Por fim, uma última interpretação pode ser feita. O termo representa o de um modelo de regressão que sempre tem como saída a média . Portanto, estamos comparando o do modelo com o de um modelo trivial que sempre prevê a média.

quando o modelo sempre acertar as previsões, ou seja, quando .

quando o modelo for substituível pelo modelo que sempre prevê a média, ou seja, .

quando o modelo for pior do que o modelo que sempre prevê a média, ou seja, . Nesse caso, seria melhor simplesmente prever a média.

#### Modelos não-lineares

Para modelos não-lineares, a equação (9.2) não é válida [15]. Isso porque e, por isso, . Dessa forma, o coeficiente de determinação é dado por

Assim como no caso linear, , sendo

quando o modelo acertar todas as previsões;

quando o modelo for equivalente a prever sempre a média;

quando o modelo for pior do que o modelo que só prevê a média.

## Métodos de Validação

Apêndices

Abaixo são apresentados os apêndices.

###### Teoria da Informação

Caso Discreto

Informação

A **informação** é uma grandeza que quantifica a “surpresa” causada por um valor observado da variável aleatória , com p.m.f . A expressão da informação é dada por

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.1) |

Quando a base do logaritmo é 2, a informação é medida em bits. Quando o logaritmo é natural, a informação é medida em nats. Em *machine learning*, usualmente utilizamos o logaritmo natural.

Reparar que, como , .

Com isso, vemos que quanto mais raro for um evento, maior é a informação associada a ele. Então, a informação de que “hoje o sol nasceu”, que tem probabilidade praticamente 1, teria informação nula, já que não é nenhuma surpresa de que o sol nasce todos os dias. Se por acaso, algum dia o sol não nascesse, a informação teria valor infinito, pois é algo com probabilidade praticamente 0 de acontecer.

Tentando dar outra interpretação intuitiva para essa grandeza, é como se ela medisse o quanto uma informação é informativa. Assim, “o sol nasceu” é pouco informativo e, por isso, tem informação nula.

De maneira similar, podemos definir a informação condicional como sendo a informação que ainda resta de um valor observado quando se conhece um valor observado da v.a. . Ela é dada por

|  |  |  |
| --- | --- | --- |
|  |  | (A.2) |

Continuamos tendo a mesma interpretação da informação. Só trocamos a p.m.f por outra p.m.f .

É importante ressaltar que, a informação condicional NÃO é a parcela de informação (ou “surpresa”) de que se esvai por conhecer , ou seja, não é a parcela da incerteza de compartilhada com . Isso ficará claro mais para frente.

Entropia

A entropia é a informação média (ou “surpresa” média) de uma variável aleatória, ou seja, é a soma da informação para cada valor observado ponderado pela sua probabilidade (ou “frequência”, sob uma ótica frequentista). Sua expressão é dada por

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.3) |

Observar que , pois , já que .

A entropia é mínima quando , ou seja, . Intuitivamente, apenas um evento ocorre com probabilidade 1, de forma que não temos nenhuma “surpresa”.

A entropia é máxima quando . Nesse caso, a entropia é dada por , com .

Entropia Condicional

É a informação condicional média. Dessa forma, nos baseando na eq. (A.3) e na *Law of The Unconscious Statistician* (LOTUS) [3, p. 170], também conhecida como *Rule of the Lazy Statistician* [2, p. 48], podemos escrever

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.4) |

Lembrando que estamos encarando como uma função das variáveis aleatórias e .

Informação Mútua

Definimos a seguinte quantidade

|  |  |  |
| --- | --- | --- |
|  |  | (A.5) |

que, em [6, p. 56], é chamada de informação mútua. Ela quantifica a informação que temos de por conhecer e vice-versa (já que ), ou seja, é a parcela da informação compartilhada por e . Isso fica mais claro quando escrevemos essa quantidade como . é a “surpresa” de que ainda resta depois de conhecermos . Ao subtrairmos essa quantidade de , que é toda a incerteza associada a , ficamos com a parcela da informação de que conhecemos plenamente só por conhecermos . A informação mútua ainda pode ser vista como a redução da incerteza ou “surpresa” associada a por conhecer .

