

- 
- 
- 
- 
- 

# Fundamentos de Aprendizagem de Máquina

Aluizio Fausto Ribeiro Araújo  
Universidade Federal de Pernambuco  
Centro de Informática

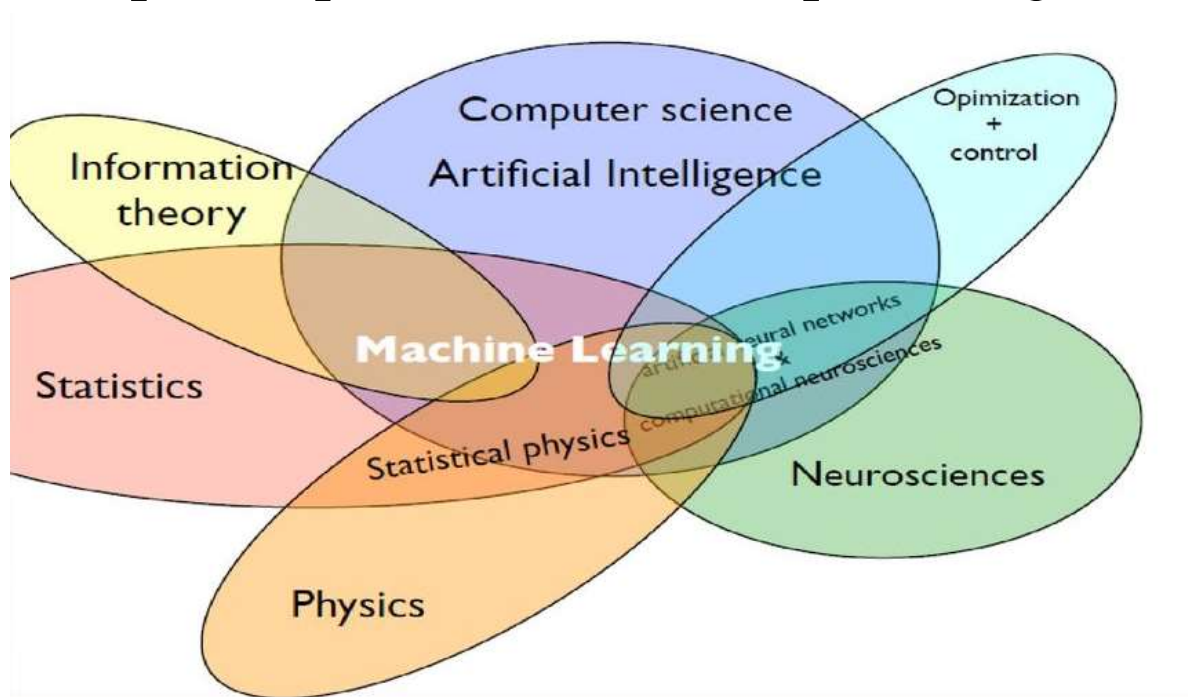


# Conteúdo

- Definição de aprendizagem de máquina
- Aprendizagem e métodos de inferência
  - Raciocínio científico
  - Aprendizagens supervisionada, não-supervisionada e por reforço
  - Aprendizagem semi-supervisionada e aprendizagem ativa
  - Outros métodos de aprendizagem
- Aprendizagem e generalização
  - Erro de generalização
  - Generalização por critério de parada
  - Generalização por regularização
  - Descarte (*Dropout*)
  - Tolerância a falhas e generalização
  - Esparsidade X estabilidade

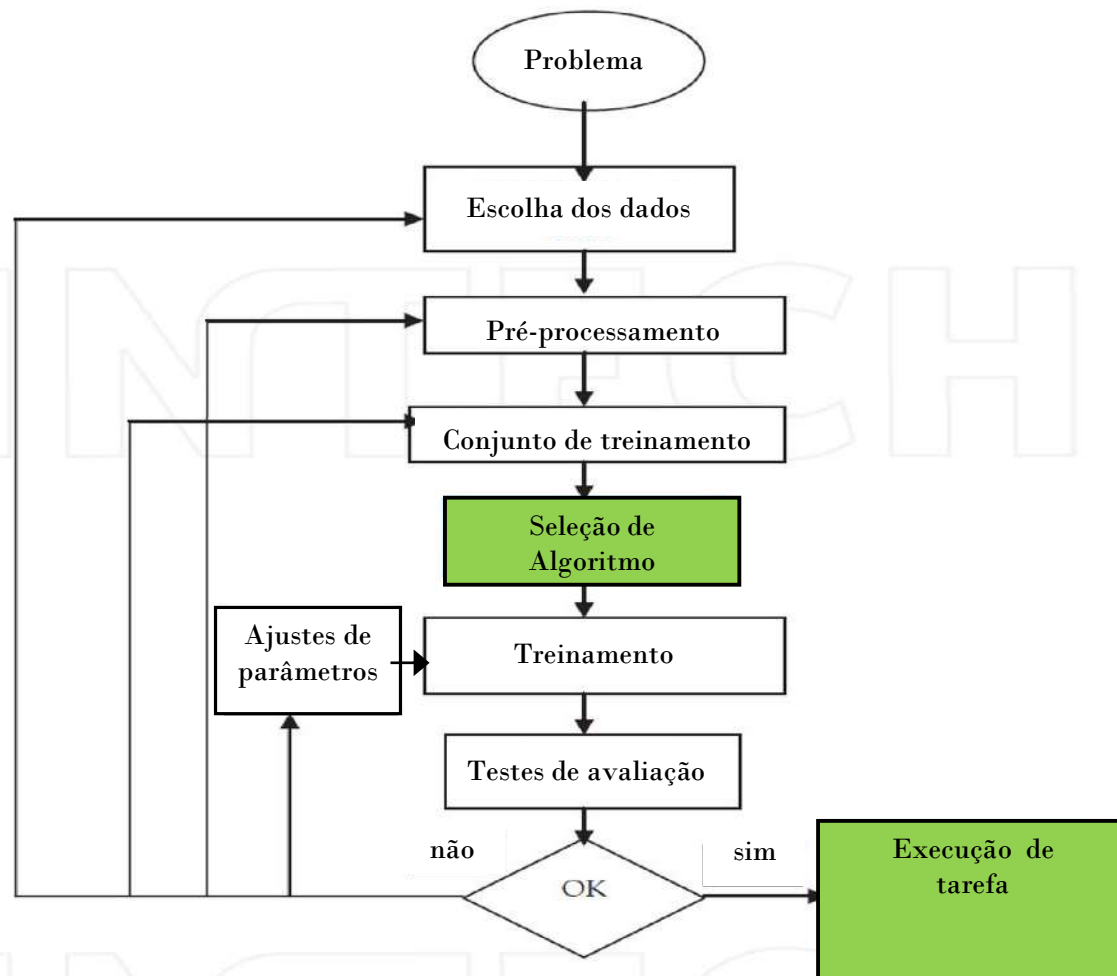
# Aprendizagem de Máquina

- Aprendizagem de máquina usa diferentes áreas de conhecimento para criar sistemas de aprendizagem que extraem conhecimento de dados para inferir, decidir ou prever sem usar intervenção humana;
- Algumas disciplinas que fundamentam aprendizagem de máquina:



# Aprendizagem de Máquina

- Esquema geral de algoritmo de aprendizagem de máquina:



# Aprendizagem de Máquina

- Arthur Samuel (1959): Aprendizagem de Máquina é o campo de estudo que dá aos computadores a capacidade de aprender sem serem explicitamente programados com o conhecimento,
  - O objetivo é construir sistemas para computadores que possam se adaptar e aprender com sua experiência;
- Tom M. Mitchell (1997): Diz-se que um programa de computador aprende com a experiência  $E$  com relação a alguma classe de tarefas  $T$  e medida de desempenho  $P$ , se seu desempenho em tarefas em  $T$ , quando medido por  $P$ , melhora com a experiência  $E$ ;

# Aprendizagem de Máquina

- Exemplos de tarefas que são bem-sucedidas quando tratadas com algoritmos de aprendizagem:
  - Reconhecimento de padrões:
    - Identidades faciais ou expressões faciais;
    - Palavras manuscritas ou faladas;
    - Imagens médicas;
  - Geração de padrões:
    - Geração de imagens ou sequências de movimento;
  - Reconhecimento de anomalias:
    - Transações incomuns com cartão de crédito;
    - Padrões incomuns de leituras de sensores em uma usina nuclear;
  - Predição:
    - Preços futuros de ações ou taxas de câmbio.

