**BỘ QUỐC PHÒNG**

**TRƯỜNG ĐẠI HỌC THÔNG TIN LIÊN LẠC**

**KHÓA LUẬN TỐT NGHIỆP**

***Đề tài :***

**TÌM HIỂU VÀ VẬN DỤNG PHƯƠNG PHÁP XỬ LÝ**

**DỮ LIỆU LỚN**

**GVHD :** ThS. Cao Mạnh Hùng

**SINH VIÊN :**  Trịnh Đình Phúc

**LỚP:**  ĐHCN1A **KHOA:** CNTT

**KHÓA HỌC:** 2014 - 2018

*Khánh Hòa, tháng 06 năm 2018*

BỘ QUỐC PHÒNG

**TRƯỜNG ĐẠI HỌC THÔNG TIN LIÊN LẠC**

**KHÓA LUẬN TỐT NGHIỆP**

***Đề tài :***

**TÌM HIỂU VÀ VẬN DỤNG PHƯƠNG PHÁP XỬ LÝ**

**DỮ LIỆU LỚN**

**GVHD :** ThS. Cao Mạnh Hùng

**SINH VIÊN :**  Trịnh Đình Phúc

**LỚP:**  ĐHCN1A **KHOA:** CNTT

**KHÓA HỌC:** 2014 - 2018

*Khánh Hòa, tháng 06 năm 2018*

LỜI CẢM ƠN

Trong thời gian làm đồ án tốt nghiệp, em đã nhận được nhiều sự giúp đỡ, đóng góp ý kiến và chỉ bảo nhiệt tình của thầy cô, gia đình và bạn bè.

Em xin gửi lời cảm ơn chân thành đến ThS. Cao Mạnh Hùng, giảng viên Bộ môn Kỹ Thuật Máy Tính - Trường ĐH Thông Tin Liên Lạc người đã tận tình hướng dẫn, chỉ bảo em trong suốt quá trình làm khoá luận.

Em cũng xin chân thành cảm ơn các thầy cô giáo trong trường ĐH Thông Tin Liên Lạc đã cho em kiến thức về các môn đại cương cũng như các môn chuyên ngành, giúp em có được cơ sở lý thuyết vững vàng và tạo điều kiện giúp đỡ em trong suốt quá trình học tập.

Cuối cùng, em xin chân thành cảm ơn gia đình và bạn bè, đã luôn tạo điều kiện, quan tâm, giúp đỡ, động viên em trong suốt quá trình học tập và hoàn thành khoá luận tốt nghiệp.

Trường Đại Học Thông Tin Liên Lạc

Tháng 06 năm 2018

Sinh Viên Thực Hiện

**Trịnh Đình Phúc**

DANH MỤC BẢNG BIỂU VÀ HÌNH VẼ

Bảng biểu

[Bảng 2.1: Bảng số giờ học và kết quả 27](#_Toc516750102)

[Bảng 3.1: Bảng cân nặng và chiều cao lớp ĐHCN1A 32](#_Toc516750103)

[Bảng 3.2: Bảng số giờ học và kết quả 49](#_Toc516750104)

[Bảng 4.1: Bảng Confusion Matrix 59](#_Toc516750105)

[Bảng 4.2: Bảng True/False Positive/Negative 61](#_Toc516750106)

[Bảng 4.3: Bảng Normalized Confusion Matrix 61](#_Toc516750107)

Hình ảnh

[Hình 2.1: Phân nhóm Machine Learning dựa trên chức năng 5](#_Toc516750147)

[Hình 2.2: Quy trình CRISP-DM 7](#_Toc516750148)

[Hình 2.3: Mô hình chung cho các bài toán Machine Learning 11](#_Toc516750149)

[Hình 2.4: Sử dụng phương pháp PCA để giảm chiều dữ liệu 3D xuống 2D 15](#_Toc516750150)

[Hình 2.5: Underfitting và Overfitting với Polynominal Regression 22](#_Toc516750151)

[Hình 2.6: Bậc của đa thức 24](#_Toc516750152)

[Hình 2.7: Mô hình được xác định tại vòng lặp mà validation error đạt giá trị nhỏ nhất 26](#_Toc516750153)

[Hình 2.8: Cách thức hoạt động của PCA 28](#_Toc516750154)

[Hình 2.9: Cách thức hoạt động của PLSQ 28](#_Toc516750155)

[Hình 3.1: Hiển thị dữ liệu về chiều cao & cân nặng trên đồ thị 33](#_Toc516750156)

[Hình 3.2: Mô hình Linear Regression sau khi học xong 34](#_Toc516750157)

[Hình 3.3: Ảnh hưởng của Outliers 35](#_Toc516750158)

[Hình 3.4: Biểu diễn các điểm local và global 36](#_Toc516750159)

[Hình 3.5: Parapol của hàm f(x) 37](#_Toc516750160)

[Hình 3.6: Minh họa thuật toán Gradient Decent – Bước 1 39](#_Toc516750161)

[Hình 3.7: Minh họa thuật toán Gradient Decent – Bước 2 39](#_Toc516750162)

[Hình 3.8: Minh họa thuật toán Gradient Decent – Bước 3 40](#_Toc516750165)

[Hình 3.9: Minh họa thuật toán Gradient Decent – Bước 4 40](#_Toc516750167)

[Hình 3.10: Minh họa thuật toán Gradient Decent – Bước 5 41](#_Toc516750168)

[Hình 3.11: Bài toán phân cụm với 3 cluster 45](#_Toc516750169)

[Hình 3.12: Kết quả thi dựa trên số giờ học 50](#_Toc516750170)

[Hình 3.13: Một số loại Activation Function 50](#_Toc516750171)

[Hình 3.14: Mô tả Linear Regression không phù hợp 51](#_Toc516750172)

[Hình 3.15: Kiến trúc tổng quát của một mạng Neuron nhân tạo 52](#_Toc516750173)

[Hình 3.16: Quá trình xử lý thông tin của một ANN 53](#_Toc516750174)

[Hình 3.17: Hàm tổng của một neuron 54](#_Toc516750175)

[Hình 3.18: Hàm tổng của nhiều neuron 54](#_Toc516750176)

[Hình 3.19: Hàm chuyển đổi giữa internal activation và output 55](#_Toc516750177)

[Hình 3.20: Quá trình học của ANN 56](#_Toc516750178)

[Hình 4.1: Ví dụ về đường ROC 63](#_Toc516750179)

[Hình 4.2: Cách tính Precision và Recall 64](#_Toc516750180)

