

CSE 5819 Assignment #6

by: Aayushi Verma (uef24001)

This assignment is organized as follows:

1. ChatGPT - pg 2–5
2. Problems - pg 6–10
3. Coding - attached as a separate .ipynb file

1 Part 1: ChatGPT Self-Learning (20pts)

You can start from the following prompts, but you need to create subsequent questions that attempt to understand the basic concepts of machine learning.

1.1 What is the most used evaluation metric for classification?

The most commonly used evaluation metrics for classification include:

- **Accuracy:** The ratio of correctly predicted instances to the total instances.
- **Precision:** The ratio of true positive predictions to the sum of true and false positives.
- **Recall:** The ratio of true positive predictions to the sum of true positives and false negatives.
- **F1-score:** The harmonic mean of precision and recall, providing a balance between the two.
- **ROC-AUC:** The Area Under the Receiver Operating Characteristic Curve, measuring the trade-off between true positive rate and false positive rate.

1.2 What is the most used evaluation metric for regression?

The most commonly used evaluation metrics for regression include:

- **Mean Squared Error (MSE):** The average of the squared differences between predicted and actual values.
- **Root Mean Squared Error (RMSE):** The square root of the MSE, providing an interpretable error metric in the same units as the target variable.
- **Mean Absolute Error (MAE):** The average of the absolute differences between predicted and actual values.
- **R-squared (Coefficient of Determination):** A statistical measure indicating how well the regression predictions approximate the real data points.
- **Mean Absolute Percentage Error (MAPE):** The average percentage difference between predicted and actual values.

1.3 For supervised learning algorithms, what would be a reliable procedure of evaluating their performance?

A reliable procedure for evaluating the performance of supervised learning algorithms includes the following steps:

- **Train-Test Split:** Divide the dataset into two parts: a training set (used for model training) and a test set (used for final performance evaluation). A common split ratio is 80% training and 20% testing.
- **Cross-Validation:** Perform k -fold cross-validation (e.g., $k = 5$ or $k = 10$), where the dataset is split into k subsets. The model is trained on $k - 1$ subsets and tested on the remaining one. This process is repeated k times, and the results are averaged.
- **Evaluation Metrics:** Select appropriate evaluation metrics based on the type of task (e.g., accuracy, precision, recall, F1-score, ROC-AUC for classification, and MSE, MAE, R-squared for regression).
- **Hyperparameter Tuning:** Use techniques such as grid search or random search with cross-validation to fine-tune the model's hyperparameters for optimal performance.
- **Handling Class Imbalance:** If dealing with imbalanced datasets, use techniques like stratified sampling in cross-validation, resampling methods (oversampling/undersampling), or adjust performance metrics (e.g., weighted F1-score).
- **Test Set Evaluation:** After training and tuning the model, evaluate its performance on the previously unseen test set to get an unbiased estimate of its real-world performance.

1.4 Study bagging (bootstrapping aggregation)?

Bagging, or Bootstrap Aggregating, is an ensemble learning technique that improves the stability and accuracy of machine learning algorithms. The main ideas behind bagging are:

- **Bootstrapping:** Create multiple subsets of the training data by randomly sampling with replacement. Each subset has the same size as the original dataset but may include duplicate instances while omitting others.
- **Model Training:** Train a separate model on each of these bootstrapped subsets. The models can be of the same type (e.g., decision trees) or different types.
- **Aggregation:** Combine the predictions of all the models to produce a final output. For regression tasks, the average of the predictions is taken, while for classification tasks, a majority vote is used to determine the final class label.
- **Reduction of Variance:** By averaging the predictions of multiple models, bagging reduces overfitting and variance, leading to more robust and generalizable predictions.
- **Popular Algorithms:** One of the most well-known implementations of bagging is the Random Forest algorithm, which combines multiple decision trees trained on bootstrapped subsets of the data.

1.5 Why can the bagging procedure create models of lower variance?

The bagging procedure can create models of lower variance due to several key factors:

- **Ensemble of Models:** Bagging combines multiple models trained on different subsets of the data. Each model captures different patterns and noise in the data, which helps to smooth out individual model fluctuations.
- **Random Sampling with Replacement:** The bootstrapping process involves sampling with replacement, meaning some data points may be duplicated while others may be omitted. This results in different training sets for each model, leading to diverse models that are less likely to make the same errors.
- **Reduction of Overfitting:** Individual models, especially complex ones like decision trees, can overfit to the training data by capturing noise. By averaging the predictions of multiple models, bagging reduces the influence of any one model that may have overfitted, thereby decreasing overall model variance.
- **Majority Voting (Classification) or Averaging (Regression):** The aggregation step in bagging helps to average out the predictions, which reduces the impact of outliers and erratic predictions from individual models. This averaging effect leads to more stable and consistent final predictions.
- **Increased Robustness:** By leveraging the strengths of multiple models, bagging can improve generalization performance, making the ensemble more robust to variations in the data compared to single models.

