

Aprendizado de Máquina

Introdução

Felipe Augusto Lima Reis

felipe.reis@ifmg.edu.br



**INSTITUTO
FEDERAL**
Minas Gerais

Sumário

- 1 Introdução
- 2 Tipos de Aprendizado
- 3 Classificação x Regressão
- 4 Processo de Aprendizado
- 5 Aplicações

INTRODUÇÃO

Aprendizado de Máquina



“Aprendizado de Máquina, em Inteligência Artificial, é uma disciplina voltada para a implementação de softwares que possam aprender de forma autônoma [Hosch, 2020].”

Aprendizado

- Forma principal de aprendizado: **a partir de dados** [Marsland, 2014] [Shalev-Shwartz and Ben-David, 2014];
 - Dado é definido como qualquer informação prévia existente a respeito de um problema;
- O aprendizado humano pode ser interpretado como o aprendizado a partir de experiências [Marsland, 2014];
 - Como máquinas não são capazes de ter experiências, o aprendizado é possível devido aos dados a elas fornecidos.

Características de Aprendizado

- Segundo [Marsland, 2014], o aprendizado humano/animal pode ser subdividido em subpartes, dos quais destacam-se¹:
 - **Memória**: lembrar ocorrência de situações e ações adotadas;
 - Caso experiências tenham sido malsucedidas, novas ações podem ser tomadas;
 - **Adaptação**: capacidade de se adaptar a novas situações;
 - Novas experiências podem necessitar de novas ações, mais adequadas;
 - **Generalização**: reconhecer similaridade entre situações;
 - As ações previamente utilizadas em uma situação podem ser aplicadas a outras;
 - Dentre as características do aprendizado, a generalização é considerada a mais útil² [Marsland, 2014].

¹ Raciocínio e Dedução Lógica também fazem parte do aprendizado, porém não serão avaliados para Aprendizado de Máquinas.

² Ao menos para as tarefas de aprendizado de máquinas.

Superstição x Aprendizado

- Ao contrário de humanos, que podem utilizar do senso comum e de conhecimento extras para tomada de decisões, as máquinas não possuem tal capacidade;
 - Desse modo, algoritmos podem “aprender” e tirar conclusões sem sentido ou que possuam um viés;
 - Algumas informações podem ser úteis para um classificador, mas podem ser óbvias ou não possuir qualquer relação lógica;
 - Cabe, então, ao analista a definição dos limites do problema e a supervisão das conclusões geradas;
 - A definição de princípios que levem a conclusões assertivas é fundamental na teoria de Aprendizado de Máquinas [Shalev-Shwartz and Ben-David, 2014].

Quando utilizar Aprendizado de Máquinas

- Algoritmos de aprendizado devem ser utilizados quando [Shalev-Shwartz and Ben-David, 2014]:
 - A tarefa é muito complexa para ser programada;
 - Tarefas executadas por humanos, porém difíceis de serem explicadas - ex.: *identificar objetos, reconhecer padrões, etc.*;
 - Tarefas que superem as capacidades humanas - ex.: *análise de bancos de dados grandes e complexos, processamento de informações astronômicas, previsão climática, etc.*;
 - Tarefas que precisam se adaptar a diferentes situações;
 - Programas imperativos permanecem imutáveis e não são adequados a mudanças de cenários;
 - Algoritmos de aprendizado de máquina podem se adaptar a diferentes contextos.

TIPOS DE APRENDIZADO

Classificação quanto a Supervisão

● **Aprendizado supervisionado**

- O algoritmo aprende utilizando dados de treinamento pré-rotulados;
- O algoritmo de treinamento supervisiona a diferença entre as saídas em relação às respostas esperadas;

● **Aprendizado não supervisionado**

- O algoritmo aprende a partir de dados não rotulados;
- Útil em situações onde dados precisam ser classificados ou *clusterizados* em classes ainda indefinidas;

● **Aprendizado semi supervisionado**

- Intermediário entre o aprendizado supervisionado e o não supervisionado;
- São fornecidas informações incompletas para treinamento, cabendo ao *software* a decisão sobre o conteúdo não rotulado.