Se , então , o que indica que conhecer o valor observado reduz a “surpresa” associada a de unidades de informação, ou seja, reduz a incerteza de a zero. Por outro lado, se e forem independentes, então , o que indica que conhecer o valor não reduz em nada a incerteza sobre .

De forma análoga ao que foi feito para a entropia e para a entropia condicional, podemos calcular a informação mútua média associada às variáveis aleatória e . A informação mútua média é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.6) |

Pode ser mostrado que , sendo nula somente quando e forem independentes.

De maneira geral, chamamos a quantidade definida pela eq. (A.6) de **informação mútua**. Apesar de em [6, p. 56] haver uma diferenciação de nomenclatura entre a eq. (A.5) e a eq. (A.6), normalmente a eq. (A.5) não é muito comum e preferimos reservar o nome “informação mútua” para a eq. (A.6).

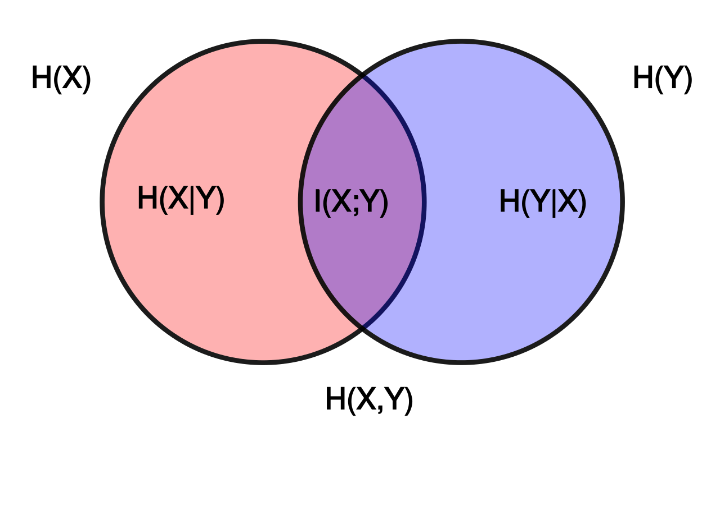
Assim, podemos ver que a informação mútua é uma ótima forma para quantificar a independência entre duas variáveis aleatórias. Com isso, vemos que outra interpretação que poderíamos fazer da informação mútua é que ela quantifica o quanto de informação e compartilham entre si.

Por fim, reparamos que também podemos escrever

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.7) |

o que está de acordo com a interpretação dada no início desta subseção, de que a informação mútua mede a redução da “surpresa” média associada a v.a. por conhecermos a v.a. .

O diagrama abaixo ilustra a relação da informação mútua com as outras quantidades vistas nesta seção:



Divergência Kullback-Leibler

A **divergência Kullback-Leibler** ou **entropia relativa** é uma medida utilizada para quantificar a diferença entre uma distribuição e uma distribuição de referência . Ela é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.8) |

que se lê como “divergência KL de para ” e com isso estamos calculando o quanto a distribuição diverge de . é a informação de , que tem distribuição , e é a informação de quando aproximamos sua distribuição por . Vemos que é tido como referência, até mesmo porque multiplicamos por no somatório, pois estamos considerando que a distribuição de é descrita por nesse referencial. É importante notar que , ou seja, ao mudarmos o referencial, a divergência muda. Logo, não podemos dizer que a divergência KL representa uma métrica de distância.

Observar que, como , temos que

em que é a entropia de quando aproximamos sua distribuição por , também chamada de **entropia cruzada**, como veremos adiante.

Em *machine learning*, muitas vezes utilizamos a expressão para quantificar o quanto uma distribuição desconhecida é divergente de uma distribuição que tenta aproximá-la.