1.6 What are the advantages of Support Vector Machine?

Support Vector Machines (SVM) offer several advantages, making them popular for various classification and regression tasks:

- **Effective in High-Dimensional Spaces:** SVMs are particularly effective in high-dimensional spaces, making them suitable for tasks involving large feature sets, such as text classification and image recognition.
- **Robust to Overfitting:** By maximizing the margin between classes, SVMs are less prone to overfitting, especially in high-dimensional datasets. The regularization parameter can further help control the trade-off between maximizing the margin and minimizing classification errors.
- **Versatile Kernel Trick:** SVMs can employ various kernel functions (e.g., linear, polynomial, radial basis function) to handle non-linear decision boundaries. This flexibility allows SVMs to adapt to complex data distributions.
- **Works Well with Smaller Datasets:** SVMs can perform well with smaller datasets, as they focus on the support vectors that define the decision boundary, rather than the entire dataset.
- **Clear Margin of Separation:** SVMs create a clear margin of separation between classes, which can lead to better generalization in the presence of noise in the data.

- **Binary and Multi-Class Classification:** Although inherently a binary classifier, SVMs can be extended to handle multi-class classification problems using strategies like one-vs-one or one-vs-all.
- **Robust to Outliers:** The decision boundary created by SVMs can be relatively unaffected by outliers, as the algorithm focuses on the support vectors that lie closest to the decision boundary.

1.7 What is Support Vector Regression?

Support Vector Regression (SVR) is an extension of Support Vector Machines (SVM) that is used for regression problems. SVR aims to find a function that approximates the relationship between the input features and the continuous target variable. The key concepts of SVR include:

- **Epsilon-Insensitive Loss Function:** SVR uses an epsilon-insensitive loss function, meaning that errors within a specified margin (epsilon) are not penalized. This allows the model to ignore small deviations between the predicted and actual values, providing a level of robustness to noise in the data.
- **Support Vectors:** Similar to SVM, SVR identifies support vectors that define the optimal regression function. Only the data points that lie outside the epsilon margin contribute to the model, focusing on the most relevant information for regression.
- **Margin of Tolerance:** The goal of SVR is to find a function that lies within the epsilon margin of the true values, ensuring that the predictions are as accurate as possible while maintaining a level of tolerance to errors.
- **Kernel Functions:** SVR can also utilize kernel functions, allowing it to handle non-linear relationships between the input features and the target variable. Common kernels include linear, polynomial, and radial basis function (RBF) kernels.
- **Regularization Parameter (C):** Similar to SVM, SVR has a regularization parameter C that controls the trade-off between achieving a low error on the training data and maintaining a smooth regression function. A smaller C results in a wider margin but allows more errors, while a larger C seeks to minimize errors at the cost of model complexity.
- **Applications:** SVR is widely used in various fields such as finance, bioinformatics, and engineering, where predicting continuous values is essential.

1.8 How many different formulations of SVM are there?

Support Vector Machines (SVM) have several formulations, each suited for different types of problems and data distributions. The main formulations include:

- **Hard Margin SVM:** This formulation assumes that the data is linearly separable without any noise. It aims to maximize the margin between the two classes while ensuring that all training samples are correctly classified. This approach is not robust to outliers.
- **Soft Margin SVM:** This formulation introduces a soft margin that allows for some misclassifications. It includes a regularization parameter C that controls the trade-off between maximizing the margin and minimizing classification errors. Soft Margin SVM is more robust to outliers and noise in the data.
- **SVM for Regression (Support Vector Regression, SVR):** This formulation adapts SVM for regression tasks. It aims to find a function that approximates the relationship between input features and continuous target variables, using an epsilon-insensitive loss function.
- **Multi-class SVM:** Although SVM is inherently a binary classifier, it can be extended to multi-class problems using techniques like one-vs-one (OvO) or one-vs-all (OvA). In OvO, a separate SVM is trained for every pair of classes, while in OvA, a separate SVM is trained for each class against all other classes.
- **Kernelized SVM:** This formulation leverages kernel functions to transform the input space, allowing SVM to find non-linear decision boundaries. Common kernels include linear, polynomial, radial basis function (RBF), and sigmoid.
- **Nu-SVM:** This is a variant of Soft Margin SVM that uses a parameter ν to control the number of support vectors and margin errors, providing additional flexibility in model training.