Classificação quanto a Supervisão

● Aprendizado por reforço

- Treinamento destinado à interação com ambientes dinâmicos, com objetivo de desempenhar uma ação;
- O algoritmo recebe uma recompensa (ou premiação), caso atinja o objetivo, ou uma punição, caso falhe;
- O objetivo é obter o maior valor de recompensa possível.

● Aprendizado evolucionário

- A evolução biológica é definida como processo de aprendizado;
- Utiliza-se o conceito de *fitness* (adaptação ao ambiente);
- Organismos mais adaptados sobrevivem, enquanto os menos adaptados perecem [Marsland, 2014].

Aprendizado Ativo x Passivo

- **Aprendizado ativo:** Aprendiz³ interage com o ambiente durante o treinamento, por meio de *queries* ou experimentos;
- **Aprendizado passivo:** Aprendiz apenas verifica as informações do ambiente (ou do professor), sem influenciá-la ou direcioná-la [Shalev-Shwartz and Ben-David, 2014].

³ Tradução literal da expressão *learner*, em inglês. Também pode ser traduzido como aluno.

Auxílio de um Professor

- Nesse tipo de aprendizado, é utilizado um “professor adversário”;
 - Esse “professor” tem como objetivo aumentar gradualmente o nível de dificuldade, tornando algoritmo mais robusto;
- Exemplo: Filtro de spam
 - Um “professor” pode ser utilizado para tentar enganar um filtro de spam;
 - Ao enganá-lo, é detectada uma limitação no algoritmo, que pode ser melhorada;
 - Espera-se que ao entrar em contato com um adversário mais fácil, o algoritmo tenha um bom desempenho (uma vez que está treinado) [Shalev-Shwartz and Ben-David, 2014].

Online x Batch

- **Online:** O algoritmo deve responder a situações ao longo do processo de aprendizado;
 - Ex.: um algoritmo de análise da bolsa de valores aprende ao longo do treinamento - a cada dia se torna mais eficiente;
- **Batch:** o algoritmo somente responderá a situações reais após ter processado grandes quantidades de dados;
 - Ex.: uma rede neural para identificação de objetos é treinada previamente, antes de começar a ser utilizada [Shalev-Shwartz and Ben-David, 2014].

CLASSIFICAÇÃO X REGRESSÃO

Aprendizado Supervisionado

- Algoritmos de regressão e classificação são utilizados principalmente com algoritmos supervisionados;
- Cada dado de treinamento consiste em um **valor de entrada** e um **rótulo** (*target*);
- Cada item possui um índice i , variando de 1 até N ;
- Valores de entrada são definidos, tradicionalmente, com a letra x , enquanto rótulos utilizam a letra y ⁴;
 - O i -ésimo dado de treino é definido como x_i ;
 - O i -ésimo rótulo de treino é definido como y_i ;
 - O conjunto de dados é definido como o par ordenado (x_i, y_i) [Marsland, 2014].

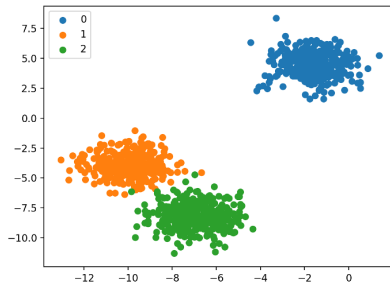
⁴[Marsland, 2014] utiliza a letra t para rótulos, enquanto [Shalev-Shwartz and Ben-David, 2014] utiliza a letra y .

Definição

- **Classificação**: rótulos t_i são definidos por uma quantidade limitada de valores discretos;
- **Regressão**: rótulos são definidos como valores contínuos.

Classificação

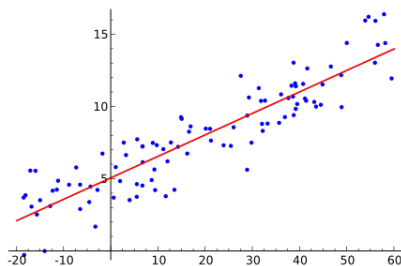
- O problema de **classificação** consiste em tomar um conjunto de elementos e decidir a qual das N classes eles pertencem;
 - A classificação é feita com base em um treinamento prévio;
- Problemas de classificação são discretos;
 - Cada elemento pertence somente a uma classe;
 - O conjunto de classes cobre todo o espaço de saídas possível.