É importante reparar que [5, p. 55].

Finalmente, reparamos que existe uma relação entre a informação mútua e a divergência KL, que é ilustrada na equação:

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.9) |

Entropia Cruzada

Às vezes, em problemas de *machine learning*, podemos nos deparar com a expressão da **entropia cruzada**, que é dada por

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.10) |

Ela é a “surpresa” média que temos ao codificarmos uma v.a. que tem distribuição com uma distribuição .

Se repararmos bem, ela é muito parecida com a equação da divergência KL. De fato, temos que

Considerando que é a distribuição que dá a codificação ótima para (que tem menor informação média necessária associada), então a divergência KL é a “surpresa” média por tentarmos utilizar uma distribuição , que não é ótima (vai exigir mais informação para codificar ), menos a “surpresa” média ao utilizarmos a distribuição ótima (entropia).

A equação da entropia cruzada surge quando temos uma variável que tem uma distribuição e queremos aproximá-la com outra distribuição , parametrizada pelo vetor de parâmetros a ser otimizado. Para isso, o mais óbvio a se fazer é minimizar a divergência , o que resulta em

pois não depende do vetor de parâmetros , já que também não depende.

Geralmente, a entropia cruzada surge no contexto de classificação, pois ela é usualmente utilizada no cálculo da função custo. Se considerarmos o caso da classificação com classes , teríamos um problema modelado da seguinte forma: , representando o espaço amostral; representando o espaço imagem da variável aleatória ; sendo a p.m.f estimada de sendo a p.m.f real de

Considerando que estejamos avaliando um ponto , que representa um dado, pertencente a uma classe , teremos a seguinte expressão para a entropia cruzada:

Como a classe do ponto é conhecida, a distribuição das classes para esse ponto é , ou seja, para . Logo,

**Observar que, no desenvolvimento acima, não representa os dados!** Para evitar confusões, podemos reescrever a equação da entropia cruzada para um determinado ponto trocando as nomenclaturas da seguinte forma:

em que é a variável aleatória que representa o número da classe a qual pertence o ponto .

Caso Contínuo

As equações para o caso discreto podem ser generalizadas para o caso contínuo. O desenvolvimento necessário para isso está explicado em [6, p. 59].

Entropia

Também chamada de **entropia diferencial** é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.11) |

A entropia é máxima quando segue uma distribuição normal.

Observar que, no caso contínuo, pode assumir valores maiores do que 1, o que pode fazer com que possamos obter valores negativos de entropia.

Entropia Condicional

A entropia condicional é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.12) |

Informação Mútua

A informação mútua é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.13) |

Divergência Kullback-Leibler

A divergência Kullback-Leibler é dada pela expressão

|  |  |  |  |
| --- | --- | --- | --- |
|  | |  | | --- | |  | | (A.14) |

###### Decomposição SVD

Qualquer matriz de pode ser decomposta da seguinte maneira

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | (B.1) |

em que

é uma matriz ortogonal cujas colunas são os autovetores de e são chamadas de left singular vectors de A [16],

é uma matriz ortogonal cujas colunas são os autovetores de e são chamadas de right singular vectors de A e

é uma matriz diagonal (possivelmente retangular) cujos valores da diagonal principal são as raízes quadradas dos autovalores de e de e são chamados de **valores singulares**.

Essa decomposição é chamada de SVD [17]. A Figura 9‑6 ilustra essa decomposição.