1.9 How to solve an SVM optimization problem?

Solving an SVM optimization problem involves finding the optimal hyperplane that maximizes the margin between different classes. The procedure can be broken down into the following steps:

- **Formulate the Optimization Problem:** For a binary classification problem with N training samples (\mathbf{x}_i, y_i) , where $y_i \in \{-1, 1\}$, the optimization problem can be formulated as:

$$\min_{\mathbf{w}, b} \frac{1}{2} \|\mathbf{w}\|^2 \quad (1)$$

$$\text{subject to } y_i(\mathbf{w} \cdot \mathbf{x}_i + b) \geq 1, \quad \forall i = 1, \dots, N \quad (2)$$

Here, \mathbf{w} is the weight vector, b is the bias term, and the constraints ensure that the samples are correctly classified with a margin of at least 1.

- **Introduce Slack Variables (Soft Margin SVM):** For non-linearly separable data, introduce slack variables ξ_i to allow for misclassifications:

$$\min_{\mathbf{w}, b, \xi} \frac{1}{2} \|\mathbf{w}\|^2 + C \sum_{i=1}^N \xi_i \quad (3)$$

$$\text{subject to } y_i(\mathbf{w} \cdot \mathbf{x}_i + b) \geq 1 - \xi_i, \quad \forall i = 1, \dots, N \quad (4)$$

$$\xi_i \geq 0 \quad (5)$$

The parameter C controls the trade-off between maximizing the margin and minimizing the classification errors.

- **Transform to the Dual Problem:** The primal problem can be transformed into a dual optimization problem using Lagrange multipliers α_i :

$$\max_{\alpha} \sum_{i=1}^N \alpha_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j y_i y_j \mathbf{x}_i \cdot \mathbf{x}_j \quad (6)$$

$$\text{subject to } \sum_{i=1}^N \alpha_i y_i = 0 \quad (7)$$

$$0 \leq \alpha_i \leq C, \quad \forall i = 1, \dots, N \quad (8)$$

- **Solve the Dual Problem:** Use optimization techniques such as Sequential Minimal Optimization (SMO) or gradient descent methods to solve the dual problem for α_i .
- **Calculate the Weight Vector and Bias:** After obtaining the optimal α_i , the weight vector \mathbf{w} can be calculated as:

$$\mathbf{w} = \sum_{i=1}^N \alpha_i y_i \mathbf{x}_i$$

The bias term b can be computed using any support vector:

$$b = y_k - \mathbf{w} \cdot \mathbf{x}_k \quad \text{for any } k \text{ where } \alpha_k > 0$$

- **Make Predictions:** Finally, to make predictions for a new sample \mathbf{x} , use the decision function:

$$f(\mathbf{x}) = \mathbf{w} \cdot \mathbf{x} + b$$

The predicted class label is determined by the sign of $f(\mathbf{x})$.

2 Problems

2.1 Question One

The method called “bagging” was not discussed in class lecture. “Bagging” is a short name of Bootstrap Aggregating. We would like you to self-study this concept via ChatGPT or any other online materials you trust. Bagging is not a model evaluation method but a model training method.

(a) Please describe the procedure of Bagging.

Bagging, short for Bootstrap Aggregating, is an ensemble learning technique designed to improve the stability and accuracy of machine learning algorithms. The procedure of bagging can be described in the following steps:

- **Bootstrap Sampling:** Create multiple subsets of the original training dataset by randomly sampling with replacement. Each subset, known as a bootstrap sample, may contain duplicate instances and will typically be of the same size as the original dataset.
- **Train Base Learners:** For each bootstrap sample, train a separate base learner (e.g., decision tree, neural network). Each model is trained independently, and the randomness introduced by bootstrap sampling ensures that the models capture different patterns in the data.
- **Aggregate Predictions:** Once all base learners are trained, aggregate their predictions to make a final prediction. For classification tasks, the most common aggregation method is majority voting, where the class predicted by the majority of the models is chosen. For regression tasks, the predictions are typically averaged.
- **Final Model Output:** The output of the bagging procedure is a single ensemble model that combines the strengths of all the individual base learners, often leading to improved performance and reduced variance compared to any single model.
- **Evaluation and Tuning:** After constructing the bagging ensemble, evaluate its performance on a validation dataset. Hyperparameters, such as the number of base learners or the type of base learner, can be tuned to optimize performance further.