BẢNG CHỮ VIẾT TẮT & THUẬT NGỮ

|  |  |
| --- | --- |
| Chữ viết tắt/thuật ngữ tiếng anh | Mô Tả |
| CRISP-DM  (Cross-industry standard process for Data Mining) | Quy trình tiêu chuẩn liên ngành cho khai thác dữ liệu |
| Data Story | Là cách mà dẫn dắt người đọc quá trình rút trích insight từ bước ban đầu như cách tiếp cận,khám phá data cho đến các kĩ thuật xử lý data, đưa vào model. |
| ETL (Extract – Transform - Load) | **Extract**: tức là đi thu gom dữ liệu từ nhiều nguồn khác.  **Transform**: tức là chuyển đổi dữ liệu.  **Load**: Sau khi được chuyển đổi thì toàn bộ các dữ liệu này được đưa vào một nơi lưu trữ mới (DataWarehouse). |
| Insight | Trong marketing, Customer Insight là những suy nghĩ, mong muốn ẩn sâu bên trong ảnh hưởng đến quyết định mua hàng của Customers/Consumers. |
| GD (Gradient Decent) | Thuật toán xuống đồi |
| Linearly separable | Tách biệt tuyến tính, nếu tồn tại một đường phẳng phân chia hai class thì ta gọi hai class đó là linearly separable. Các thuật toán classification tạo ra các boundary là các đường phẳng được gọi chung là Linear Classifier. |
| Marketing | Marketing là một hệ thống tổng thể các hoạt động của tổ chức được thiết kế nhằm hoạch định, đặt giá, xúc tiến và phân phối các sản phẩm, dịch vụ, ý tưởng để đáp ứng nhu cầu của thị trường mục tiêu và đạt được các mục tiêu của tổ chức. |
| Marketer | Những người làm công việc marketing trong doanh nghiệp được gọi là Marketer. |
| Machine Learning | Machine Learning: (Máy Học) là một lĩnh vực nhỏ của Khoa Học Máy Tính, nó có khả năng tự học hỏi dựa trên dữ liệu đưa vào mà không cần phải được lập trình cụ thể. |
| Model Tuning | Là tinh chỉnh mô hình, hiểu được các thông số (parameter) của mô hình và tinh chỉnh các thông số này ra sao sẽ làm thay đổi đáng kể độ chính xác của mô hình dự đoán. Kĩ năng này đòi hỏi phải có hiểu biết thấu đáo về các thuật toán machine learning. |

MỤC LỤC

[Chương 1: TỔNG QUAN VỀ PHƯƠNG PHÁP XỬ LÝ DỮ LIỆU LỚN 1](#_Toc516750183)

[1.1. Tính thực tiễn 1](#_Toc516750184)

[1.2. Mục đích đề tài 2](#_Toc516750185)

[1.3. Phạm vi đề tài 2](#_Toc516750186)

[1.4. Phương pháp nghiên cứu 3](#_Toc516750187)

[1.5. Bố cục luận văn 3](#_Toc516750188)

[Chương 2: CỞ SỞ LÝ THUYẾT 5](#_Toc516750189)

[2.1. Machine Learning 5](#_Toc516750190)

[2.1.1. Định nghĩa 5](#_Toc516750191)

[2.1.2. Phân nhóm 5](#_Toc516750192)

[2.1.3. Regression 5](#_Toc516750193)

[2.1.4. Classification 6](#_Toc516750194)

[2.1.5. Clustering 6](#_Toc516750195)

[2.2. Quy trình khai phá dữ liệu 7](#_Toc516750196)

[2.2.1. Tìm hiểu nghiệp vụ (Business understanding) 7](#_Toc516750197)

[2.2.2. Tìm hiểu dữ liệu (Data understanding) 7](#_Toc516750198)

[2.2.3. Chuẩn bị dữ liệu (Data preparation) 7](#_Toc516750199)

[2.2.4. Mô hình hoá (Modeling) 8](#_Toc516750200)

[2.2.5. Đánh giá mô hình (Evaluation Model) 8](#_Toc516750201)

[2.2.6. Triển khai (Deployment) 8](#_Toc516750202)

[2.3. Các phương pháp khai thác dữ liệu 9](#_Toc516750206)

[2.3.1. Thống kê mô tả (Descriptive Statistics) 9](#_Toc516750207)

[2.3.2. Thống kê suy luận (Inferential Statistics) 9](#_Toc516750208)

[2.3.3. Phân tích dữ liệu thăm dò (Exploratory Data Analysis - EDA) 9](#_Toc516750209)

[2.3.4. Phân tích dự đoán (Predictive Analysis) 10](#_Toc516750210)

[2.4. Mô hình chung cho các bài toán Machine Learning 11](#_Toc516750211)

[2.4.1. Training phase 11](#_Toc516750212)

[2.4.2. Testing phase 13](#_Toc516750213)

[2.5. Feature Engineering 13](#_Toc516750214)

[2.5.1. Feature Selection 13](#_Toc516750215)

[2.5.2. Bag-of-Word 16](#_Toc516750216)

[2.5.3. Feature Scaling & Normalization 19](#_Toc516750217)

[2.6. Overfitting 21](#_Toc516750218)

[2.6.1. Giới thiệu 21](#_Toc516750219)

[2.6.2. Ví dụ 21](#_Toc516750220)

[2.6.3. Một số phương pháp tránh overfitting 23](#_Toc516750221)

[2.7. Multicollinearity (Đa cộng tuyến) 27](#_Toc516750222)

[2.7.1. Giới thiệu 27](#_Toc516750223)

[2.7.2. Cách phát hiện trường hợp đa cộng tuyến 28](#_Toc516750224)

[2.7.3. Hệ quả của đa cộng tuyến: 28](#_Toc516750225)

[2.7.4. Cách giải quyết đa cộng tuyến: 28](#_Toc516750226)

[Chương 3: MỘT SỐ MÔ HÌNH MACHINE LEARNING 29](#_Toc516750227)

[3.1. Linear Regression/Ordinary least squares 29](#_Toc516750229)

[3.1.1. Giới thiệu 29](#_Toc516750230)

[3.1.2. Dạng của Linear Regression 30](#_Toc516750231)

[3.1.3. Sai số dự đoán 30](#_Toc516750232)

[3.1.4. Hàm mất mát (Cost Function /Lost Function) 30](#_Toc516750233)

[3.1.5. Nghiệm trên bài toán Linear Regression 31](#_Toc516750234)

[3.1.6. Ví dụ trên Python 32](#_Toc516750235)

[3.1.7. Hạn chế của Linear Regression 35](#_Toc516750236)

[3.2. Gradient Decent 36](#_Toc516750237)

[3.2.1. Gradient Decent cho hàm một biến 37](#_Toc516750238)