# Aprendizagem de Máquina

- Aprendizagem de máquina possui duas grandes classes: aprendizagem indutiva e aprendizagem transdutiva:
  - Aprendizagem indutiva visa categorizar todo um espaço de entrada:
    - A inferência indutiva estima a função do modelo considerando a relação dos dados com todo o espaço de hipóteses e usa esse modelo para prever valores de saída para exemplos além do conjunto de treinamento;
  - Aprendizagem transdutiva visa rotular um conjunto-alvo de dados não previamente rotulados:
    - Esta aprendizagem, também chamada de inferência transdutiva, busca prever funções exclusivas do modelo para testes específicos usando observações adicionais no conjunto de dados de treinamento relacionadas a novos casos;
  - Aprendizagem indutiva generaliza a partir de casos observados, enquanto aprendizagem transdutiva faz previsões específicas de casos observados.

# Aprendizagem de Máquina

## Raciocínio Científico

- O raciocínio científico é expresso como dedução, indução e abdução;
  - A dedução é necessariamente verdadeira, a indução plausivelmente verdadeira e a abdução hipoteticamente verdadeira;
- O raciocínio dedutivo considera uma causa para dedução da consequência ou dos efeitos (fechamento transitivo),
  - Examina-se as premissas e o resultado é uma verdade necessária;
- O raciocínio indutivo deduz possíveis causas partindo de uma consequência (utiliza generalização),
  - A conclusão pode não ser necessariamente ou plausivelmente verdadeira;
- O raciocínio abduativo estabelece conclusão a partir de uma regra e de um resultado (verificação experimental),
  - A conclusão é hipoteticamente plausível.



# Aprendizagem de Máquina

## Raciocínio Científico

- Raciocínio dedutivo

- No raciocínio dedutivo (*top-down*), uma conclusão é obtida de forma redutiva através da aplicação de regras gerais válidas para a totalidade de um domínio fechado, estreitando seguidamente o intervalo em consideração até que restem apenas a(s) conclusão(ões).
- A lei do desapego, também conhecida como afirmação do antecedente e *modus ponens* (latim para “o caminho que afirma afirmando”), é a primeira forma de raciocínio dedutivo. Na lógica proposicional, o *modus ponens* ou eliminação de implicações é uma regra de inferência. Pode ser resumido como “P implica Q ( $P \rightarrow Q$ )” e “se P for afirmado como verdadeiro (P), então Q deve ser verdadeiro (Q)”.

# Aprendizagem de Máquina

## Raciocínio Científico

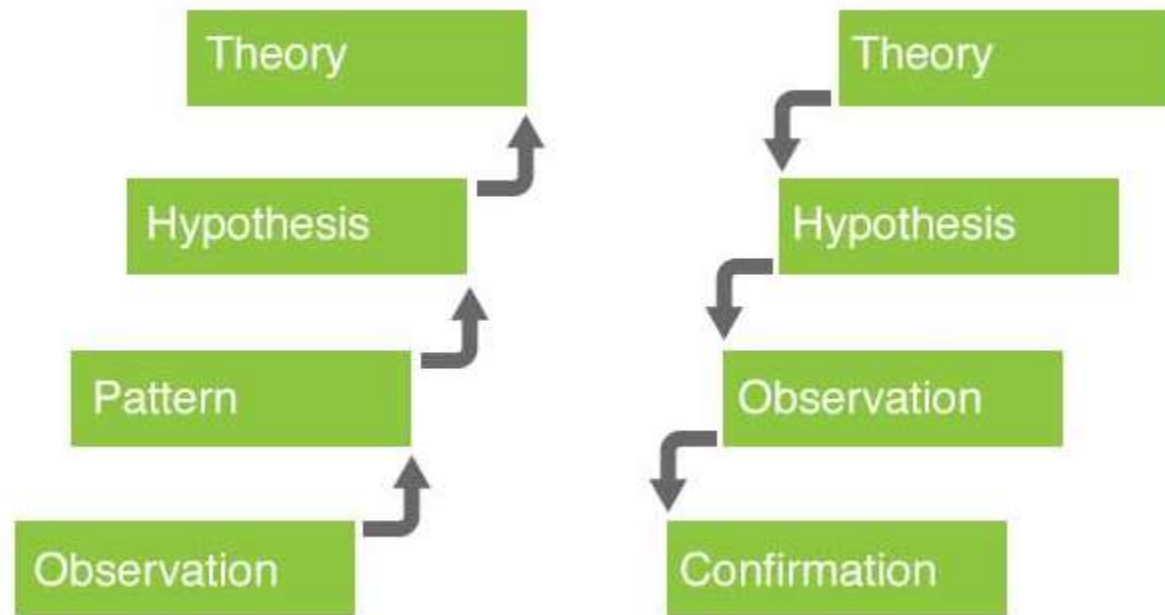
- Raciocínio indutivo

- No raciocínio indutivo (*bottom-up*), uma conclusão é obtida por generalização ou extrapolação de casos específicos para regras gerais, portanto, há incerteza epistemológica;
- Aprendizagem indutiva é uma classe especial de técnicas supervisionadas de aprendizagem, onde dado um conjunto de pares estímulo-resposta  $\{\mathbf{x}_i, f(\mathbf{x}_i)\}$ , determina-se uma hipótese  $h(\mathbf{x}_i)$  tal que  $h(\mathbf{x}_i) \approx f(\mathbf{x}_i), \forall i$ ;
- Na aprendizagem indutiva, deve-se formar um conceito que suporte a maioria dos vários exemplos positivos, mas nenhum negativo;
- Esta aprendizagem demanda uma série de instâncias de treinamento para formar um conceito de aprendizagem indutiva.

# Aprendizagem de Máquina

## Raciocínio Científico

- Raciocínio indutivo X dedutivo



# Aprendizagem de Máquina

## Raciocínio Científico

- Raciocínio Abduativo
- No raciocínio abduativo, parte-se de uma observação e depois procura-se a explicação mais simples e provável adotando provisoriamente uma hipótese, todas as consequências possíveis da hipótese podem ser verificadas experimentalmente;
- No raciocínio abduativo, as premissas não garantem a conclusão pois ele pode ser visto como uma inferência para a melhor explicação;

# Aprendizagem de Máquina

## Tipos de Aprendizagem

- Tipos mais comuns de aprendizagem:
  - Métodos historicamente relevantes como aprendizagem supervisionada (AS), não-supervisionada (ANs) e por reforço (AR);
  - Do ponto de vista estatístico, dados pares entrada saída ( $\mathbf{x}$ ,  $\mathbf{y}$ ):
    - Aprendizagem não-supervisionada aprende a função de distribuição de probabilidade (pdf) de um conjunto de treinamento,  $p(\mathbf{x})$ ;
    - Aprendizagem supervisionada aprende a pdf de  $p(\mathbf{y}|\mathbf{x})$ ;
  - No que diz respeito às utilizações típicas das aprendizagens:
    - AS é largamente usada em classificação, aproximação, controle, modelagem e identificação, processamento de sinais e otimização;
    - ANS é comumente empregada para agrupamento, quantização vetorial, extração de características, codificação de sinal e análise de dados;
    - AR é geralmente usado em controle e inteligência artificial.