Fonte: [Jason Brownlee - Machine Learning Mastery, 2020]

Regressão

- **Regressão** é um processo estatístico que busca ajustar uma função matemática para descrever uma curva;
 - O objetivo da regressão é que a curva/reta se aproxime o máximo possível de todos os pontos;
 - A regressão pode ser um problema de aproximação ou interpolação de funções [Marsland, 2014].



Fonte: [Wikipedia contributors, 2020]

PROCESSO DE APRENDIZADO

Processo de Aprendizado

- Segundo [Marsland, 2014], o processo de aprendizado pode ser subdividido nas seguintes etapas:
 - Coleta e preparação de dados;
 - Seleção de *features*;
 - Escolha do Algoritmo;
 - Seleção de Modelos e Parâmetros;
 - Treinamento;
 - Avaliação.

Coleta e preparação de dados

- Coleta de dados corresponde à obtenção de dados para o processo do qual se deseja aprender;
- Em alguns casos, é possível utilizar conjuntos de dados prontos, cujas informações foram previamente coletadas;
 - No entanto, em alguns cenários, é necessário produzir esse conjunto de dados;
- Após a coleta de dados, é necessária a preparação dos mesmos para produção de aprendizado;
 - Podem ser necessárias transformações, correções e ajustes nos dados;
 - Esses passos podem alterar o tipo dos dados, corrigir, ajustar ou descartar informações pouco fidedignas, erros significativos ou dados muito incompletos.

Seleção de *features*

- Objetiva-se identificar e selecionar as informações mais importantes no problema examinado;
 - A partir da seleção de *features* (características) é possível traçar hipóteses;
- São necessários conhecimentos acerca do problema e dos dados a ele relacionado;
 - Caso o problema não seja conhecido, dificilmente serão produzidas informações relevantes;
 - Caso informações pouco relevantes sejam selecionadas, o aprendizado poderá não produzir conhecimento útil;

Escolha do Algoritmo

- Após definição do conjunto de dados e entendimento do problema, podem ser definidos os algoritmos que serão utilizados;
 - A escolha do algoritmo deve ser feita a partir da análise de adequação ao problema e no conhecimento prévio a respeito das técnicas;
 - Apesar do item anterior parecer óbvio, muitas vezes o uso de ferramentas induz ao uso de um ou outro algoritmo;
 - Além disso, algoritmos “da moda” podem ser escolhidos, mesmo que não sejam adequados ao problema.

Seleção de Modelos e Parâmetros

- Algumas técnicas podem utilizar modelos pré-definidos para melhor desempenho;
 - Em redes neurais, por exemplo, é comum utilizar redes já conhecidas e treinadas, ao invés de criar novos modelos;
 - Diversas arquiteturas de rede foram propostas na literatura, com uso mais adequado a determinadas tarefas;
 - Ex.: Redes convolucionais são mais indicadas para o processamento de imagens e menos indicadas para extração de informações de bancos de dados;
- Mesmo após escolher modelos pré-definidos, são necessários, muitas vezes, ajustes de parâmetros para melhor desempenho.

Treinamento

- Corresponde à fase de uso de recursos computacionais para treinamento do modelo;
 - O treinamento pode levar muito tempo para ser realizado ou requerer recursos computacionais especiais, dependendo do algoritmo e do volume de informação;
- Após treinado, o sistema será capaz de prever adequadamente saídas para novas entradas de dados.

Avaliação



- Corresponde à avaliação do modelo treinado em um conjunto de dados diferente daquele em que houve o treinamento;
 - Essa fase é necessária para que o algoritmo consiga generalizar, não apenas decorar o conjunto de treinamento;
- Podem ser feitas comparações com especialistas humanos;
 - Essa comparação pode ser útil em modelos que desejam auxiliar ou substituir um especialista humano;
- A comparação deve ser feita utilizando métricas adequadas;
 - O uso de métricas inadequadas pode causar distorções;
 - A avaliação inadequada pode superestimar resultados.