[3.2.2. Gradient Decent cho hàm nhiều biến 42](#_Toc516750239)

[3.2.3. Stopping Criteria (điều kiện dừng) 42](#_Toc516750240)

[3.2.4. Biến thể của Gradient Descent 42](#_Toc516750241)

[3.2.5. Thứ tự lựa chọn điểm dữ liệu 43](#_Toc516750242)

[3.3. K-Means 44](#_Toc516750243)

[3.3.1. Giới thiệu 44](#_Toc516750244)

[3.3.2. Ví dụ 44](#_Toc516750245)

[3.3.3. Phân tích mặt toán học 45](#_Toc516750246)

[3.3.4. Thuật toán 46](#_Toc516750247)

[3.3.5. Hàm mất mát và bài toán tối ưu 46](#_Toc516750248)

[3.3.6. Thuật toán tối ưu hàm mất mát 47](#_Toc516750249)

[3.4. Logistic Regression 48](#_Toc516750250)

[3.4.1. Giới thiệu 48](#_Toc516750251)

[3.4.2. Ví dụ 49](#_Toc516750252)

[3.4.3. Mô hình Logistic Regression 50](#_Toc516750253)

[3.4.4. Sigmoid Function 51](#_Toc516750254)

[3.4.5. Tanh Function (Hyperpolic Tangent) 51](#_Toc516750255)

[3.5. Artificial Neural Network (ANN) 52](#_Toc516750256)

[3.5.1. Kiến trúc tổng quát của một ANN 52](#_Toc516750257)

[3.5.2. Quá trình xử lý thông tin của một ANN 53](#_Toc516750258)

[3.5.3. Transfer function 54](#_Toc516750259)

[3.5.4. Quá trình học (Learning Processing) của ANN 55](#_Toc516750260)

[3.5.5. Nguyên tắc huấn luyện (Training Protocols) 56](#_Toc516750261)

[Chương 4: ĐÁNH GIÁ MÔ HÌNH (MODEL EVALUATION) 58](#_Toc516750262)

[4.1. Giới Thiệu 58](#_Toc516750263)

[4.2. Accuracy 58](#_Toc516750264)

[4.3. Confusion Matrix (CM) 58](#_Toc516750265)

[4.4. True/False Positive/Negative 60](#_Toc516750266)

[4.5. Receiver operating characteristic curve (ROC) 62](#_Toc516750267)

[4.6. Area Under the Curve 63](#_Toc516750268)

[4.7. Precision và Recall 63](#_Toc516750269)

[4.8. Residual sum of squares (RSS) 65](#_Toc516750270)

[KẾT LUẬN 66](#_Toc516750272)

[1.1. Những phần đã làm hoàn thành 66](#_Toc516750273)

[1.2. Đánh giá ưu nhược điểm 66](#_Toc516750274)

[1.3. Phương hướng phát triển 66](#_Toc516750275)

Chương 1:  
TỔNG QUAN VỀ PHƯƠNG PHÁP XỬ LÝ DỮ LIỆU LỚN

* 1. Tính thực tiễn

Trong những năm gần đây, với sự phát triển vượt bậc của Công Nghệ Thông Tin và Truyền Thông, một khối lượng dữ liệu khổng lồ được sản sinh ra hàng ngày. Việc đưa ra các công cụ khai thác hiệu quả trên khối lượng lớn dữ liệu ấy nhằm rút trích các tri thức tiềm ẩn phục vụ cho nhu cầu sử dụng của con người là vô cùng cấp thiết.

* **Ngành Marketing:** Với việc đánh giá dữ liệu từ người dùng, các marketer có thể dễ dàng đưa ra các chiến dịch marketing cực kì hiệu quả, nhờ vào việc khai phá dữ liệu từ khách hàng với các đặc điểm như hành vi mua hàng trước đây, lịch sử mua hàng, thói quen người dùng, nhóm khách hàng....
* **Chính Phủ:** Các tổ chức chính phủ hoạt động về an ninh cộng đồng hoặc tiện ích xã hội sở hữu rất nhiều nguồn dữ liệu có thể khai thác insights. Ví dụ, khi phân tích dữ liệu cảm biến, chính phủ sẽ tăng mức độ hiệu quả của dịch vụ và tiết kiệm chi phí. Machine Learning còn hỗ trợ phát hiện gian lận và giảm thiểu khả năng trộm cắp danh tính.
* **Các dịch vụ tài chính:** Ngân hàng và các doanh nghiệp hoạt động trong lĩnh vực tài chính sử dụng việc khai thác dữ liệu với 2 mục đích chính: xác định insights trong dữ liệu và ngăn chặn lừa đảo. Insights sẽ cho biết được các cơ hội đầu tư hoặc thông báo đến nhà đầu tư thời điểm giao dịch hợp lý. Ngoài ra, dựa vào dữ liệu, các công ty, tổ chức cũng có thể tìm được những khách hàng đang có hồ sơ rủi ro cao hoặc sử dụng giám sát mạng để chỉ rõ những tín hiệu lừa đảo.

Như vậy, việc vận dụng khai phá dữ liệu có thể giải quyết được các nhu cầu trên.

* 1. Mục đích đề tài

Việc nghiên cứu đề tài “Tìm hiểu và vận dụng phương pháp xử lý dữ liệu lớn” trước hết là để hoàn thành khóa luận tốt nghiệp đại học tại trường Đại học Thông Tin Liên Lạc. Tiếp theo là nghiên cứu khoa học, bổ sung kiến thức bản thân phục vụ cho việc học tập, làm việc của bản thân và rộng hơn nữa là cho các cá nhân tổ chức có như cầu nghiên cứu lĩnh vực này có thêm nguồn tài liệu nghiên cứu, định hình được một khái niệm về việc khai phá dữ liệu. Và mục đích cuối cùng là có thể tạo ra được sản phẩm nền tảng giải quyết các vấn đề thực tiễn đáp ứng nhu cầu của các cá nhân tổ chức.

Mục đích cụ thể sẽ là tạo ra một báo cáo khoa học về quy trình dụng phương pháp xử lý dữ liệu lớn.

* 1. Phạm vi đề tài

Đối với đề tài khóa luận tốt nghiệp “Tìm hiểu và vận dụng phương pháp xử lý dữ liệu lớn” sẽ có các phạm vi nghiên cứu cũng như xây dựng đề tài trong giới hạn kiến thức và kinh phí của sinh viên cũng như là nội dung mà đề tài đề cập đến. Cụ thể như sau:

**Thời gian nghiên cứu:**

* Từ 3 tháng đến 4 tháng.
* Có kết hợp việc học và thực tập tại cơ quan.