# Aprendizagem de Máquina

## Tipos de Aprendizagem

- Alguns usos dos tipos de aprendizagem mais comuns:

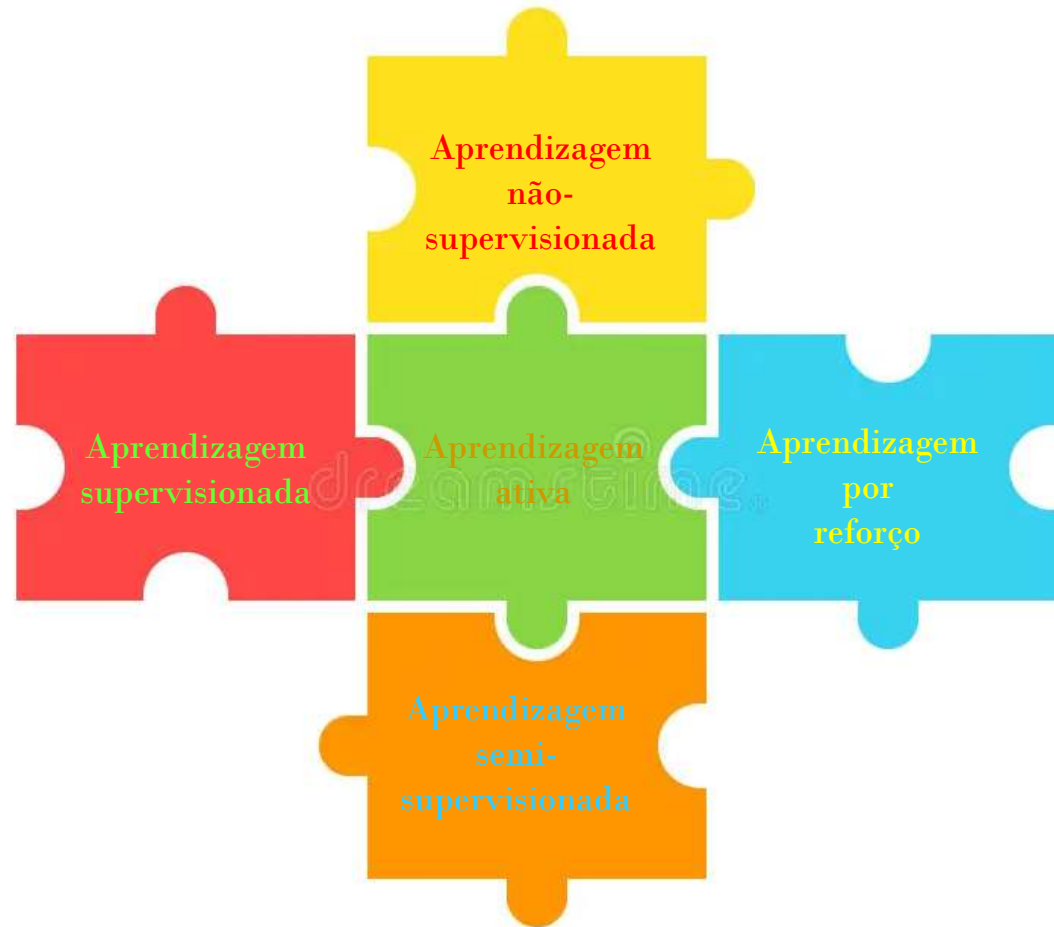


# Aprendizagem de Máquina

## Tipos de Aprendizagem

- Tipos de aprendizagens mais comuns (visão atual):

- Supervisionada: Todos os dados são rotulados;
- Não-supervisionada: Não há dados rotulados;
- Reforço: Há retorno do meio-ambiente;
- Semi-supervisionada: Dados rotulados (poucos) e sem rótulos (muitos);
- Ativa: Reduz número de dados rotulados, privilegiando dados com mais informação;

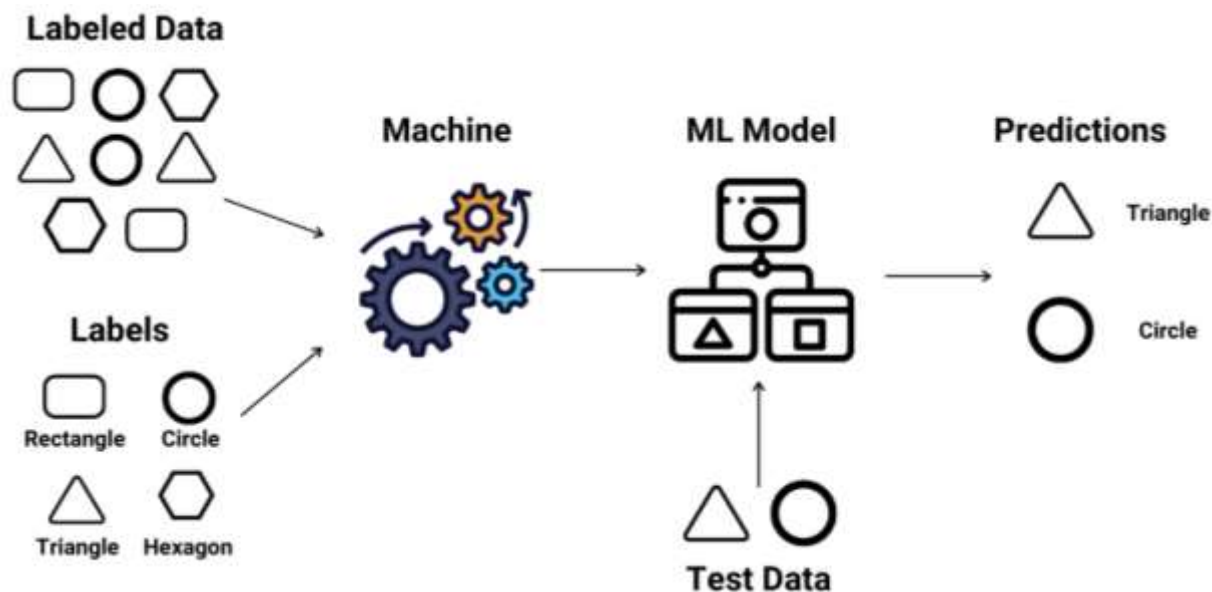




# Aprendizagem de Máquina

## Tipos de Aprendizagem: Supervisionada

- Esta aprendizagem ajusta os parâmetros do modelo de aprendizagem por comparação direta da saída do modelo com a saída desejada,
  - A medida de erro, diferença entre a saída obtida e aquela desejada para as amostras de treinamento, é usada para orientar a aprendizagem;



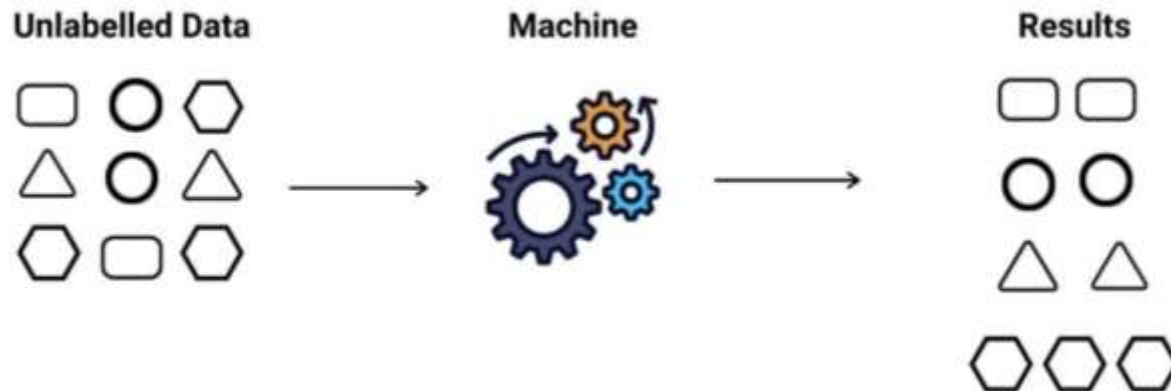
– Fonte: <https://www.enjoyalgorithms.com/blogs/supervised-unsupervised-and-semisupervised-learning>



# Aprendizagem de Máquina

## Tipos de Aprendizagem: Não-supervisionada

- Esta aprendizagem não usa saídas desejadas, baseando-se apenas nas correlações dos dados de entrada, logo, determina compartilhamento de características significativas sem a participação de um professor,
  - ANS é comumente um tipo de aprendizagem hebbiana, que usa relações locais envolvendo dois neurônios e uma sinapse: A mudança de peso sináptico é proporcional à correlação entre os sinais pré e pós-sinápticos.

