Stable Conformal Prediction Sets

Reviewer : Seokhun Park

Department of Statistics
Seoul National University

Contents

Outline

Outline

Notation

- Consider data $\{(\mathbf{X}_i, Y_i)\}_{i=1}^{n+1} \in (\mathcal{X}, \mathcal{Y}) \sim^{iid} \mathbb{P}_{\mathbf{X},Y}$.
- Let $(\mathbf{X}_{n+1}, Y_{n+1})$ be a target data point.
- For a given set $\{U_1, ..., U_n\}$, the rank of $U_j, j \in [n]$ is defined as

$$\text{Rank}(U_j) = \sum_{i=1}^{n} \mathbb{I}(U_i \leq U_j),$$

where $\mathbb{I}$ is the indicator function.

Outline

What is conformal prediction ?

- Conformal prediction is a method for constructing prediction sets that contain the true outcome and has the following properties.
  1. Model-agnostic
  2. Distribution-free
  3. Applicable to finite data
- We want to find prediction set $C_\alpha(\mathbf{X}_{n+1})$ that is valid in the following sense:

$$\mathbb{P}(Y_{n+1} \in C_\alpha(\mathbf{X}_{n+1})) \geq 1 - \alpha, \tag{1}$$

where $\mathbb{P} = \prod_{i=1}^{n+1} \mathbb{P}_{\mathbf{X}_i, Y_i}$ and $\alpha \in (0, 1)$.

Lemma

Lemma 1

Let $U_1, \ldots, U_n, U_{n+1}$ *be an exchangable and identically distributed sequence of random variables. Then, for any* $\alpha \in (0,1)$, *we have*

$$\mathbb{P}_{\boldsymbol{U}}(Rank(U_{n+1}) \leq (n+1)(1-\alpha)) \geq 1-\alpha,$$

where $\mathbb{P}_{\boldsymbol{U}}$ *is a joint probability distribution for* $U_1, \ldots, U_{n+1}$.

- Lemma 1 means that the probability that U_{n+1} lies below the lower $100(1-\alpha)\%$ quantile is at least $(1-\alpha)$.

Score function (Nonconformity function)

1. Set score (Nonconformity) function $S(y,x)$ which measures nonconformity (unusualness) of y, i.e., $(S(y,x)\uparrow : y$ is unusual).
2. Calculate nonconformity values $E_i = S(Y_i, \mathbf{X}_i)$ for $i = 1, \ldots, n+1$.
3. Generate prediction sets for target data point using quantile of nonconformity values :

$$C_\alpha(\mathbf{X}_{n+1}) = \left\{ z \in \mathcal{Y} : \mathrm{Rank}(z, \mathbf{X}_{n+1}) \leq (n+1)(1-\alpha) \right\} \tag{2}$$

- In other words, prediction set is the **set of values considered usual**.
- Choosing the score function is very important.

Conformal coverage guarantee

- If $E_1, ..., E_{n+1}$ satisfies the conditions (exchangable and identically distributed), $C_\alpha(\mathbf{X}_{n+1})$ is valid, i.e.,

$$\mathbb{P}(Y_{n+1} \in C_\alpha(\mathbf{X}_{n+1})) \geq 1 - \alpha.$$

Outline

1. Preliminaries
   - Notation
   - Conformal prediction
   - Full Conformal Prediction
   - Split Conformal Prediction
2. Stable Conformal Prediction (2022 ICML)

Full Conformal Prediction

- Let $z \in \mathcal{Y}$ be a candidate for Y_{n+1}.
- Let $\hat{f}_z$ be a trained model on the data $\mathcal{D} \cup \{(\mathbf{X}_{n+1}, z)\}$.
- The score function in Full Conformal Prediction is :

$$E_i^{Full}(z) = S(Y_i, \mathbf{X}_i) = \ell(Y_i, \hat{f}_z(\mathbf{X}_i)), \quad \text{for} i = 1, ..., n \tag{3}$$

$$E_{n+1}^{Full}(z) = S(z, \mathbf{X}_{n+1}) = \ell(z, \hat{f}_z(\mathbf{X}_{n+1})), \tag{4}$$

where ℓ is a real-valued function .e.g., $\ell(a, b) = |a - b|$ for regression problem.

Full Conformal Prediction

- The full conformal prediction set for Y_{n+1} is given as

$$C_\alpha^{Full}(\mathbf{X}_{n+1}) = \left\{ z \in \mathcal{Y} : \text{Rank}(E_{n+1}^{Full}(z)) \leq (n+1)(1-\alpha) \right\}. \tag{5}$$

- Since conformity values $\{E_i^{Full}(Y_{n+1})\}_{i=1}^{n+1}$ satisfy the conditions of Lemma 1, $C_\alpha^{Full}(\mathbf{X}_{n+1})$ is valid.