(b) Why Bagging generally reduce model variance?

Bagging (Bootstrap Aggregating) generally reduces model variance due to the following reasons:

- **Independence of Base Learners:** By training multiple models on different bootstrap samples of the data, bagging introduces diversity among the base learners. Each model captures different aspects of the data, which helps to smooth out the predictions when aggregated.
- **Averaging Effect:** In regression tasks, the predictions from the individual models are averaged, while in classification tasks, majority voting is used. This aggregation process tends to cancel out the errors made by individual models. If one model makes a high variance error due to a particular subset of data, other models are less likely to make the same mistake, leading to a more stable overall prediction.
- **Reduction of Overfitting:** Models with high variance often overfit the training data, capturing noise and specific patterns that do not generalize well to new data. Bagging mitigates this effect by combining the outputs of multiple models, each trained on slightly different data, which can lead to a more generalized model that performs better on unseen data.
- **Error Reduction through Diversity:** When base learners are trained on different samples, they are likely to make different errors. The aggregation of these diverse predictions helps to reduce the overall error, resulting in lower variance in the ensemble model compared to individual models.
- **Robustness to Outliers:** Bagging is more robust to outliers since the influence of any single data point is diminished across the ensemble. As each model sees a different subset of the data, the impact of outliers on the final prediction is reduced.

2.2 Support Vector Machine

(a) [10 pts] The following is the primal formulation of L2 SVM (with the squared slack variables), which is a variant of the standard SVM that we discussed in our lecture.

$$\min_{w,b,\xi} \quad \frac{1}{2} \mathbf{w}^T \mathbf{w} + \frac{C}{2} \sum_{i=1}^N \xi_i^2 \quad (9)$$

$$\text{s.t.} \quad y_i(\mathbf{w}^T \mathbf{x}_i + b) \geq 1 - \xi_i, \quad i \in \{1, \dots, N\}, \quad (10)$$

$$\xi_i \geq 0, \quad i \in \{1, \dots, N\}. \quad (11)$$

If we remove the last constraints ($\xi_i \geq 0$), we might get a simpler optimization problem:

$$\min_{w,b,\xi} \quad \frac{1}{2} \mathbf{w}^T \mathbf{w} + \frac{C}{2} \sum_{i=1}^N \xi_i^2 \quad (12)$$

$$\text{s.t.} \quad y_i(\mathbf{w}^T \mathbf{x}_i + b) \geq 1 - \xi_i, \quad i \in \{1, \dots, N\}. \quad (13)$$

Please provide the Lagrangian of the above simplified formulation.

The Lagrangian for the simplified primal formulation of L2 SVM, where the last constraint $\xi_i \geq 0$ is removed, can be formulated as follows:

The simplified optimization problem is:

$$\min_{w,b,\xi} \quad \frac{1}{2} \mathbf{w}^T \mathbf{w} + \frac{C}{2} \sum_{i=1}^N \xi_i^2$$

subject to the constraints:

$$y_i(\mathbf{w}^T \mathbf{x}_i + b) \geq 1 - \xi_i, \quad \forall i \in \{1, \dots, N\}$$

The Lagrangian \mathcal{L} is formed by incorporating the constraints with Lagrange multipliers α_i :

$$\mathcal{L}(w, b, \xi, \alpha) = \frac{1}{2} \mathbf{w}^T \mathbf{w} + \frac{C}{2} \sum_{i=1}^N \xi_i^2 - \sum_{i=1}^N \alpha_i (y_i(\mathbf{w}^T \mathbf{x}_i + b) - (1 - \xi_i))$$

where: - $\alpha_i \geq 0$ are the Lagrange multipliers corresponding to each constraint.

The Lagrangian combines the original objective function and the penalty for violating the constraints, which will be optimized along with the primal variables w , b , and ξ .

(b) [15 pts] Please find the partial derivative of the Lagrangian in (a) with respect to w , b , and ξ_i .