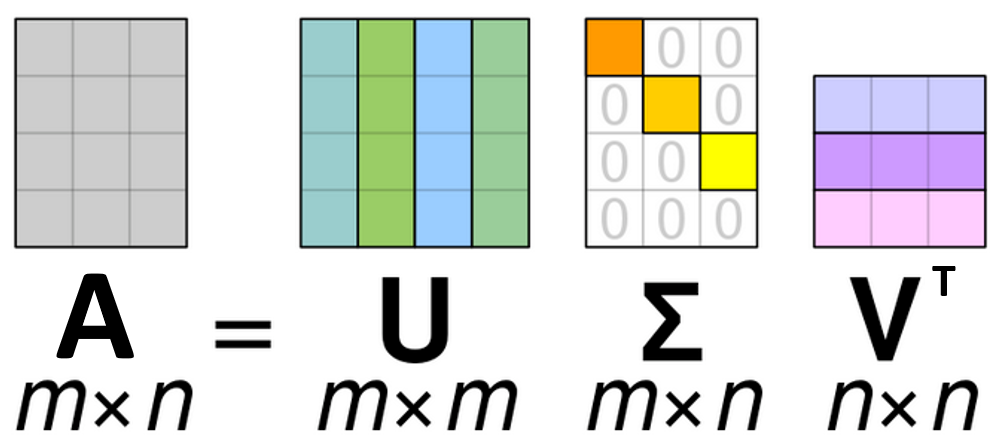


Figura 9‑6: Representação gráfica da decomposição SVD.

Lembrando que e de são matrizes diferentes (normalmente com dimensões diferentes) que apresentam autovetores diferentes, mas os mesmos autovalores. Lembrando também que, o número de autovalores é igual ao posto (*rank*) da matriz.

A partir da eq. (B.1), podemos escrever

lembrando que e que , pois é ortogonal. A expressão acima é a diagonalização da matriz (decomposição espectral). Logo, fica claro que as colunas de são de fato os autovetores de . Além disso, vemos que os valores da diagonal de correspondem a

|  |
| --- |
|  |

em que são os valores da diagonal da matriz de autovalores de .

É possível provar que toda matriz de posto 1 pode ser escrita como produto externo de um vetor de tamanho por outro de tamanho [16]:

Além disso, toda matriz de posto pode ser escrita como a soma de matrizes de posto 1 [16]. A título de ilustração, uma matriz de posto 2 ficaria

|  |  |  |
| --- | --- | --- |
|  |  | (B.2) |

Com isso, podemos escrever a decomposição SVD como

|  |  |  |
| --- | --- | --- |
| |  | | --- | |  | | (B.3) |

Logo, podemos escrever a decomposição SVD como a soma dos produtos externos da coluna da matriz com a linha da matriz escalados pelo valor singular . Isso faz sentido quando olhamos para o termo da direita da eq. (B.2).

*Low-rank Aproximation* por SVD

A *low-rank approximation* de uma matriz usando SVD consiste em aproximar a matriz por uma matriz de posto . Isso é feito ao organizar a decomposição da eq. (B.1) de forma que os valores singulares estejam dispostos em em ordem decrescente (o primeiro valor da diagonal é o maior) e zerando os menores valores singulares (e as colunas/linhas correspondentes nas matrizes e ) até restarem valores singulares não-nulos. Isso é equivalente, na eq. (B.3), a eliminar as parcelas com os menores valores de até restarem apenas parcelas.

Isso faz sentido porque, como e são unitários, a norma de Frobenius do seu produto externo é .

Lembrando que é o equivalente a colocar todos os elementos de em um único vetor e calcular . Assim, a norma de Frobenius transmite uma ideia da magnitude dos elementos armazenados na matriz.

Logo, a contribuição da parcela na matriz final tende a ser menor quanto menor for . Portanto, eliminamos as parcelas da eq. (B.3) em ordem crescente de .

Ao fazer isso, encontramos uma matriz aproximada tal que , sendo uma matriz de dimensões , assim como . Isso quer dizer que é a matriz mais próxima de se usarmos a norma de Frobenius como medida de distância [16].

**Exemplo:**

Decomposição da matriz

Ao realizarmos a decomposição SVD de encontramos uma matriz de valores singulares

A matriz aproximada de posto 2 é

Assim, em vez de ter que armazenar os 25 valores da matriz A original, bastaria armazenar os 2 valores singulares de mais 20 valores das linhas e colunas de e correspondentes, totalizando 22 valores. O ganho parece pouco nesse exemplo, mas em aplicações em que a matriz é muito grande, ao guardarmos apenas alguns valores singulares, temos um ganho muito significativo.