**Nội dung nghiên cứu:**

* Kiến thức toán liên quan đến việc khai phá dữ liệu (đại số tuyến tính, giải tích, xác suất – thống kê, tối ưu hóa).
* Hệ cơ sở dữ liệu Cassandra.
* Quy trình khai phá dữ liệu.
* Kết hợp lý thuyết và thực tiễn tạo nên bài luận về đề tài “Tìm hiểu và vận dụng phương pháp xử lý dữ liệu lớn”.
  1. Phương pháp nghiên cứu

Để thực hiện được đề tài này cần phải áp dụng các phương pháp nghiên cứu khoa học logic, thống nhất, hiệu quả để đạt năng xuất và chất lượng cao nhất cho đề tài này.

**Đối với việc thu thập thông tin:**

* Thu thập thông tin từ các blog chuyên về Machine Learning như Machine Learning Cơ Bản, Ông Xuân Hồng.
* Nghiên cứu từ các khóa học online ở: Standford, Edx, Cousera, Udemy.
* Tham khảo từ một số đầu sách nổi tiếng về Machine Learning: Bishop, MachineLearningMastery.

**Đối với việc xử lý thông tin:**

* Nhận tất cả các thông tin liên quan nhưng chỉ xử lý và chắt lọc các thông tin liên quan trực tiếp hoặc gián tiếp gần với đề tài.
* Kiểm chứng lại thông tin trước khi sử dụng.
* Mô hình hóa các thông tin nhận được để chuyển thông tin thành dạng khoa học logic.
  1. Bố cục luận văn

Bố cục luận văn được chia làm 4 phần:

**Phần 1:** Cơ sở lý thuyết

Ở phần này, ta sẽ tìm hiểu hệ quản trị cơ sở dữ liệu NoSQL tên là Cassandra, quy trình khai phá dữ liệu, các phương pháp khai thác dữ liệu, mô hình chung cho các bài toán Machine Learning và các tình huống/trường hợp mắc phải (Overfitting, Multicollinearity...).

**Phần 2:** Một số mô hình Machine Learning

Ở phần 2, ta sẽ điểm qua một số mô hình Machine Learning tiêu biểu và được áp dụng trong đồ án tốt nghiệp. Một số mô hình như: Linear Regression, K-Means, Logistic Regression, Artificial Neural Network, Support Vector Machine.

**Phần 3:** Đánh giá mô hình

Ở phần 3, sau khi sử dụng mô hình Machine Learning, ta sẽ đánh giá mô hình bằng một số phương pháp như Accuracy, Confusion Matrix, True/False Positive/Negative, ROC, Area Under the Curve, Precision-Recall và RSS.

**Phần 4:** Kết Luận

Kết luận tổng thể các mô hình, nhận xét, nêu nguyên nhân và phương hướng phát triển để cải thiện mô hình Machine Learning.

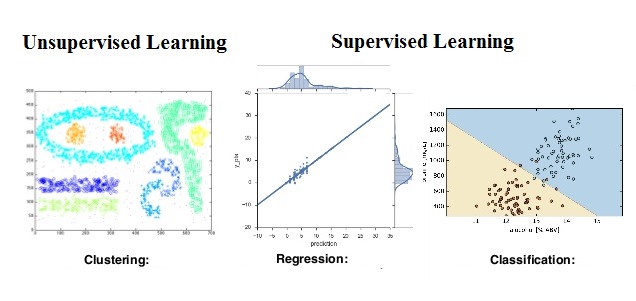
Chương 2:  
CỞ SỞ LÝ THUYẾT

* 1. Machine Learning
     1. **Định nghĩa**

**Machine Learning (máy học) là một lĩnh vực nhỏ của Khoa Học Máy Tính, nó có khả năng tự học hỏi dựa trên dữ liệu đưa vào mà không cần phải được lập trình cụ thể.**

* + 1. **Phân nhóm**

**Theo phương thức học, các thuật toán Machine Learning thường được chia làm 4 nhóm: Supervise learning, Unsupervised learning, Semi-supervised learning và Reinforcement learning.**



Hình 2.1: Phân nhóm Machine Learning dựa trên chức năng

* + 1. **Regression**

**Phân tích hồi quy là một phân tích thống kê để xác định xem các biến độc lập quy định các biến phụ thuộc như thế nào. Được dùng trong các bài toán dự đoán.**

**Ví dụ: Dự đoán giá nhà dựa vào địa điểm, diện tích, số phòng, giá nhà các năm trước đây...**

* + 1. **Classification**

**Một bài toán được gọi là classification nếu các label của input data được chia thành một số hữu hạn nhóm.**

**Ví dụ: Gmail xác định xem một email có phải là spam hay không; các hãng tín dụng xác định xem một khách hàng có khả năng thanh toán nợ hay không.**

* + 1. **Clustering**

**Một bài toán phân nhóm toàn bộ dữ liệu thành các nhóm nhỏ dựa trên sự liên quan giữa các dữ liệu trong mỗi nhóm.**

**Ví dụ: phân nhóm khách hàng dựa trên hành vi mua hàng. Điều này cũng giống như việc ta đưa cho một đứa trẻ rất nhiều mảnh ghép với các hình thù và màu sắc khác nhau, ví dụ tam giác, vuông, tròn với màu xanh và đỏ, sau đó yêu cầu trẻ phân chúng thành từng nhóm. Mặc dù không cho trẻ biết mảnh nào tương ứng với hình nào hoặc màu nào, nhiều khả năng chúng vẫn có thể phân loại các mảnh ghép theo màu hoặc hình dạng.**

* 1. Quy trình khai phá dữ liệu

Quy trình tiêu chuẩn liên ngành cho khai thác dữ liệu, thường được biết đến với từ viết tắt CRISP-DM (Cross Industry Standard Process for Data Mining) là một quy trình lặp, có khả năng quay lui (backtracking) gồm 6 giai đoạn:

Hình 2.2: Quy trình CRISP-DM

* + 1. Tìm hiểu nghiệp vụ (Business understanding)
* Hiểu mục tiêu nghiệp vụ
* Đánh giá tình huống
* Quy đổi từ mục tiêu nghiệp vụ sang mục tiêu khai phá dữ liệu
* Xây dựng kế hoạch dự án
  + 1. Tìm hiểu dữ liệu (Data understanding)
* Xem xét các yêu cầu về dữ liệu
* Thu thập, thăm dò và đánh giá chất lượng ban đầu
  + 1. Chuẩn bị dữ liệu (Data preparation)
* Lựa chọn dữ liệu
* Thu thập dữ liệu
* Tích hợp và định dạng dữ liệu (ETL)
* Làm sạch dữ liệu
* Chuyển đổi dữ liệu
  + 1. Mô hình hoá (Modeling)
* Lựa chọn kỹ thuật mô hình thích hợp
* Tách tập dữ liệu thành dữ liệu tập huấn (training data) và dữ liệu thử nghiệm (testing data) tập hợp con cho mục đích đánh giá
* Phát triển và kiểm tra các thuật toán mô hình thay thế và cài đặt tham số
* Tinh chỉnh cài đặt mô hình theo đánh giá ban đầu về hiệu suất của mô hình
  + 1. Đánh giá mô hình (Evaluation Model)
* Đánh giá mô hình trong bối cảnh ứng với các tiêu chí nghiệp vụ
* Phê duyệt mẫu
  + 1. Triển khai (Deployment)
* Tạo báo cáo kết quả
* Lập kế hoạch và phát triển quy trình triển khai
* Triển khai mô hình
* Phân phối kết quả mô hình và tích hợp trong hệ thống của tổ chức
* Lập kế hoạch bảo trì / cập nhật
* Đánh giá dự án

1. 3. Các phương pháp khai thác dữ liệu
      1. Thống kê mô tả (Descriptive Statistics)

Là các phương pháp liên quan đến việc thu thập số liệu, tóm tắt, trình bày, tính toán và mô tả các đặc trưng khác nhau để phản ánh một cách tổng quát đối tượng nghiên cứu.

* Các nguyên tắc định lượng mô tả các features chính của một tập dữ liệu. Về bản chất, nó mô tả một bộ dữ liệu.
* Quy trình mô tả và diễn dịch là các bước khác nhau.
  + 1. Thống kê suy luận (Inferential Statistics)

Là bao gồm các phương pháp ước lượng các đặc trưng của tổng thể, phân tích mối liên hệ giữa các hiện tượng nghiên cứu, dự đoán hoặc ra quyết định trên cơ sở thu thập thông tin từ kết quả quan sát mẫu. Nghĩa là, thống kê từ một lượng sample để dự đoán về population.

* Suy luận thường là mục tiêu của các mô hình thống kê (Statistical models).
* Suy luận phụ thuộc rất nhiều vào population và sample.
  + 1. Phân tích dữ liệu thăm dò (Exploratory Data Analysis - EDA)

Là một cách tiếp cận để phân tích các tập dữ liệu để tóm tắt các đặc điểm chính của chúng, tìm các mối quan hệ chưa được biết trước đó, thường với các phương pháp visual. EDA khác với phân tích dữ liệu ban đầu (Initial Data Analysis - IDA) tập trung hẹp hơn trong việc kiểm tra các giả định cần thiết cho việc kiểm tra mô hình và giả thuyết, và xử lý các giá trị thiếu và thực hiện các biến đổi khi cần. EDA bao gồm IDA.

* Khám phá các model tốt cho việc khám phá các kết nối mới.
* Có ích cho việc định nghĩa các nghiên cứu và câu hỏi trong tương lai.
* Không nên sử dụng phân tích thăm dò để khái quát hoặc dự đoán.
  + 1. Phân tích dự đoán (Predictive Analysis)

Phân tích dự đoán là nhánh của phân tích nâng cao được sử dụng để đưa ra dự đoán về các sự kiện không xác định trong tương lai. Phân tích dự báo sử dụng nhiều kỹ thuật từ khai phá dữ liệu, thống kê, mô hình hóa, học máy và trí thông minh nhân tạo để phân tích dữ liệu hiện tại để đưa ra dự đoán về tương lai. Nó sử dụng một số khai thác dữ liệu, mô hình tiên đoán và các kỹ thuật phân tích để tập hợp quản lý, công nghệ thông tin và quy trình nghiệp vụ mô hình hóa để đưa ra dự đoán về tương lai. Các mẫu tìm thấy trong dữ liệu lịch sử và giao dịch có thể được sử dụng để xác định các rủi ro và cơ hội cho tương lai. Các mô hình phân tích dự đoán nắm bắt các mối quan hệ giữa nhiều yếu tố để đánh giá rủi ro với một tập hợp các điều kiện cụ thể để gán điểm hoặc trọng số. Bằng cách áp dụng thành công các phân tích dự báo, các doanh nghiệp có thể giải thích một cách hiệu quả các dữ liệu lớn vì lợi ích của họ.

* 1. Mô hình chung cho các bài toán Machine Learning

Phần lớn các bài toán Machine Learning có thể được thể hiện trong hình vẽ dưới đây:

Hình 2.3: Mô hình chung cho các bài toán Machine Learning

* + 1. Training phase
       1. Đầu vào

Mục đích của Feature Engineering là tạo ra một “Feature Extractor” biến dữ liệu thô ban đầu thành dữ liệu phù hợp với từng mục đích khác nhau.

* + - 1. Đầu ra
* Raw training input:

Raw input là tất cả các thông tin ta biết về dữ liệu. Ví dụ: với ảnh thì là giá trị của từng pixel, với văn bản thì là từng từ, từng câu. với file âm thanh thì nó là một đoạn tín hiệu.

* Output của training set
  + Trong các bài toán Unsupervised learning, ta không biết output nên hiển nhiên sẽ không có đầu vào này.
  + Trong các bài toán Supervised learning, có khi dữ liệu này cũng không được sử dụng.

Ví dụ: nếu raw input đã có cùng số chiều rồi nhưng số chiều quá lớn, ta muốn giảm số chiều của nó thì cách đơn giản nhất là chiếu vector đó xuống một không gian có số chiều nhỏ hơn bằng cách lấy một ma trận ngẫu nhiên nhân với nó. Ma trận này thường là ma trận béo (số hàng ít hơn số cột, tiếng Anh - fat matrices) để đảm bảo số chiều thu được nhỏ hơn số chiều ban đầu. Việc làm này mặc dù làm mất đi thông tin, trong nhiều trường hợp vẫn mang lại hiệu quả vì đã giảm được lượng tính toán ở phần sau. Đôi khi ma trận chiếu không phải là ngẫu nhiên mà có thể được học dựa trên toàn bộ raw input, ta sẽ có bài toán tìm ma trận chiếu để lượng thông tin mất đi là ít nhất.

Trong nhiều trường hợp, dữ liệu output của training set cũng được sử dụng để tạo ra Feature Extractor. Ví dụ: trong bài toán classification, ta không quan tâm nhiều đến việc mất thông tin hay không, ta chỉ quan tâm đến việc những thông tin còn lại có đặc trưng cho từng class hay không. Ví dụ, dữ liệu thô là các hình vuông và hình tam giác có màu đỏ và xanh. Trong bài toán phân loại đa giác, các output là tam giác và vuông, thì ta không quan tâm tới màu sắc mà chỉ quan tâm tới số cạnh của đa giác. Ngược lại, trong bài toán phân loại màu, các class là xanh và đỏ, ta không quan tâm tới số cạnh mà chỉ quan tâm đến màu sắc thôi.