The Lagrangian from part (a) is given by:

$$\mathcal{L}(\mathbf{w}, b, \xi, \alpha) = \frac{1}{2} \mathbf{w}^T \mathbf{w} + \frac{C}{2} \sum_{i=1}^N \xi_i^2 - \sum_{i=1}^N \alpha_i (y_i(\mathbf{w}^T \mathbf{x}_i + b) - (1 - \xi_i))$$

We need to compute the partial derivatives with respect to \mathbf{w} , b , and ξ_i :

1. ****Partial Derivative with respect to \mathbf{w} **:**

$$\frac{\partial \mathcal{L}}{\partial \mathbf{w}} = \mathbf{w} - \sum_{i=1}^N \alpha_i y_i \mathbf{x}_i$$

2. ****Partial Derivative with respect to b **:**

$$\frac{\partial \mathcal{L}}{\partial b} = - \sum_{i=1}^N \alpha_i y_i$$

3. ****Partial Derivative with respect to ξ_i **:**

$$\frac{\partial \mathcal{L}}{\partial \xi_i} = C \xi_i - \alpha_i$$

These partial derivatives are essential for setting up the conditions for optimality in the optimization problem of the L2 SVM formulation.

2.3 Cluster Analysis

[25 pts] Consider the following set of one-dimensional data points: $\{0.1, 0.25, 0.45, 0.55, 0.8, 0.9\}$. All the points are located in the range between $[0, 1]$.

(a) [15 pts] Suppose we apply K-Means clustering to obtain three clusters, A, B, and C. If the initial centroids are located at $\{0, 0.4, 1\}$, respectively, show the cluster assignments and locations of the updated centroids after the first three iterations by filling out the following table. (Hint: although you can directly calculate all distances, if you draw a real axis and put down the points, it might be easier to see the cluster assignment.)

Iter	Cluster assignment of data points	Centroid Location
0	0.10, 0.25 0.45, 0.55 0.80, 0.90	A B C
1	0.10, 0.25 0.45, 0.55 0.80, 0.90	A (0.175) B (0.5) C (0.95)
2	0.10, 0.25 0.45, 0.55, 0.80 0.90	A (0.175) B (0.55) C (0.90)
3	0.10, 0.25 0.45, 0.55, 0.80 0.90	A (0.175) B (0.55) C (0.90)

Table 1: K-Means clustering results after three iterations.

(b) [5 pts] Find the sum-of-squared errors (SSE) of the clustering after the third iteration.

To calculate the SSE, we need to compute the squared distances of each data point from its respective cluster centroid.

$$SSE = \sum_{i=1}^k \sum_{x_j \in C_i} (x_j - \mu_i)^2$$

Where: - μ_i is the centroid of cluster C_i . - x_j is a data point in cluster C_i .

For the clusters after the third iteration:

- ****Cluster A****: Centroid = 0.175 - Points: 0.1, 0.25 - $SSE_A = (0.1 - 0.175)^2 + (0.25 - 0.175)^2 = 0.005625 + 0.005625 = 0.01125$

- ****Cluster B****: Centroid = 0.55 - Points: 0.45, 0.55, 0.8 - $SSE_B = (0.45 - 0.55)^2 + (0.55 - 0.55)^2 + (0.8 - 0.55)^2 = 0.010000 + 0 + 0.062500 = 0.072500$

- ****Cluster C****: Centroid = 0.90 - Points: 0.90 - $SSE_C = (0.9 - 0.90)^2 = 0$

Thus, the total SSE is:

$$SSE = SSE_A + SSE_B + SSE_C = 0.01125 + 0.0725 + 0 = 0.08375$$

(c) [5 pts] For the dataset given in part (1), is it possible to obtain empty clusters? Why?

Yes, it is possible to obtain empty clusters in K-Means clustering, particularly when the initial centroids are poorly chosen.

In the context of the dataset $\{0.1, 0.25, 0.45, 0.55, 0.8, 0.9\}$ and the initial centroids $\{0, 0.4, 1\}$, the following scenarios can lead to empty clusters:

1. ****Poor Initialization****: If the initial centroids are chosen such that no data points are close enough to a particular centroid, that cluster will remain empty throughout the iterations. For instance, if the centroid at 1 does not have any data points near it, it may end up being an empty cluster.

2. ****Distance-based Assignments****: During the assignment step of K-Means, each data point is assigned to the nearest centroid. If the distances are such that all points are closer to the other centroids (e.g., points being closer to centroid 0 or 0.4), then the centroid at 1 will have no points assigned to it, leading to an empty cluster.

Thus, the occurrence of empty clusters is primarily influenced by the selection of initial centroids and the distribution of the data points.