Outline

Split Conformal Prediction

- Let $\mathcal{D}_{tr} = \{\mathbf{X}_i, Y_i\}_{i=1}^{m}$ be a train set, where $m < n$.
- Let $\mathcal{D}_{cal} = \{\mathbf{X}_i, Y_i\}_{i=m+1}^{n}$ be a calibration set.
- Let $\hat{f}_{\mathcal{D}_{tr}}$ be a trained model on the $\mathcal{D}_{tr}$.
- The score function in Split Conformal Prediction is :

$$E_i^{Splt} = S(Y_i, X_i) = \ell(Y_i, \hat{f}_{\mathcal{D}_{tr}}(\mathbf{X}_i)), \quad \text{for } i = m+1, ..., n \tag{6}$$

$$E_{n+1}^{Split}(z) = S(z, X_{n+1}) = \ell(z, \hat{f}_{\mathcal{D}_{tr}}(\mathbf{X}_{n+1})) \tag{7}$$

- The following split conformal prediction set is :

$$C_{\alpha}^{Split}(\mathbf{X}_{n+1}) = \left\{ z \in \mathcal{Y} : \mathrm{Rank}(E_{n+1}^{Split}(z)) \leq (n - m + 1)(1 - \alpha) \right\} \tag{8}$$

Comparison between Full and Split

- Full Conformal Prediction
  - To compute nonconformity values

$$\{E_1(z), ..., E_{n+1}(z)\},$$

    we need the trained model $\hat{f}_z$ for each $z \in \mathcal{Y}$.
  - That is, this leads to fitting a new model for each $z \in \mathcal{Y}$. It is computationally very demanding.
- Split Conformal Prediction
  - The prediction model needs to be trained only once on the train data $\mathcal{D}_{tr}$.
  - However, for small datasets, the prediction performance of the trained model may decrease, leading to a wider conformal prediction set.

Outline

Outline

Introduction

- Under the stability assumption of the prediction model in the full conformal prediction method, they proposed an algorithm that generates a prediction set by training the prediction model only once.

Notation Review

- Let $\hat{f}_\bullet$ be a trained model on the data $\mathcal{D} \cup \{\mathbf{X}_{n+1}, \bullet\}$.
- For $i \in [n]$, let

$$E_i^{Full}(z) = S(Y_i, \mathbf{X}_i) = \ell(Y_i, \hat{f}_z(\mathbf{X}_i)), \tag{9}$$

where ℓ is a real-valued function .e.g., $\ell(a,b) = |a-b|$ for regression problem.

Outline

Assumption of Stability

Definition 2 (Algorithmic Stability)

A prediction model $\hat{f}_\bullet$ is stable if for any observed features $x_i, i \in [n+1]$, there exists stability bounds $\{\tau_i\}_{i=1}^{n+1}$ such that

$$|\ell(q, \hat{f}_z(x_i)) - \ell(q, \hat{f}_{z_0}(x_i))| \leq \tau_i, \quad \text{for} \quad q, z_0, z \in \mathbb{R}.$$

- It means the assumption that when only one element (data point) in the train data changes, the prediction of the trained models does not change drastically.

Stable Conformal Set

Theorem 3

Assume that prediction model $\hat{f}_{\bullet}$ is stable, then for a given $z_0 \in \mathbb{R}$, we have

$$Rank(E_{n+1}^{Full}(z)) \geq Rank(E_{n+1}^{Stable}(z, z_0)), \tag{10}$$

where

$$E_i^{Stable}(z_0) = E_i^{Full}(z_0) - \tau_i, \quad i = 1, ..., n \tag{11}$$

$$E_{n+1}^{Stable}(z, z_0) = \ell(z, \hat{f}_{z_0}(X_{n+1})) - \tau_{n+1}, \tag{12}$$

for all $z \in \mathbb{R}$.

Stable Conformal Set

The stable conformal set is defined as

$$C_{\alpha,z_0}^{stable} = \left\{ z \in \mathcal{Y} : \mathrm{Rank}(E_{n+1}^{Stable}(z, z_0)) \leq (n+1)(1-\alpha) \right\}. \tag{13}$$

Since

$$\begin{aligned} &\left\{ \mathrm{Rank}(E_{n+1}(Y_{n+1})) \leq (n+1)(1-\alpha) \right\} \\ &\subseteq \left\{ \mathrm{Rank}(E_{n+1}^{Stable}(Y_{n+1}, z_0)) \leq (n+1)(1-\alpha) \right\}, \end{aligned} \tag{14}$$

the stable conformal set is valid.

Stability Bound

- Stability Bound
  - Let $\mathcal{L}$ be a loss function used for training prediction model.
  - Under the assumptions that the function $S(q, \cdot)$ is ρ-Lipschitz and a loss function $\mathcal{L}$ is γ-Lipschitz, they calculated τ_i, which depends on ρ and γ.

- Problem
  - Since the Lipschitz constants are not unknown, the stability bound τ_i is tuned as a hyperparameter.

Thank You

References