###### Otimização e Dualidade

Um problema de otimização (não necessariamente convexo) na forma padrão tem a seguinte forma:

|  |  |  |
| --- | --- | --- |
|  |  | (C.1) |

em que é chamada de **função objetivo** e as funções e são chamadas de **funções de restrição**. Denotamos o valor ótimo desse problema . O valor , valor de que leva a , é chamado de **ótimo primal**. Além disso, todo que pertence ao domínio de e respeita as restrições do problema (C.1) é chamado de **ponto viável**. Por fim, muitas vezes chamamos o problema (C.1) de **problema primal** (essa nomenclatura fará sentido mais para frente).

A ideia básica da dualidade de Lagrange é levar em conta as restrições em uma única equação estendendo a expressão da função objetivo [18]. Essa expressão estendida é chamada de **Lagrangiano** (ou função de Lagrange) e é dada por:

|  |  |  |
| --- | --- | --- |
|  |  | (C.2) |

Os termos e são chamados de **multiplicadores de Lagrange**. Os primeiros associados às restrições de desigualdade e os segundos às restrições de igualdade. Observar que, quando , estamos premiando os valores se que tornam muito negativa, pois, quanto mais negativa menos vale .

Dando prosseguimento, ao tentar minimizar , encontramos a **função de Lagrange dual**, que é definida como o mínimo do Lagrangiano com relação a . Ela é dada por

|  |  |  |
| --- | --- | --- |
|  |  | (C.3) |

A função de Lagrange dual é côncava, mesmo que o problema definido em (C.1) não seja (checar as condições necessárias para a convexidade de um problema de otimização em [18, p. 136]).

Para entender a afirmação acima, precisamos reparar que estamos falando da concavidade de com relação a , e não a . Levando isso em conta, podemos escrever o Lagrangiano como , colocando como um parâmetro e como as únicas variáveis. Nesse caso, ao fixarmos um , podemos dizer que é uma soma de funções afins, pois com , e tornam-se constantes. Com isso, podemos dizer que é uma família de funções afins. Logo, , que é uma função côncava, pois para cada valor de , é côncava [18, pp. 80, 87].

A função de Lagrange dual representa um limite inferior para o valor ótimo, ou seja, . Isso porque, para um ponto viável e para ( é igual a elemento a elemento), , já que e . Logo, . Assim, para cada par com , representa um limite inferior diferente para .

Poderíamos nos perguntar qual é o melhor limite inferior que poderíamos encontrar a partir de . Essa pergunta dá origem ao **problema dual de Lagrange** que é definido como:

|  |  |  |
| --- | --- | --- |
|  |  | (C.4) |

Nos referimos a como **ótimo dual** e denotamos seu valor ótimo correspondente . Reparar que o problema (C.4) é convexo, pois a função objetivo é côncava e a restrição é convexa.

Podemos afirmar que , já que é um limite inferior para . Essa propriedade é chamada de **dualidade fraca**. Quando temos uma igualdade, ou seja, , falamos em **dualidade forte**. Além disso, chamamos de **gap de dualidade** a diferença . Em geral, a dualidade forte não é válida. No entanto, quando o problema primal é convexo, normalmente temos dualidade forte [18, p. 226].

Quando a dualidade forte é válida, podemos escrever

Com isso, podemos concluir que, na verdade, as desigualdades são igualdades. Logo, quando o gap de dualidade é zero, temos . Mas, como todos os termos dessa soma são não-positivos, temos que

Essa propriedade é chamada de complementary slackness*.* Além disso, podemos ver que minimiza com relação a

Por fim, todo problema de otimização na forma (C.1) e com restrições e função objetivo diferenciáveis devem respeitar as chamadas **condições de KKT** (Karush-Kuhn-Tucker), que são as seguintes:

As duas primeiras condições são as restrições definidas inicialmente em (C.1). A condição 3 é necessária para que a função de Lagrange dual seja um limite inferior para , como visto anteriormente. A condição 4 vem da *complementary slackness*. A condição vem do fato de que , como visto anteriormente.