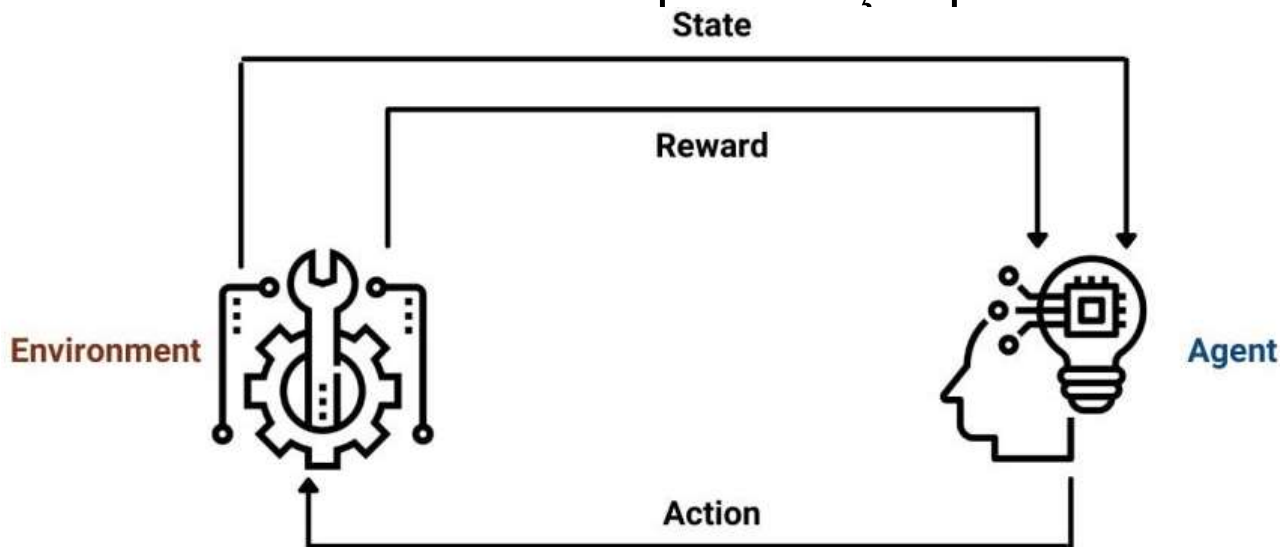


– Fonte: <https://www.enjoyalgorithms.com/blogs/supervised-unsupervised-and-semisupervised-learning>

# Aprendizagem de Máquina

## Tipos de Aprendizagem: por Reforço

- Esta aprendizagem especifica como um agente aprende a selecionar ações para maximizar uma recompensa cumulativa, esse caso especial de AS utiliza sinais de retorno indicativos da qualidade da saída,
  - O sinal de reforço consiste em um retorno avaliando o sucesso ou fracasso de uma dada saída, isto é, há recompensa para o modelo em caso de bom resultado de saída e penalização para mau resultado.

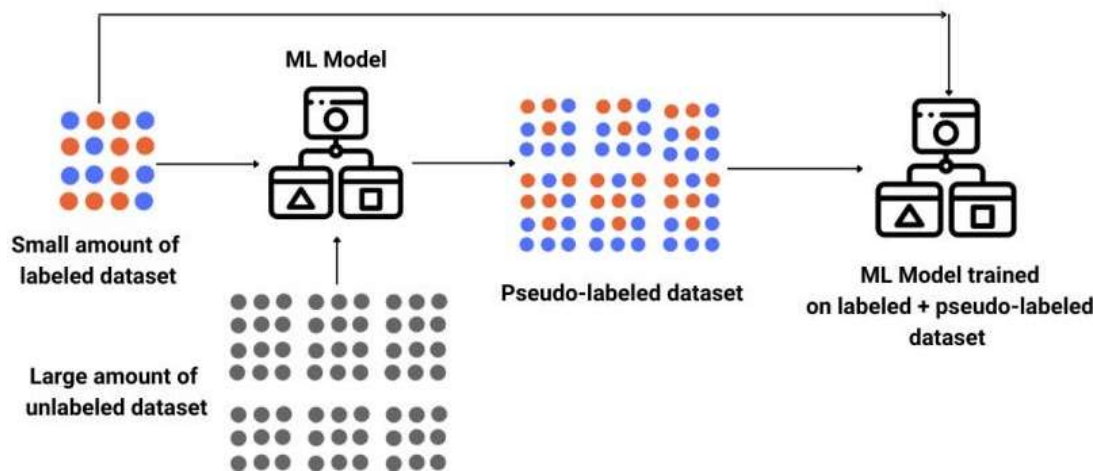


Fonte: <https://www.enjoyalgorithms.com/blogs/supervised-unsupervised-and-semisupervised-learning>

# Aprendizagem de Máquina

## Tipos de Aprendizagem: Semi-supervisionada

- O objetivo desta aprendizagem é utilizar uma grande coleção de dados não rotulados juntamente com alguns exemplos rotulados para melhorar a capacidade de generalização,
  - Abordagens típicas: aprender com hipótese de grupo ou com hipótese de variedade (*manifold*), em ambas dados dentro de um grupo ou em uma variedade têm maior probabilidade de ter o mesmo rótulo;

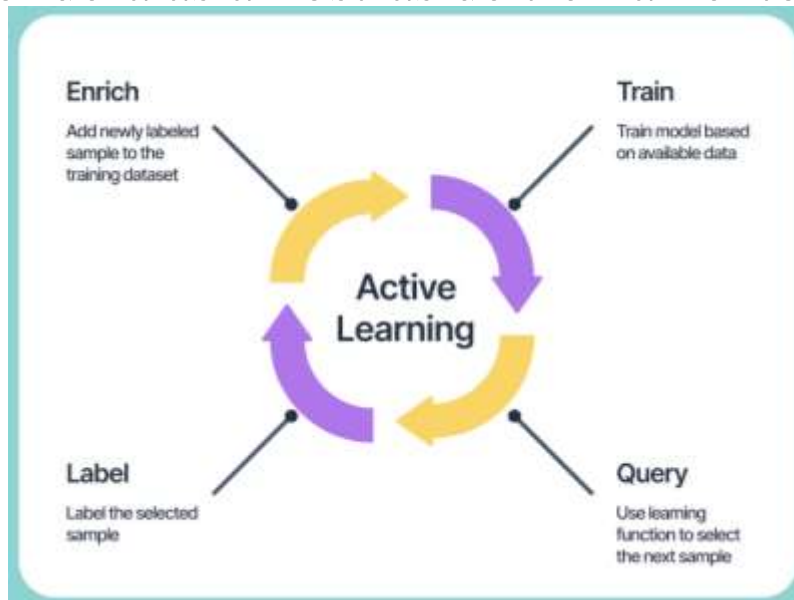


– Fonte: <https://www.enjoyalgorithms.com/blogs/supervised-unsupervised-and-semisupervised-learning>

