

**ĐẠI HỌC QUỐC GIA HÀ NỘI
TRƯỜNG ĐẠI HỌC CÔNG NGHỆ**



**BÁO CÁO BÀI TẬP LỚN
MÔN HỌC CÁC VẤN ĐỀ HIỆN ĐẠI TRONG
CÔNG NGHỆ THÔNG TIN**

Conformal Prediction

Giảng viên: PGS.TS. Nguyễn Hải Châu

Thành viên tham gia:

Vũ Minh Giang 19020807

Cao Việt Hoàng 19020819

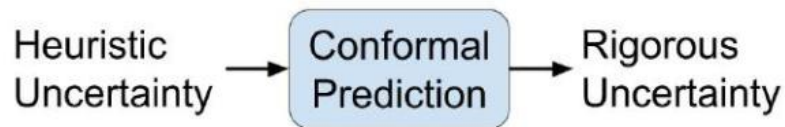
Nguyễn Quang Thịnh 20020476

Hà Nội, 2023

PHẦN LÝ THUYẾT

1. Conformal là gì, tại sao cần áp dụng conformal prediction cho các mô hình machine learning?

+ **Conformal prediction** là phương pháp để đo lường sự không chắc chắn của các mô hình học máy. Conformal prediction là chuyển đổi một điểm không chắc chắn (uncertainty score) thành điểm chặt chẽ (rigorous score). "Rigorous " có nghĩa là kết quả đầu ra có đảm bảo xác suất, đảm bảo rằng nó bao gồm kết quả thực sự.



Conformal prediction không quan tâm đến việc vấn đề dự đoán cơ bản có phải là rời rạc/liên tục hay là phân loại/hồi quy. Conformal prediction thay đổi hình dạng của một dự đoán: nó biến đổi các point predictions thành prediction regions. Đối với bài toán phân loại (classification) và hồi quy (regression), Conformal prediction biến đổi các bộ phân loại (classifiers) và bộ dự đoán (regressors) thành các dự đoán độ tin cậy (confidence predictors).

+ Cần áp dụng conformal prediction cho các mô hình machine learning vì:

Áp dụng conformal prediction cho các mô hình machine learning mang lại một số lợi ích quan trọng, đặc biệt là khi cần đánh giá mức độ không chắc chắn của dự đoán:

+ **Không phụ thuộc vào phân phối (Distribution-free):** Không có giả định về phân phối dữ liệu, khác với các phương pháp Bayesian nơi bạn phải chỉ định các tiên đề và phân phối dữ liệu.

+ **Không phụ thuộc vào mô hình (Model-agnostic):** Conformal prediction có thể được áp dụng cho bất kỳ mô hình dự đoán nào.

+ **Bảo đảm phủ (Coverage guarantee):** Các tập dự đoán kết quả cuối cùng đi kèm với đảm bảo về việc bao phủ kết quả thực sự với một xác suất nhất định.

2. Các giả thiết (asumption) của conformal prediction:

Các giả định chính của conformal prediction:

+ **Exchangeability of Data (Tính trao đổi của dữ liệu):** Conformal prediction giả sử rằng các điểm dữ liệu là có thể trao đổi, có nghĩa là thứ tự của các điểm dữ liệu không ảnh hưởng đến dự đoán. Giả định này đảm bảo phương pháp này có thể áp dụng cho nhiều tình huống dữ liệu khác nhau.

+ **Symmetry of the Model Fitting Algorithm (Sự đối xứng của thuật toán khớp mô hình):** Thuật toán được sử dụng để khớp mô hình không được thiên vị về bất kỳ thứ tự cụ thể nào của dữ liệu. Điều này đảm bảo rằng các khoảng dự đoán không bị ảnh hưởng bởi cách mô hình được đào tạo cụ thể.

Ngoài ra có cần nhắc thêm các giả định:

+ **Calibration:** Conformal prediction hoạt động tốt khi mô hình cơ bản được hiệu chỉnh đúng, nghĩa là xác suất dự đoán tương ứng với xác suất thực sự. Nếu mô hình không hiệu chỉnh tốt, các khoảng dự đoán kết quả có thể không chính xác phản ánh mức độ không chắc chắn thực sự.