Se o problema primal for convexo, a validade das condições de KKT já são suficientes para afirmar que existe dualidade forte.

Portanto, vemos que o problema de otimização apresentando em (C.1) se resume a com e, sob condição de gap de dualidade nulo, respeitando as condições de KKT.

###### Reproducing Kernel Hilbert Spaces

Para entender o conceito de Reproducing Kernel Hilbert Spaces (RKHS), é necessário entender outros conceitos mais básicos, como o conceito de espaço de Hilbert.

Um espaço de Hilbert é um espaço com um produto interno que é completo com respeito à norma definida pelo produto interno. Um espaço completo é aquele em toda sequência de Cauchy converge para um membro desse espaço, sendo uma sequência de Cauchy é uma sequência cujos elementos se tornam arbitrariamente muito próximos uns dos outros à medida que a sequência progride [19].

O espaço de Hilbert é uma generalização do espaço Euclidiano para um espaço de dimensão finita ou infinita (o espaço Euclidiano tem dimensão finita) [19]. Aparentemente, um espaço de Hilbert finito é bem parecido com o espaço Euclidiano. Prece que as diferenças começam a surgir quando falamos de um espaço de Hilbert de dimensão infinita.

Por simplicidade, o produto interno e a norma do espaço de Hilbert serão escritos sem o subscrito .

Um reproducing kernel Hilbert space(RKHS) é um espaço de Hilbert de funções com um *reproducing kernel* (ou **kernel**) em que e . Essa igualdade é chamada ***reproducing property****.*

Considere uma função kernel de duas variáveis. Suponha que, para pontos, fixemos a variável para ter , que são todas funções da variável . RKHS é um espaço de funções que é o conjunto de todas as possíveis combinações lineares dessas funções, ou seja,

Trazendo para algo concreto, poderíamos ter o kernel . As funções e seriam exemplo de funções pertencentes ao RKHS

Então, vemos que o kernel é a base para gerar o RKHS.

Dado um kernel, o RKHS é único e, dado um RKHS, o kernel correspondente é único [19].

A partir da *reproducing property*, se , então

|  |  |  |
| --- | --- | --- |
|  |  | (D.1) |

ou seja, a ordem dos argumentos não importa.

Na primeira igualdade, temos o produto interno entre e , ou seja, uma função de um único parâmetro e outra com dois parâmetros, mas o segundo parâmetro está fixado em . Logo, o resultado é . A segunda igualdade vem do fato que , em que vem do fato de esse espaço de Hilbert ser composto apenas de funções reais.

|  |
| --- |
| Seja um RKHS, associado a uma função kernel e com sendo um conjunto de elementos. Então, o mapeamento  é chamado de feature map e o espaço é chamado de **espaço das** features. é chamado de **espaço das entradas** (*input space*). |

O mapa das *features*, que pode ser finito ou infinito, é um vetor Um exemplo de *feature map* finito de dimensão 3 é , com . Nesse espaço, temos apenas três *features*: .

O seguinte produto interno é chamado de **kernel trick**:

A prova para isso pode ser encontrada em [19].

A partir da eq. (D.1), vemos que Com isso, fica claro que o *feature map* é uma função em que fixamos um dos argumentos em . Logo, o *feature map* leva os dados do espaço das entradas para o espaço das *features* composto por funções, que costuma ter um número de dimensões muito mais elevado, possivelmente infinito.

No exemplo do espaço finito apresentado acima, o kernel é dado por , com . No caso específico desse exemplo, vemos que o *features map* avaliado no ponto não é função da variável , apesar de isso não ser sempre verdade (aparentemente).