# Aprendizagem de Máquina

## Tipos de Aprendizagem: Ativa

- O objetivo da aprendizagem ativa (AA) é escolher ativamente os exemplos mais informativos para rotulagem manual na aprendizagem, ou seja, estabelecer sinais de entrada para generalização ótima,
  - Com base na expectativa condicional do erro de generalização, a AA pondera as amostras de treinamento de acordo com sua importância;

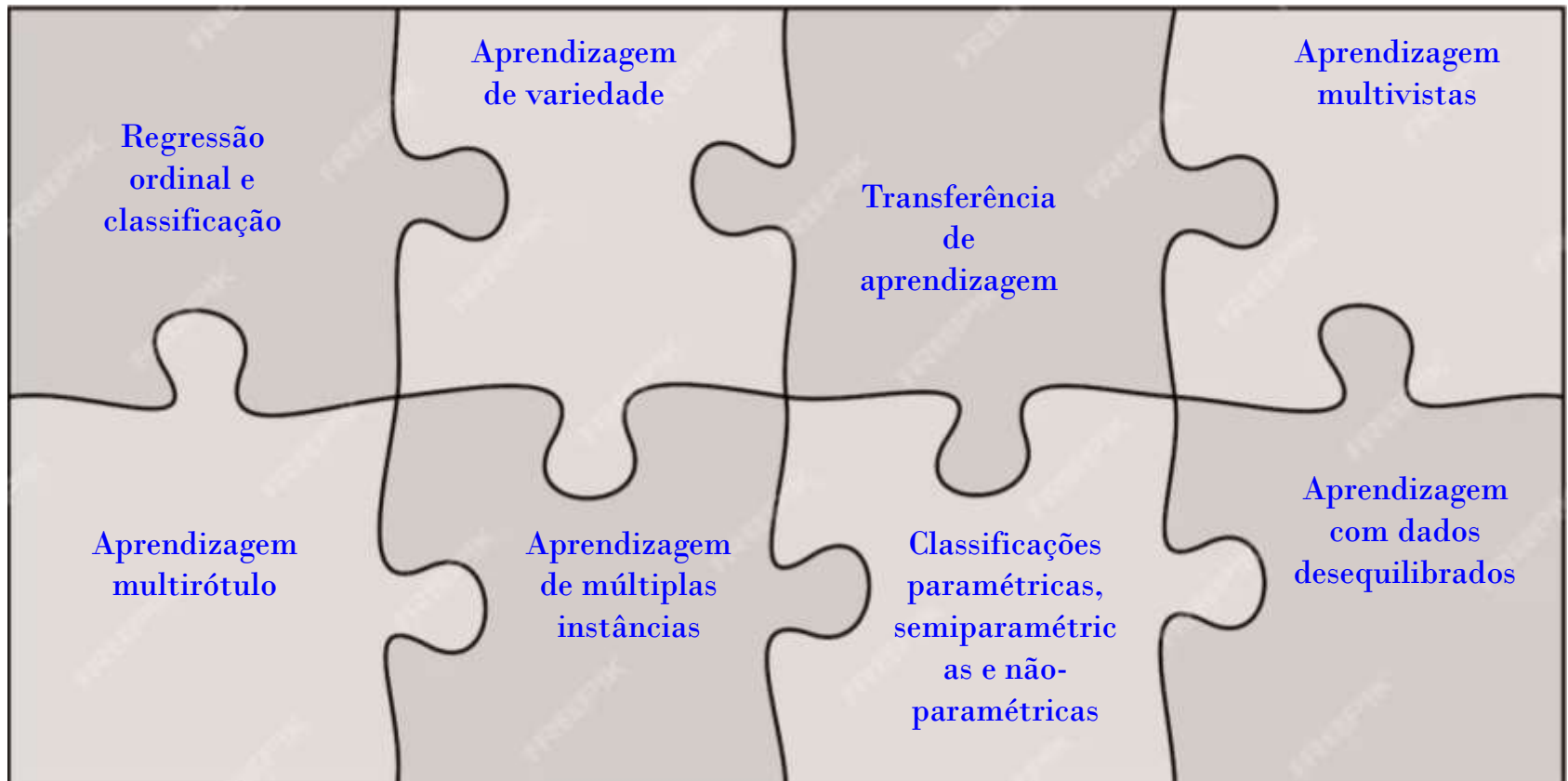


– Fonte: <https://www.v7labs.com/blog/active-learning-guide>

# Aprendizagem de Máquina

## Tipos de Aprendizagem

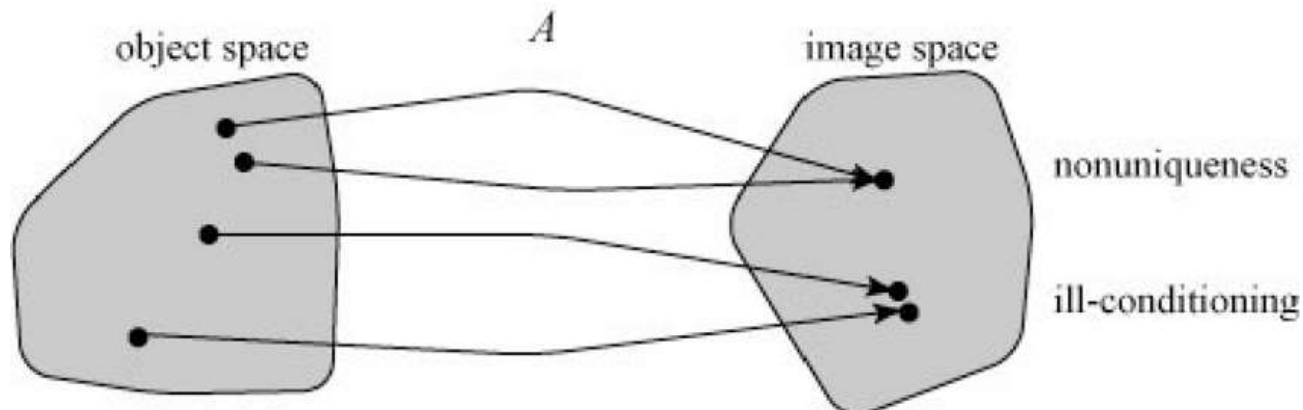
- Alguns outros tipos:



# Aprendizagem de Máquina

## Aprendizagem e Generalização

- Sob o ponto de vista da aproximação, aprendizagem é reconstruir uma hipersuperfície baseada em exemplos e generalização diz respeito a estimar o valor na hipersuperfície de uma entrada não treinada,
  - Matematicamente, aprendizagem é um ajuste não-linear de curva e a generalização é a interpolação e extrapolação de dados de entrada;
- A aprendizagem é um problema inverso mal-posto pois os dados de entrada podem ser ruidosos ou imprecisos e também podem ser insuficientes para construir o mapeamento de maneira exclusiva;