+ **Independence:** Phương pháp này giả định sự độc lập giữa các điểm dữ liệu. Nếu có sự phụ thuộc hoặc tương quan giữa các điểm dữ liệu, có thể ảnh hưởng đến hiệu suất của conformal prediction.

+ **Finite Sample Size (Kích thước mẫu hữu hạn):** Conformal prediction cung cấp kết quả đáng tin cậy hơn với kích thước mẫu lớn hơn. Trong trường hợp kích thước mẫu rất nhỏ, các bảo đảm phủ có thể không chính xác.

+ **Reasonable Amount of Data (Lượng dữ liệu hợp lý):** Conformal prediction có thể không hoạt động tốt với một lượng dữ liệu rất nhỏ hoặc trong các tình huống dữ liệu rải rác. Có một lượng dữ liệu hợp lý là quan trọng để phương pháp này có thể tạo ra kết quả đáng tin cậy.

3. Một số phương pháp conformal prediction

+ **Split Conformal Prediction:** Phương pháp này chia dữ liệu thành các phần và xây dựng các dự đoán độ tin cậy cho mỗi phần, từ đó tạo ra một dự đoán tổng thể với độ tin cậy. Phương pháp này giúp tăng cường độ tin cậy của dự đoán bằng cách xem xét từng phần của dữ liệu và xây dựng dự đoán có độ tin cậy cho mỗi phần. Việc kết hợp các độ tin cậy này sau đó tạo ra một dự đoán chung mà cả tập dữ liệu đều được áp dụng, với mức độ tin cậy được tăng lên so với việc chỉ sử dụng toàn bộ tập dữ liệu một cách đồng nhất.

+ **Random Forest Conformal Prediction:** Sử dụng kỹ thuật rừng ngẫu nhiên (random forest) để xây dựng mô hình và ước lượng khoảng tin cậy dựa trên sự đa dạng của các cây quyết định.

+ **Support Vector Machines Conformal Prediction:** Sử dụng Support Vector Machines để ước lượng nonconformity scores và xây dựng các khoảng tin cậy. Được sử dụng chủ yếu cho bài toán phân loại và hồi quy.

+ **K-Nearest Neighbors Conformal Prediction (Dự Đoán Chuẩn Hóa K-Điểm Gần Nhất):** Sử dụng nguyên lý của K-Nearest Neighbors để xác định độ tin cậy cho dự đoán.

+ **Nonconformity Measures (Ước lượng Phi thường):** Phương pháp này dựa trên việc đo lường mức độ "phi thường" của mỗi điểm dữ liệu đối với mô hình. Nonconformity measures đo lường sự không phù hợp giữa dự đoán cho mỗi điểm dữ liệu so với toàn bộ tập dữ liệu. Các nonconformity measures này sau đó được sử dụng để xác định khoảng tin cậy.

+ **Inductive Conformal Prediction (ICP):** Sử dụng một tập huấn luyện để xác định nonconformity scores và xây dựng các khoảng tin cậy. Được thực hiện thông qua việc đo đặc sự không chắc chắn của mỗi điểm dữ liệu so với mô hình đã được huấn luyện.

+ **Transductive Conformal Prediction (TCP):** Giống như ICP, nhưng sử dụng cả tập huấn luyện và tập thử nghiệm để ước lượng nonconformity scores và tạo ra khoảng tin cậy. TCP có thể mang lại hiệu suất tốt hơn đối với dữ liệu ít.

+ **Algorithmic Conformal Prediction (ACP):** ACP sử dụng một thuật toán để tạo ra các tập hợp dự đoán conformal. Phương pháp này thường áp dụng thuật toán kiểm thử như k-Nearest Neighbors để đo lường sự giống nhau giữa các điểm dữ liệu và ước lượng mức độ tin cậy.