Machine Learning Fundamentals

Machine learning is a subset of artificial intelligence that focuses on building systems that learn from data. Rather than being explicitly programmed, these systems improve their performance on a specific task through experience.

Supervised Learning involves training a model on labeled data. The algorithm learns a mapping function from input variables to output variables. Common algorithms include linear regression, logistic regression, support vector machines, decision trees, and neural networks.

In linear regression, the model finds the best-fitting line through the data points by minimizing the sum of squared residuals. The cost function J(theta) = (1/2m) * sum((h(x) - y)^2) is minimized using gradient descent.

Unsupervised Learning works with unlabeled data to discover hidden patterns. Clustering algorithms like K-means, hierarchical clustering, and DBSCAN group similar data points together. Dimensionality reduction techniques like PCA and t-SNE help visualize high-dimensional data.

K-means clustering partitions n observations into k clusters. The algorithm iteratively assigns each point to the nearest centroid and then recalculates centroids. The objective is to minimize within-cluster sum of squares (WCSS).

Neural Networks and Deep Learning

Neural networks are computing systems inspired by biological neural networks. They consist of layers of interconnected nodes (neurons) that process information. A typical network has an input layer, one or more hidden layers, and an output layer.

The backpropagation algorithm is the cornerstone of neural network training. It computes gradients of the loss function with respect to each weight by applying the chain rule of calculus, propagating error signals backward through the network.

Convolutional Neural Networks (CNNs) are specialized for processing grid-like data such as images. They use convolutional layers with learnable filters that detect features like edges, textures, and complex patterns at different spatial scales.

Recurrent Neural Networks (RNNs) are designed for sequential data. Long Short-Term Memory (LSTM) networks address the vanishing gradient problem by introducing gate mechanisms that control information flow through the network.

Transformers have revolutionized NLP by using self-attention mechanisms. The attention mechanism computes a weighted sum of values based on the compatibility between queries and keys, enabling the model to focus on relevant parts of the input.

Model Evaluation and Metrics

Evaluating machine learning models requires appropriate metrics. For classification, common metrics include accuracy, precision, recall, F1-score, and area under the ROC curve (AUC-ROC).

Cross-validation is a resampling technique used to evaluate models on limited data. K-fold cross-validation divides data into k subsets, trains on k-1 folds and validates on the remaining fold, rotating through all combinations.

The bias-variance tradeoff is a fundamental concept. High bias leads to underfitting (model too simple), while high variance leads to overfitting (model too complex). The goal is to find the sweet spot that minimizes total error.

Regularization techniques like L1 (Lasso) and L2 (Ridge) add penalty terms to the loss function to prevent overfitting. L1 promotes sparsity while L2 promotes small weights. Elastic Net combines both approaches.

Hyperparameter tuning optimizes model configuration. Grid search exhaustively evaluates all combinations, random search samples randomly from parameter space, and Bayesian optimization uses probabilistic models to guide the search.