* Main Algorithms (các thuật toán chính)

Khi có được extracted features rồi, chúng ta sử dụng những thông tin này cùng với training output và prior knowledge để tạo ra các mô hình phù hợp.

* Lưu ý: Khi xây dựng bộ feature extractor và main algorithms, chúng ta không được sử dụng bất kỳ thông tin nào trong tập test data. Ta phải giả sử rằng những thông tin trong test data chưa được nhìn thấy bao giờ.
  + 1. Testing phase

Bước này đơn giản hơn nhiều. Với raw input mới, ta sử dụng feature extractor đã tạo được ở trên (tất nhiên không được sử dụng output của nó vì output là cái ta đang đi tìm) để tạo ra feature vector tương ứng. Feature vector được đưa vào main algorithm đã được học ở training phase để dự đoán output.

* 1. Feature Engineering

Khi làm việc với các bài toán Machine Learning thực tế, nhìn chung chúng ta chỉ có được dữ liệu thô (raw) chưa qua chỉnh sửa, chọn lọc. Chúng ta cần phải tìm một phép biến đổi để loại ra những dữ liệu nhiễu (noise), và để đưa dữ liệu thô với số chiều khác nhau về cùng một chuẩn (cùng là các vector hoặc ma trận). Dữ liệu chuẩn mới này phải đảm bảo giữ được những thông tin đặc trưng (features) cho dữ liệu thô ban đầu. Không những thế, tùy vào từng bài toán, ta cần thiết kế những phép biến đổi để có những features phù hợp. Quá trình quan trọng này được gọi là Feature Extraction, hoặc Feature Engineering, tiếng việt gọi là trích chọn đặc trưng. Feature engineering cố gắng biểu diễn tốt nhất tập dữ liệu ban đầu sao cho tương thích với mô hình dự đoán đang sử dụng.

* + 1. Feature Selection

Giả sử rằng các điểm dữ liệu có số features khác nhau (do kích thước dữ liệu khác nhau hay do một số feature mà điểm dữ liệu này có nhưng điểm dữ liệu kia lại không thu thập được) và số lượng features là cực lớn. Chúng ta cần chọn ra một số lượng nhỏ hơn các feature phù hợp với bài toán.

*Một số cách trong Feature Selection như:*

* + - 1. Cách 1: Loại bỏ các features có giá trị phương sai thấp:

Ngưỡng phương sai (*VarianceThreshold*) là một phương pháp cơ bản của Feature Selection. Nó loại bỏ tất cả các features có phương sai không đáp ứng giá trị ngưỡng. Theo mặc định, nó loại bỏ tất cả các tính năng zero-variance (phương sai bằng 0), tức là các features có cùng giá trị trong tất cả các sample.

Trong đó: **p** là số phần trăm muốn loại bỏ của một sample, như ví dụ dưới đây, ta chọn 80% = 0.8

**from** sklearn.feature\_selection **import** VarianceThreshold  
**import** numpy **as** np  
X = [[0, 0, 1], [0, 1, 0], [1, 0, 0], [0, 1, 1], [0, 1, 0], [0, 1, 1]]  
sel = VarianceThreshold(threshold=(.8 \* (1 - .8)))  
print(**"Ma trận ban đầu:\n{}\n\nMa trận sau khi transform:\n{}\n"**.format(X, sel.fit\_transform(X)))**def** column(matrix, i):  
 **return** [row[i] **for** row **in** matrix]  
print(**"Giá trị của varianceThreshold là: {}"**.format(sel))  
print(**"Giá trị variance của cột 0 là: {}\nGiá trị variance của cột 1 là: {}"**.format(np.var(column(X,0)),np.var(column(X,1))))

*Kết Quả:*

Ma trận ban đầu:

[[0, 0, 1], [0, 1, 0], [1, 0, 0], [0, 1, 1], [0, 1, 0], [0, 1, 1]]

Ma trận sau khi transform:

[[0 1] [1 0] [0 0] [1 1] [1 0] [1 1]]

#Ta có thể thấy VarianceThreshold đã xóa cột đầu tiên của ma trận vì variance của cột 0 < giá trị VarianceThreshold

#để kiểm chứng, ta sẽ thử xem giá trị của cột 0 và cột 1 của ma trận

Giá trị của varianceThreshold là:

VarianceThreshold(threshold=0.15999999999999998)

Giá trị variance của cột 0 là: 0.13888888888888892

Giá trị variance của cột 1 là: 0.22222222222222224

* + - 1. Dimentionality Reduction

Khi Một phương pháp khác là làm giảm số chiều của dữ liệu để giảm bộ nhớ và khối lượng tính toán. Việc giảm số chiều này có thể được thực hiện bằng nhiều cách, trong đó random projection là cách đơn giản nhất. Tức chọn một ma trận chiếu (projection matrix) ngẫu nhiên rồi nhân nó với từng điểm dữ liệu (giả sử dữ liệu ở dạng vector cột) để được các vector có số chiều thấp hơn.

Ví dụ, vector ban đầu có số chiều là 784, chọn ma trận chiếu có kích thước (100x784), khi đó nếu nhân ma trận chéo này với vector ban đầu, ta sẽ được một vector mới có số chiều là 100, nhỏ hơn số chiều ban đầu rất nhiều. Lúc này, có thể ta không có tên gọi cho mỗi feature nữa vì các feature ở vector ban đầu đã được trộn lẫn với nhau theo một tỉ lệ nào đó rồi lưu và vector mới này. Mỗi thành phần của vector mới này được coi là một feature (không tên).

Việc chọn một ma trận chiếu ngẫu nhiên đôi khi mang lại kết quả tệ không mong muốn vì thông tin bị mất đi quá nhiều.

Một phương pháp được sử dụng nhiều để hạn chế lượng thông tin mất đi có tên là Principle Component Analysis:

Hình 2.4: Sử dụng phương pháp PCA để giảm chiều dữ liệu 3D xuống 2D

Chú ý: Feature learning không nhất thiết phải làm giảm số chiều dữ liệu, đôi khi feature vector còn có số chiều lớn hơn raw data. Random projection cũng có thể làm được việc này nếu ma trận chiếu là một ma trận cao (số cột ít hơn số hàng).