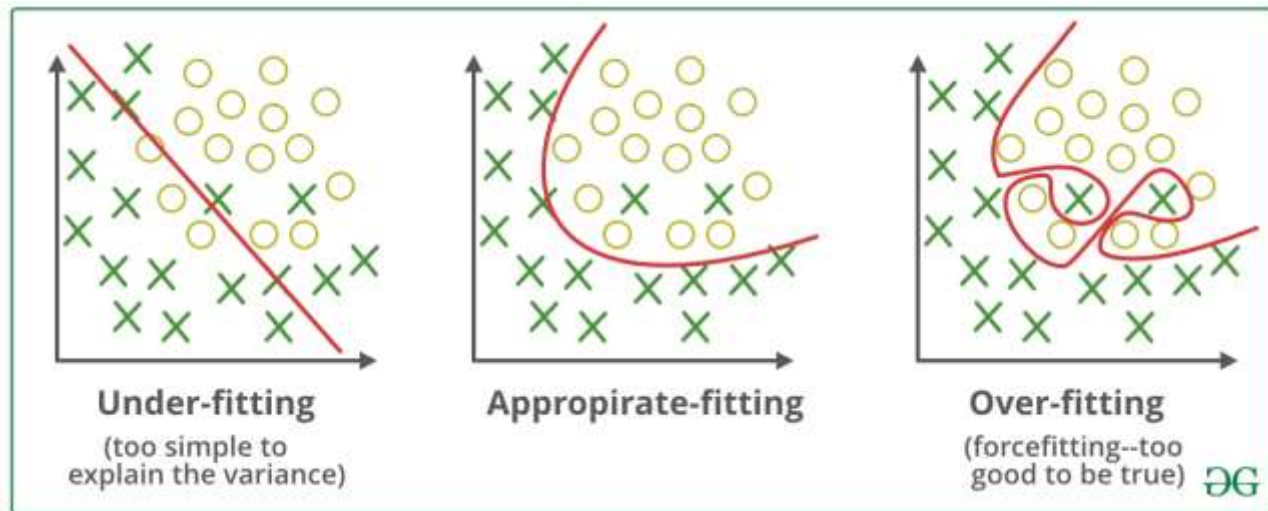




# Aprendizagem de Máquina

## Aprendizagem e Generalização

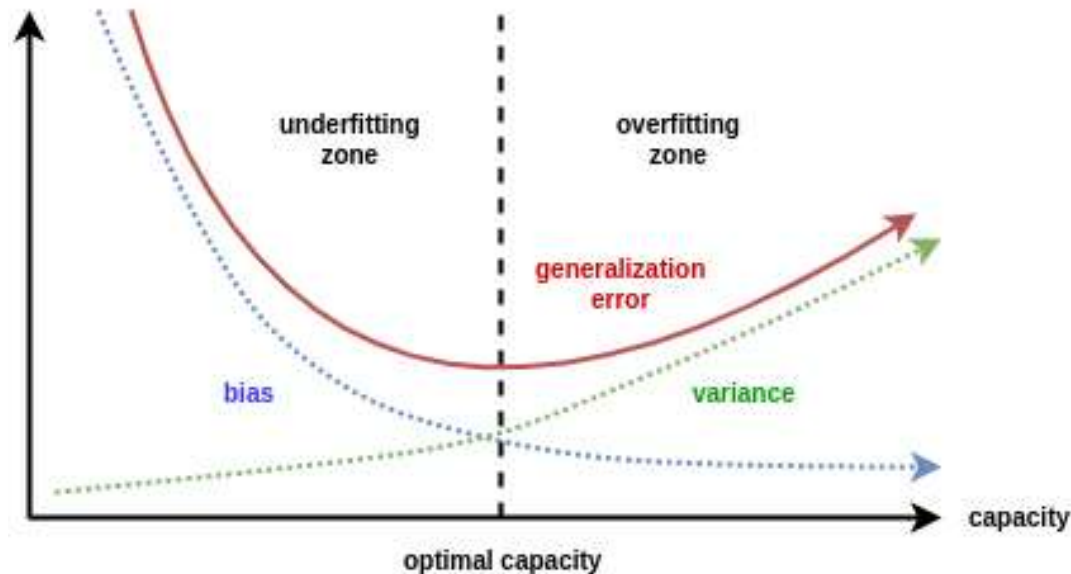
- Sobreajuste: Um algoritmo de aprendizagem é sobretreinado com muitos exemplos, parâmetros ou épocas, logo, ele pode ser acurado para dados de treinamento, mas impreciso para dados de teste,
  - O conjunto de treinamento deve ser suficientemente grande e diversificado para representar bem o problema;



# Aprendizagem de Máquina

## Avaliando Capacidade de Generalização

- Erro de generalização de uma rede neural tipicamente composto por:
  - Erro de aproximação devido a número finito de parâmetros do esquema de aproximação usado e a ruído desconhecido nos dados de treinamento;
  - Erro de estimação devido a um número finito de dados disponíveis;



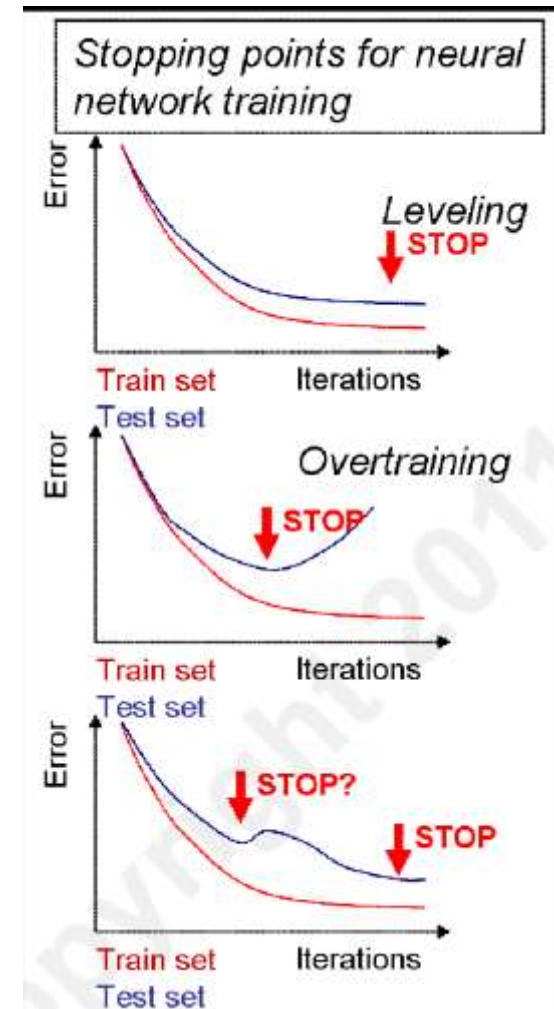


# Aprendizagem de Máquina

## Avaliando Capacidade de Generalização

- Critério de parada pode evitar o sobretreinamento, interrompendo o treinamento antes que o mínimo erro absoluto seja atingido, se o treinamento de uma rede neural for interrompido em um ponto apropriado, a rede não aprenderá o ruído de alta frequência,

- O erro de treinamento tende a diminuir até seu mínimo enquanto o erro de generalização deve atingir seu mínimo antes e depois passa a crescer;
- O erro de generalização é definido da mesma forma que o erro de aprendizagem, só que para um conjunto de dados de validação;



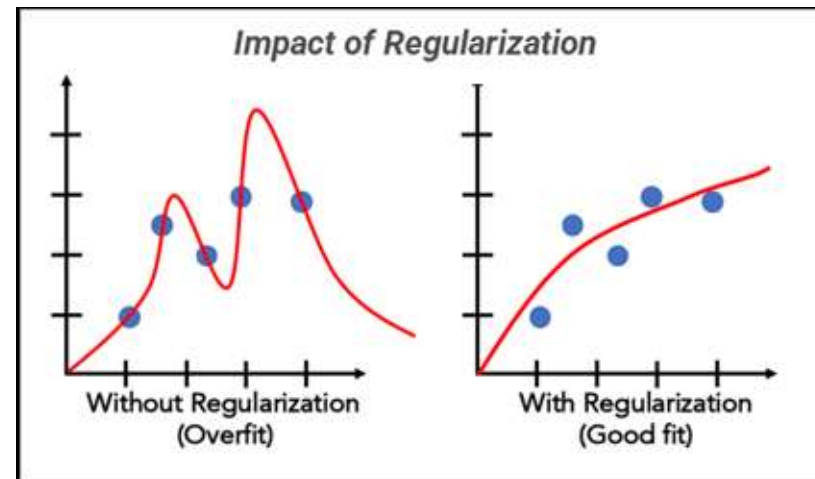
# Aprendizagem de Máquina

## Avaliando Capacidade de Generalização

- Generalização por regularização emprega um termo de restrição ( $E_C$ ) que penaliza a complexidade (causa de generalização baixa) de uma solução, tornando a função de custo:

$$- E_T = E_A + \lambda E_C ;$$

- Equacionamento de regularização L1 e L2:



L1 Regularization

$$\text{Cost} = \sum_{i=0}^N (y_i - \sum_{j=0}^M x_{ij} W_j)^2 + \lambda \sum_{j=0}^M |W_j|$$

L2 Regularization

$$\text{Cost} = \sum_{i=0}^N (y_i - \sum_{j=0}^M x_{ij} W_j)^2 + \lambda \sum_{j=0}^M W_j^2$$

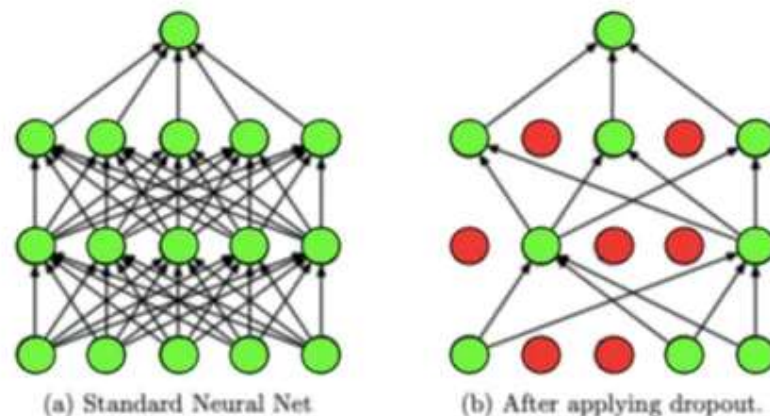
Loss function

Regularization Term

# Aprendizagem de Máquina

## Avaliando Capacidade de Generalização

- Descarte (*dropout*) descarta aleatoriamente nodos e suas conexões no treinamento de uma rede neural (RN) para interromper co-adaptações frágeis, como no MLP-BP, que não generalizam para dados de testes,
  - No caso mais simples, cada nodo é mantido com probabilidade fixa  $p$  independente das outras unidades;
  - A eliminação de 20% das unidades de entrada e 50% das unidades escondidas é frequentemente considerada adequada.



# Aprendizagem de Máquina

## Avaliando Capacidade de Generalização

- A tolerância a falhas nos pesos ou nodos é importante para uma RN,
  - No treinamento, ruído na entrada melhora a capacidade de generalização e o ruído sináptico melhora a tolerância a falhas;
    - Quando a tolerância a falhas é melhorada, a capacidade de generalização geralmente é melhorada e vice-versa;
    - Quanto menor a magnitude do peso, maior a tolerância a falhas;
- Esparsidade e estabilidade são as duas propriedades conflitantes dos algoritmos de aprendizagem que colaboram na capacidade de generalização: um algoritmo esparsos não pode ser estável e vice-versa,
  - Um dado algoritmo de aprendizagem precisa equilibrar esparsidade e estabilidade.

# Tarefas de Aprendizagem

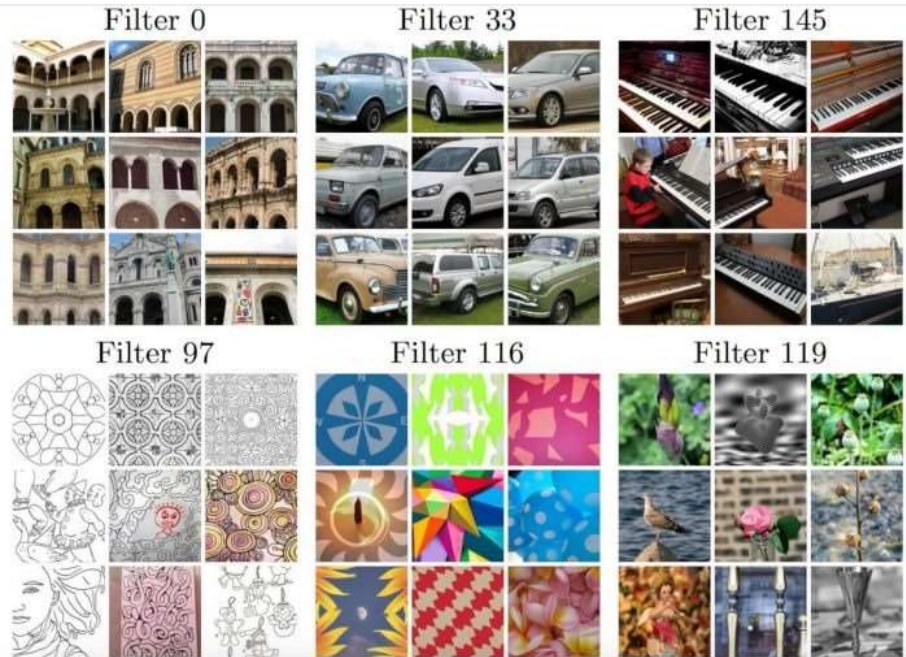
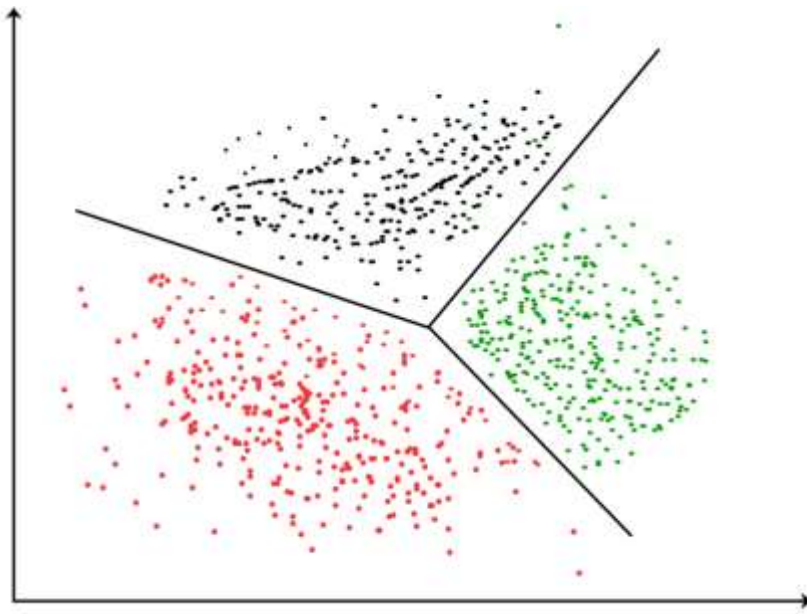
- Associação de padrões - Memória distribuída, inspirada no cérebro incorpora conhecimento por associação:
  - Auto-associação: Padrão armazenado após apresentações à rede. Recuperação de padrão parcialmente informado à rede.
  - Hetero-associação: Neste caso um conjunto de entrada é associado a um conjunto de saída distinto, portanto, a aridade pode ser qualquer.