Com isso, vemos que, podemos realizar produtos internos de maneira bastante eficiente quando empregamos esse mapeamento, pois basta avaliar o kernel nos pontos e .

Abaixo, são listados alguns kernel mais conhecidos.

**Kernel linear**

Nesse tipo de kernel, conhecemos o *feature map*, que é

**Kernel Gaussiano ou *Radial Basis Function* (RBF)**

Um valor típico para é , em que é a dimensionalidade dos dados.

**Kernel polinomial**

Com sendo o coeficiente angular, o coeficiente linear e a dimensionalidade dos dados. Valores típicos para os parâmetros são e .

# Referências

|  |  |
| --- | --- |
| [1] | J. H. Friedman, “Greedy function approximation: a gradient boosting machine,” *Annals of statistics,* pp. 1189-1232, 2001. |
| [2] | L. Wasserman, All of Statistics, Pittsburgh: Springer, 2003. |
| [3] | J. K. Blitzstein e J. Hwang, Introduction to Probability, 2 ed., Boca Raton: CRC Press, 2019. |
| [4] | T. Hastie, R. Tibshirani e J. Friedman, The Elements of Statistical Learning, 2nd ed., New York: Springer, 2009. |
| [5] | C. M. Bishop, Pattern Recognition and Machine Learning, New York: Springer, 2006. |
| [6] | S. Theodoridis, Machine Learning: a bayesian and optimization perspective, 2nd ed., London: Elsevier, 2020. |
| [7] | A. Géron, Hands-on Machine Learning with Scikit-learn, Keras & Tensorflow: Concepts, Tools and Techniques to Build Intelligent Systems, Sebastopol: O'Reilly, 2019. |
| [8] | J. Li, K. Cheng, S. Wang, F. Morsttater, R. P. Trevino, J. Tang e H. Liu, “Feature Selection: A Data Perspective,” *ACM Computing Surveys,* vol. 50, 2017. |
| [9] | M. Cabral e P. Goldfeld, Curso de Álgebra Linear: Fundamentos e Aplicações, 3 ed., Rio de Janeiro: Instituto de Matemática, 2012. |
| [10] | T. Roughgarden e G. Valiant, “Lecture #7: Understanding and using Principal Component Analysis (PCA),” 2023. |
| [11] | “Covariance Matrix,” Wikipédia, [Online]. Available: https://en.wikipedia.org/wiki/Covariance\_matrix. [Acesso em 14 10 2023]. |
| [12] | N. Japkowicz e M. Shah, Evaluating Learning Algorithms: A Classification Perspective, Cambridge University Press, 2011. |
| [13] | M. Grandini, E. Bagli e G. Visani, “Metrics for Multi-Class Classification: An Overview,” *arXiv preprint arXiv:2008.05756,* 2020. |
| [14] | S. Chatterjee e A. S. Hadi, Regression Analysis by Example, 5 ed., Cairo: Wiley, 2012. |
| [15] | T. O. Kvalseth, “Note on the R2 measure of goodness of fit for nonlinear models,” *Bulletin of the Psychonomic Society,* vol. 21, nº 1, pp. 79-80, 1983. |
| [16] | T. Roughgarden e G. Valiant, “The Singular Value Decomposition (SVD) and Low-Rank Matrix Approximations,” 2023. |
| [17] | G. Strang, Linear Algebra and Its Applications, 4 ed., Cengage Learning, 2005. |
| [18] | S. Boyd e L. Vandenberghe, Convex Optimization, Cambridge University Press, 2004. |
| [19] | B. Ghojogh, A. Ghodsi, F. Karray e M. Crowley, “Reproducing Kernel Hilbert Space, Mercer's Theorem, Eigenfunctions, Nyström Method, and Use of Kernels in Machine Learning: Tutorial and Survey,” *arXiv preprint arXiv:2106.08443,* 2021. |