* + 1. Bag-of-Word

Bag-of-word (BoW) là phương pháp đưa các từ, các câu, đoạn văn ở dạng text trong các văn bản về một vector mà mỗi phần tử là một số. Ý tưởng của BoW là phân tích và phân nhóm dựa theo "Bag of Words". Với test-data mới, tiến hành tìm ra số lần từng từ của test data xuất hiện trong "bag". Tuy nhiên BoW vẫn tồn tại khuyết điểm, nên TF-IDF là phương pháp khắc phục. Có thể ứng dụng BoW + TF-IDF vào việc tìm kiếm, phân loại tài liệu, lọc mail spam xác định ý định của người dùng.

Giải pháp phổ biến là sử dụng một phương pháp thống kê có tên là Term Frequency– Inverse Document Frequency (TF-IDF), giá trị TF-IDF của một từ là một con số thu được qua thống kê thể hiện mức độ quan trọng của từ này trong một văn bản, mà bản thân văn bản đang xét nằm trong một tập hợp các văn bản.

Đầu tiên, TF(Term Frequency) là tần số xuất hiện của 1 từ trong 1 văn bản có cách tính như sau:

*Trong đó:*

* *f(t,d)**số lần xuất hiện từ t trong văn bản d*
* *Mẫu số là tổng số từ trong văn bản d*

Tiếp theo, là IDF (Inverse Document Frequency): Tần số nghịch của 1 từ trong tập văn bản.

Mục đích của việc tính IDF là giảm giá trị của các từ thường xuyên xuất hiện như "is", "the"... Do các từ này không mang nhiều ý nghĩa trong việc phân loại văn bản.

*Trong đó:*

* ***N:*** *là tổng các văn bản trong một tập văn bản* ***N =* |D|**
* *số lượng văn bản khi mà t xuất hiện.*

Cuối cùng, **TF-IDF** những từ có giá trị TF-IDF cao là những từ xuất hiện nhiều trong văn bản này, và xuất hiện ít trong các văn bản khác. Việc này giúp lọc ra những từ phổ biến và giữ lại những từ có giá trị cao (từ khoá của văn bản đó). Được tính bởi công thức:

**Áp dụng:**

Khởi tạo 2 văn bản, tính số lần xuất hiện của mỗi từ trong văn bản:

*# Khởi tạo 2 văn bản text1, text2*

text1 = **"Phúc thích xem phim , Trâm cũng thích xem phim"**text2 = **"Ngoài ra , Phúc còn thích bơi lội"**bowA = text1.split(**" "**) *# tách từ ở văn bản 1*bowB = text2.split(**" "**) *# tách từ ở văn bản 2*

*#Tạo một dictionary*word\_dict = set(bowA).union(set(bowB))  
wordDictA = dict.fromkeys(word\_dict, 0)  
wordDictB = dict.fromkeys(word\_dict, 0)  
  
*#Đếm số lượng từ***for** word **in** bowA:  
 wordDictA[word]+=1  
**for** word **in** bowB:  
 wordDictB[word]+=1  
  
print(**"Các từ trong 2 văn bản là:\n {}"**.format(word\_dict))  
print(**"Số từ xuất hiện trong văn bản 1 là:\n {}\n\nSố từ xuất hiện trong văn bản 2 là:\n {}"**.format(wordDictA,wordDictB))

*Kết quả:*

Các từ trong 2 văn bản là:

{'thích', 'phim', ',', 'lội', 'cũng', 'ra', 'Trâm', 'còn', 'Ngoài', 'Phúc', 'xem', 'bơi'}

Số từ xuất hiện trong văn bản 1 là:

{'thích': 2, 'phim': 2, ',': 1, 'lội': 0, 'cũng': 1, 'ra': 0, 'Trâm': 1, 'còn': 0, 'Ngoài': 0, 'Phúc': 1, 'xem': 2, 'bơi': 0}

Số từ xuất hiện trong văn bản 2 là:

{'thích': 1, 'phim': 0, ',': 1, 'lội': 1, 'cũng': 0, 'ra': 1, 'Trâm': 0, 'còn': 1, 'Ngoài': 1, 'Phúc': 1, 'xem': 0, 'bơi': 1}

***Tính TF*:**

**def** compute\_TF(word\_dict, bow):  
 tf\_dict = {}  
 bow\_count = len(bow)  
 **for** word, count **in** word\_dict.items():  
 tf\_dict[word] = count / float(bow\_count)  
 **return** tf\_dict

print(**"\nKết quả TF:\n văn bản 1: {}\n văn bản 2 {}"** .format(compute\_TF(wordDictA,bowA),compute\_TF(wordDictB,bowB)))

*Kết quả:*

Kết quả TF:

văn bản 1: {'xem': 0.2, 'thích': 0.2, 'còn': 0.0, 'Ngoài': 0.0, 'ra': 0.0, 'Trâm': 0.1, ',': 0.1, 'bơi': 0.0, 'lội': 0.0, 'Phúc': 0.1, 'phim': 0.2, 'cũng': 0.1}

văn bản 2: {'xem': 0.0, 'thích': 0.125, 'còn': 0.125, 'Ngoài': 0.125, 'ra': 0.125, 'Trâm': 0.0, ',': 0.125, 'bơi': 0.125, 'lội': 0.125, 'Phúc': 0.125, 'phim': 0.0, 'cũng': 0.0}

**Tính IDF:**

**def** compute\_IDF(doc\_list):  
 **import** math *#import thư viện math* idf\_dict = {} *#tạo một dictionary rỗng* N = len(doc\_list) *#gán độ dài của list cho biến N* idf\_dict = dict.fromkeys(doc\_list[0].keys(), 0) *#tạo dictionary lưu các keys với value = 0  
 #lọc ra thành 1 list gồm các từ xuất hiện >=1 lần* **for** doc **in** doc\_list:  
 **for** word, count **in** doc.items():  
 **if** count > 0:  
 idf\_dict[word] += 1  
 **for** word, count **in** idf\_dict.items():  
 idf\_dict[word] = math.log(N / float(count))  
 **return** idf\_dict

print(**"Kết Quả IDF:\n {}"**.format(compute\_IDF([wordDictA, wordDictB])))

*Kết quả:*

Kết Quả IDF:

{'cũng': 0.6931471805599453, 'Phúc': 0.0, 'bơi': 0.6931471805599453, 'Trâm': 0.6931471805599453, 'ra': 0.6931471805599453, 'phim': 0.6931471805599453, 'lội': 0.6931471805599453, 'còn': 0.6931471805599453, 'xem': 0.6931471805599453, 'Ngoài': 0.6931471805599453, ',': 0.0, 'thích': 0.0}

Từ kết quả trên có thể nhìn thấy những từ có trọng số càng cao thì những từ đó càng có giá trị phân loại và ngược lại ví dụ như từ "thích", dấu “,” xuất hiện nhiều nên sẽ không có giá trị phân loại các văn bản với nhau. Tuy nhiên bộ train data lần này ít nên hiệu quả không rõ rệt, nếu thử trên lượng data lớn chắc chắn sẽ rất hiệu quả.