APLICAÇÕES

Aplicações

- São exemplos de aplicações que podem utilizar Aprendizado de Máquinas [Data Science Academy, 2018]:
 - **Sistemas de recomendação**
 - Sistemas de recomendação podem ser utilizados para recomendar produtos para compra, filmes, vídeos e/ou jogos eletrônicos;
 - **Análise de crédito de clientes**
 - Instituições financeiras podem utilizar aprendizado de máquina para definir se um cliente terá ou não acesso a crédito, com base na faixa etária, faixa salarial, escolaridade, etc.;
 - **Filtragem de spam**
 - Serviços de e-mail podem utilizar informação de domínio, assunto e conteúdo do e-mail para classificar se uma mensagem é indesejada ou não;

Aplicações



- São aplicações de Aprendizado de Máquinas [cont.]:
 - Previsão de falha em equipamentos
 - Empresas podem utilizar informações históricas de equipamentos para aprender quando substituir peças ou realizar manutenções, mesmo que a recomendação do fabricante seja diferente;
 - Detecção de fraudes
 - Bancos e serviços de cartão de crédito podem utilizar aprendizado de máquina para identificar e negar transações que possam ser fraudulentas;
 - Refinamento de mecanismos de busca
 - Máquinas de busca podem utilizar aprendizado de máquina para fornecer resultados mais próximos ao desejo de um grupo de usuários ou a uma determinada região;

Aplicações



- São aplicações de Aprendizado de Máquinas [cont.]:
 - **Processamento de linguagem natural**
 - Assistentes pessoais, como Siri, Cortana, Alexa, Google Now, etc., podem entender solicitações, a fim de retornar informações ou executar ações para os usuários;
 - **Detecção de anomalias**
 - Sistemas de aprendizado de máquinas podem identificar processos anômalos, resultando em itens defeituosos. Inspeção visual humana de produtos podem ser substituídas por inspeções computadorizadas;
 - **Previsão de demanda**
 - Sistemas podem utilizar dados históricos para prever demanda por produtos e/ou serviços. Podem ainda detectar aumento da demanda e elevar/reduzir preços automaticamente;

Aplicações

- São aplicações de Aprendizado de Máquinas [cont.]:
 - **Segurança em TI**
 - Sistemas inteligentes podem ser utilizados para identificar comportamentos “normais” e potenciais ataques *hackers* a servidores;
 - **Operação no mercado financeiro**
 - Sistemas inteligentes podem aprender a operar ativos financeiros, incluindo ações, moedas e contratos, de forma automática, com base em informações históricas, de modo a sugerir ou realizar compra e venda de ativos.
 - **Chat bots**
 - Agentes automáticos podem responder a perguntas, analisar solicitações, tirar dúvidas e abrir requisições para os clientes, melhorando o atendimento;

Referências I



Data Science Academy (2018).

17 casos de uso de machine learning.

Disponível em <http://datascienceacademy.com.br/blog/17-casos-de-uso-de-machine-learning/>.



Hosch, W. L. (2020).

Machine learning - Encyclopedia Britannica.

Disponível em: <https://www.britannica.com/technology/machine-learning>.



Jason Brownlee - Machine Learning Mastery (2020).

4 types of classification tasks in machine learning.

Disponível em <https://machinelearningmastery.com/types-of-classification-in-machine-learning>.



Kopec, D. (2019).

Classic Computer Science Problems in Python.

Manning Publications Co, 1 edition.



Marsland, S. (2014).

Machine Learning: An Algorithm Perspective.

CRC Press, 2 edition.

Disponível em: <https://homepages.ecs.vuw.ac.nz/~marslast/MLbook.html>.



Richert, W. and Coelho, L. P. (2013).

Building Machine Learning Systems with Python.

Packt Publishing Ltd., 1 edition.

Referências II



Shalev-Shwartz, S. and Ben-David, S. (2014).

Understanding Machine Learning: From Theory to Algorithms.

Cambridge University Press, 1 edition.

Disponível em: <http://www.cs.huji.ac.il/~shais/UnderstandingMachineLearning>.



Wikipedia contributors (2020).

Regression analysis.

Disponível em https://en.wikipedia.org/wiki/Regression_analysis.