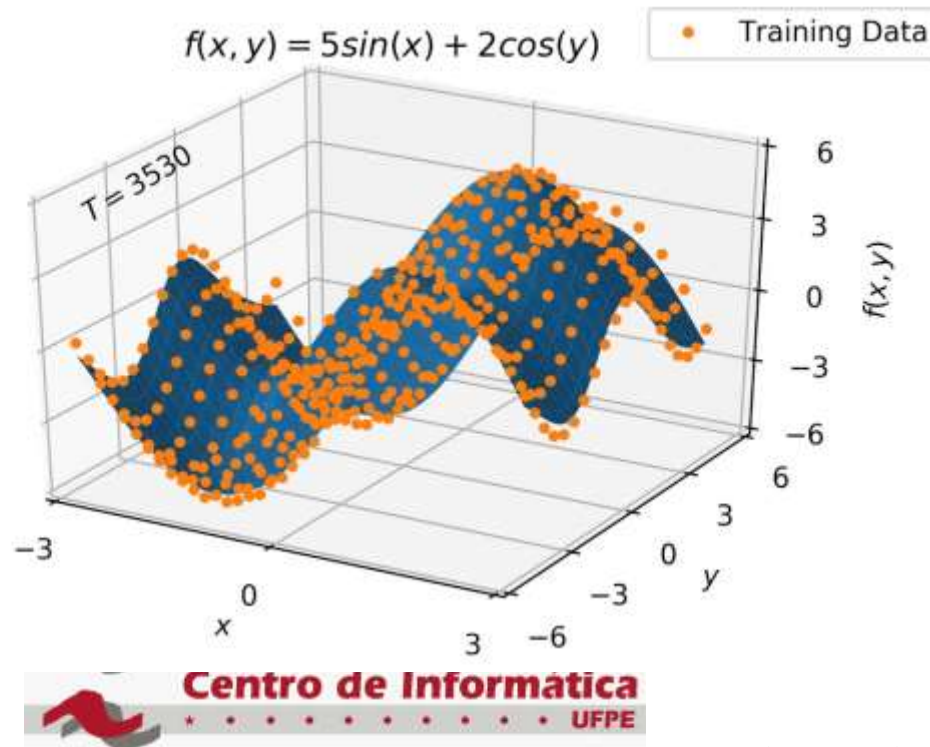
# Tarefas de Aprendizagem

- Reconhecimento de padrões - Um padrão ou sinal de entrada é incluído em uma entre possíveis categorias:
  - Classificação: Se a aprendizagem for supervisionada.
  - Agrupamento: Se a aprendizagem for não-supervisionada.



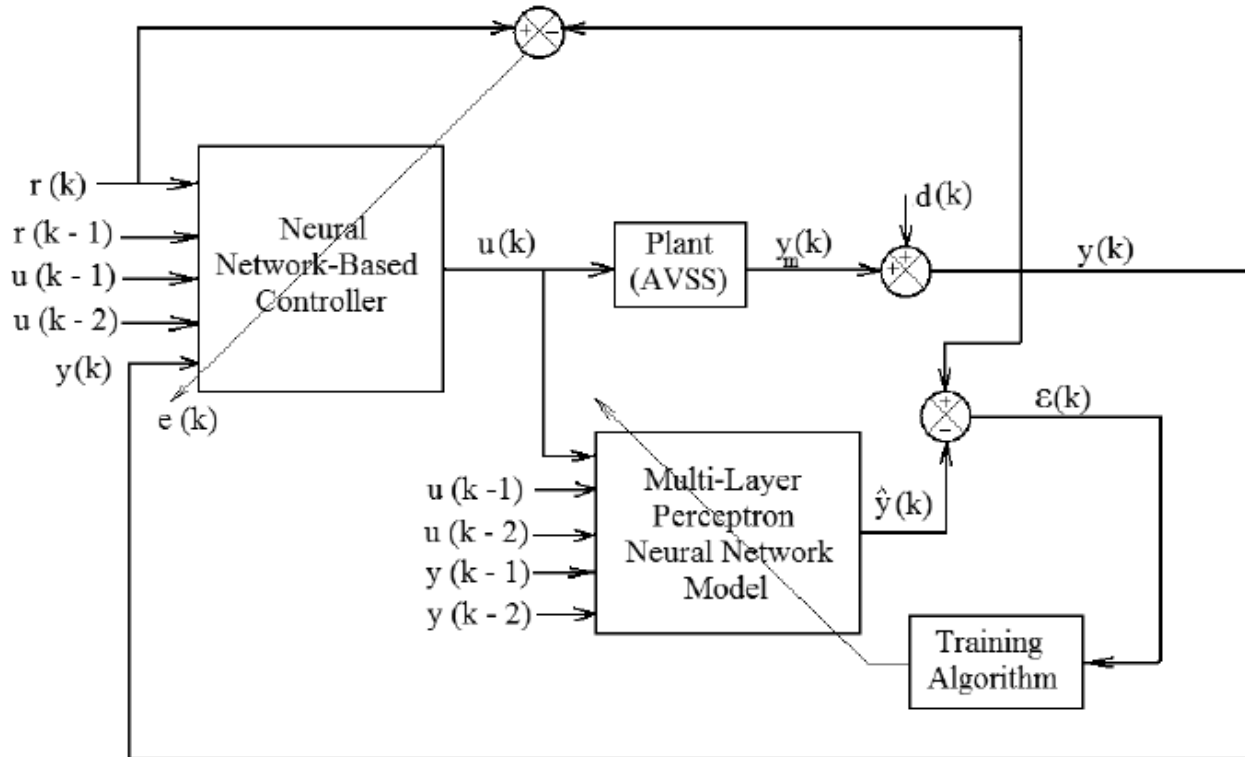
# Tarefas de Aprendizagem

- Determinação de funções – Produz rede neural que define uma função que replique um dado mapeamento entrada-saída:
  - Interpolação: Mapeamento que interpola pontos aos existentes;
  - Aproximação: Mapeamento que aproxima a relação (figura).



# Tarefas de Aprendizagem

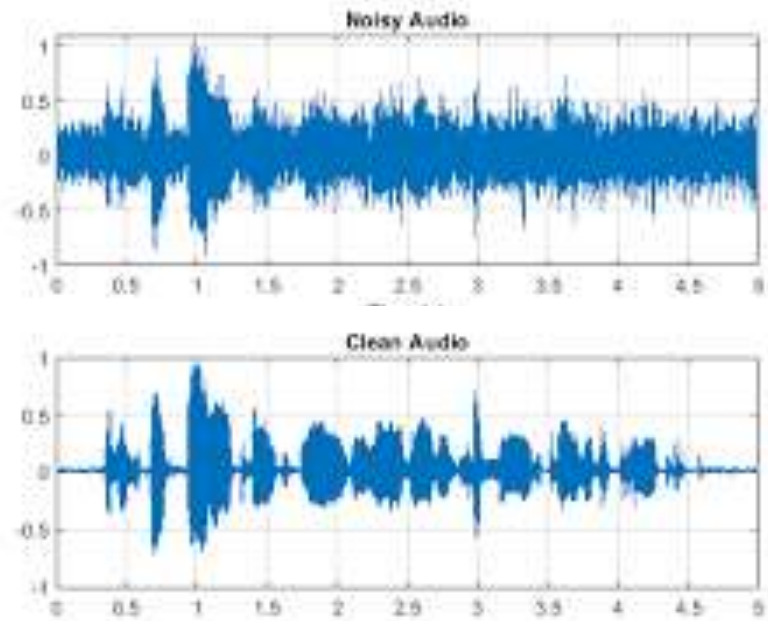
- Controle de processos - Rede neural para realizar identificação ou controle de um dado processo ou sistema:
  - Identificação de sistemas: Modela operação de um sistema;
  - Sistema inverso: Modela o controlador do sistema.





# Tarefas de Aprendizagem

- Filtragem de sinais – Separação de componentes de um sinal:
  - Filtragem: Elimina partes indesejáveis de um sinal;
  - Suavização: Retira variações bruscas de um sinal;
  - Predição: Antevê o comportamento futuro de um dado sinal.
- Exemplo: Retirando ruído com redes neurais profundas.



# Referências

- Du, K. L., & Swamy, M. N. (2019). *Neural networks and statistical learning*. Springer-Verlag. Second Edition.
- Mitchell, T. (1997). *Machine Learning*. McGraw Hill.
- Samuel, A. L. (1959). Some studies in machine learning using the game of checkers. *IBM Journal of Research and Development*, 3(3): 210-229.