**Introdução**

Aprendizado de máquina é a extração de conhecimento a partir de dados. É um campo de pesquisa localizado na interseção da estatística, da inteligência artificial e da ciência da computação. A aplicação do aprendizado de máquina atualmente é onipresente nas nossas vidas. Exemplos:

* Recomendações de filmes
* Recomendações de comida
* Recomendações de produtos
* Reconhecimento facial em fotos

Além das aplicações comerciais, o aprendizado de máquina tem sido muito utilizado nas ciências para:

* Entender as estrelas
* Encontrar planetas distantes
* Descobrir novas partículas
* Analisar sequências de DNA
* Fornecer tratamentos personalizados de câncer

**Por que usar aprendizado de máquina?**

No início da utilização das aplicações inteligentes, os sistemas utilizavam regras de decisão “if” e “else” programadas à mão para processar dados como, por exemplo, os filtros de spam. Bastava adicionar palavras indesejadas ao filtro para que este automaticamente identificasse e-mails que continham tais palavras como spam. Desenvolver regras de decisão manualmente é factível para determinadas aplicações, particularmente aquelas nas quais os humanos possuem um bom entendimento do processo a ser modelado. Contudo, usar regras de decisão programadas à mão apresenta duas grandes desvantagens:

1. A lógica requerida para fazer uma decisão é específica para uma única tarefa. Qualquer alteração mínima nesta tarefa pode exigir que todo o modelo seja reprogramado.
2. Desenhar regras de decisão requer um conhecimento profundo de como uma decisão deve ser tomada.

Um exemplo no qual a abordagem de regras de decisão programas por humanos falha é no reconhecimento facial por imagens. O problema do reconhecimento facial só foi resolvido em 2001. A questão principal é que a maneira como os pixels que compõem as imagens são percebidos pelo computador é totalmente diferente da maneira como os humanos os percebem. Esta diferença torna praticamente impossível que um humano desenvolva e programe uma série de regras para descrever o que constitui um rosto em uma imagem digital.

Contudo, ao usarmos aprendizado de máquina, apresentar um grande conjunto de imagens digitais contendo o rosto de pessoas é o suficiente para que o algoritmo de aprendizado de máquina determine quais são as características necessárias para identificar um rosto.

**Problemas que o aprendizado de máquina pode solucionar**

Os algoritmos mais bem sucedidos de aprendizado de máquina são aqueles que automatizam o processo de tomada de decisão generalizando a partir de exemplos conhecidos. Neste tipo de algoritmo, conhecido como aprendizado supervisionado, o usuário fornece pares de inputs e outputs desejados, e o algoritmo encontra uma maneira de produzir o output esperado dado o input fornecido. Em particular, o algoritmo é capaz de criar um output para um input nunca visto antes sem qualquer ajuda humana. No exemplo do filtro de spam, usando aprendizado de máquina, o usuário fornece ao algoritmo um grande número de e-mails, os inputs, junto com a informação que determina se um e-mail é spam ou não, os outputs desejados. Assim, quando um novo e-mail é recebido, o algoritmo, com base nos dados fornecidos, automaticamente o classifica como spam ou não spam.

Os algoritmos de aprendizado de máquina que aprendem a partir de pares de inputs e outputs são chamados de algoritmos de aprendizado supervisionado porque o usuário ensina o algoritmo os outputs desejados para cada exemplo de input fornecido. Apesar de ser trabalhoso criar uma base de dados para fornecer para o algoritmo, os algoritmos de aprendizado supervisionado são fáceis de entender e a sua performance é fácil de ser medida.

**Exemplos de tarefas de aprendizado de máquina supervisionado**

* **Identificar o CEP com dígitos escritos à mão em um envelope**

Neste caso, os inputs são uma digitalização dos dígitos do CEP escrito à mão e os outputs são os dígitos do CEP de fato. A base de dados é construída a partir de um grande número de digitalizações de envelopes e seus respectivos CEPs. Uma vez fornecida a base, o algoritmo será capaz de digitalizar os envelopes e automaticamente informar o CEP para o sistema.

* **Determinar se um tumor é maligno ou benigno com base em um exame médico de imagem**

Neste caso, os inputs são as imagens e os outputs são as classificações “maligno” e “benigno”. A base de dados é construída a partir de um grande número de imagens e suas respectivas classificações, fornecidas por médicos especialistas após a avaliação de cada exame de imagem.

* **Detectar atividade fraudulenta em transações de cartão de crédito**

Neste caso, os inputs são os históricos de transações dos cartões de crédito e os outputs são as probabilidades da transação ser fraudulenta ou não. A base de dados é criada pela empresa fornecedora do cartão de crédito com base no histórico de cada cartão e as denúncias de transações fraudulentas de cada usuário.

Um ponto importante a ser destacado nestes exemplos é a grande diferença entre as maneiras de como os dados são obtidos em cada caso. Enquanto nos casos de identificação do CEP e de detecção de atividade fraudulenta em transações de cartão de crédito os dados são obtidos de maneiras relativamente fáceis e baratas, no caso da classificação de um tumor como maligno ou benigno o processo é muito caro, complexo e exige profissionais altamente especializados.

O outro tipo de algoritmo são os algoritmos de aprendizado não supervisionado. Neste tipo de algoritmo, apenas os inputs são conhecidos e nenhum output é fornecido para o algoritmo. Apesar de existirem muitas aplicações para estes algoritmos, eles são mais difíceis de entender e de serem avaliados.

**Exemplos de tarefas de aprendizado de máquina não supervisionado**

* **Identificar tópicos em um conjunto de publicações de um blog**

Neste caso, o input é um conjunto de dados de texto e não há output. O algoritmo é capaz de identificar e resumir os temas abordados neste conjunto de dados, ou seja, a partir do input o algoritmo fornece o output.

* **Segmentar os consumidores em grupos com preferências similares**

Neste caso, os inputs são os históricos de compras dos consumidores e não há output. O algoritmo identifica e agrupa os consumidores em grupos com preferências similares com base nos seus históricos de compras.

* **Detectar padrões anormais de acesso a um website**

Neste caso, o input é o tráfego de acesso dos usuários de um website. O algoritmo identifica padrões de acessos muito diferentes do normal a partir do tráfego de inúmeros usuários.