* + 1. Feature Scaling & Normalization

Các điểm dữ liệu đôi khi được đo đạc với những đơn vị khác nhau, m và feet chẳng hạn. Hoặc có hai thành phần (của vector dữ liệu) chênh lệch nhau quá lớn, một thành phần có khoảng giá trị từ **0** đến **1000**, thành phần kia chỉ có khoảng giá trị từ **0** đến **1** chẳng hạn. Lúc này, chúng ta cần chuẩn hóa dữ liệu trước khi thực hiện các bước tiếp theo.

**Rescaling**

Phương pháp đơn giản nhất là đưa tất cả các thành phần về cùng một khoảng, **[0,1]** hoặc **[-1,1]**. Nếu muốn đưa một thành phần (feature) về khoảng **[0,1]** công thức sẽ là:

Trong đó, **x** là giá trị ban đầu, **x’** là giá trị sau khi chuẩn hóa. **min(x), max(x)** được tính trên toàn bộ dữ liệu training data ở cùng một thành phần. Việc này được thực hiện trên từng thành phần của vector dữ liệu **x**.

*#thêm thư viện xử lý ma trận***import** numpy **as** np  
*#thư viện sklearn để lấy hàm min\_max\_scaler***from** sklearn **import** preprocessing  
*#Tạo một ma trận tên X\_Train*X\_train = np.array([[1.,-1.,2.],[2.,0.,0.],[0.,1.,-1.]])  
*#gán biến min\_max\_scaler từ hàm MinMaxScaler() cho khoảng [0,1]  
#gán biến max\_abs\_scaler từ hàm MaxAbsScaler() cho khoảng [-1,1]*min\_max\_scaler = preprocessing.MinMaxScaler()  
max\_abs\_scaler = preprocessing.MinMaxScaler()  
*#Thực hiện chuyển đổi về khoảng [0,1] và [-1,1] bằng hàm fit\_transform*X\_train\_minmax = min\_max\_scaler.fit\_transform(X\_train)  
X\_train\_maxabs = max\_abs\_scaler.fit\_transform(X\_train)  
*#in ra màn hình ma trận sau khi scaled!*print(**"Ma trận ban đầu:\n{}\n\nMa trận sau khi scaling:\nĐối với khoảng [0,1]:\n{}\n\n""Đối với khoảng [-1,1]:\n{}"** .format(X\_train,X\_train\_minmax,X\_train\_maxabs))

*Kết quả:*

Ma trận ban đầu:

[[ 1. -1. 2.]

[ 2. 0. 0.]

[ 0. 1. -1.]]

Ma trận sau khi scale:

Đối với khoảng [0,1]:

[[ 0.5 0. 1. ]

[ 1. 0.5 0.33333333]

[ 0. 1. 0. ]]

Đối với khoảng [-1,1]:

[[ 0.5 -1. 1. ]

[ 1. 0. 0. ]

[ 0. 1. -0.5]]

**Standardization**

Một phương pháp nữa cũng hay được sử dụng là giả sử mỗi thành phần đều có phân phối chuẩn với kỳ vọng là 0 và phương sai là 1. Khi đó, công thức chuẩn hóa sẽ là:

*Trong đó:* ***,***  *lần lượt là kỳ vọng và phương sai (standard deviation) của thành phần đó trên toàn bộ training data.*

*#thêm thư viện xử lý ma trận***import** numpy **as** np  
*#thư viện sklearn để lấy hàm min\_max\_scaler***from** sklearn **import** preprocessing  
*#Tạo một ma trận tên X\_Train*X\_train = np.array([[1.,-1.,2.],[2.,0.,0.],[0.,1.,-1.]])  
*#gán biến scaler từ hàm StandardScaler() sau khi fit ma trận*scaler = preprocessing.StandardScaler().fit(X\_train)  
print(**"Ma trận ban đầu:\n{}\n\nMa trận sau khi scaling:\n{}"** .format(X\_train,scaler.transform(X\_train)))

*Kết quả:*

Ma trận ban đầu:

[[ 1. -1. 2.]

[ 2. 0. 0.]

[ 0. 1. -1.]]

Ma trận sau khi scaling:

[[ 0. -1.22474487 1.33630621]

[ 1.22474487 0. -0.26726124]

[-1.22474487 1.22474487 -1.06904497]]

**Scaling to unit length**

Một lựa chọn khác nữa cũng được sử dụng rộng rãi là chuẩn hóa các thành phần của mỗi vector dữ liệu sao cho toàn bộ vector có độ lớn (Euclid, tức norm 2) bằng 1. Việc này có thể được thực hiện bằng:

* 1. Overfitting
     1. Giới thiệu

Overfitting là hiện tượng mô hình tìm được quá khớp với dữ liệu training. Việc quá khớp này có thể dẫn đến việc dự đoán nhầm nhiễu, và chất lượng mô hình không còn tốt trên dữ liệu test nữa. Dữ liệu test được giả sử là không được biết trước, và không được sử dụng để xây dựng các mô hình Machine Learning.

* + 1. Ví dụ

Có 50 điểm dữ liệu được tạo bằng một đa thức bậc ba cộng thêm nhiễu. Tập dữ liệu này được chia làm hai, 30 điểm dữ liệu màu đỏ cho training data, 20 điểm dữ liệu màu vàng cho test data. Đồ thị của đa thức bậc ba này được cho bởi đường màu xanh lá cây. Bài toán của chúng ta là giả sử ta không biết mô hình ban đầu mà chỉ biết các điểm dữ liệu, hãy tìm một mô hình “tốt” để mô tả dữ liệu đã cho.



Hình 2.5: Underfitting và Overfitting với Polynominal Regression

Bài toán này hoàn toàn có thể được giải quyết bằng Linear Regression với dữ liệu mở rộng cho một cặp điểm là với cho đa thức bậc . Điều quan trọng là chúng ta cần tìm bậc của đa thức cần tìm.

Trong ví dụ trên, độ phức tạp của mô hình có thể được coi là bậc của đa thức cần tìm. Rõ ràng là một đa thức bậc không vượt quá 29 có thể fit được hoàn toàn với 30 điểm trong training data. Chúng ta cùng xét vài giá trị . Với , mô hình không thực sự tốt vì mô hình dự đoán quá khác so với mô hình thực. Trong trường hợp này, ta nói mô hình bị ***underfitting***. Với, với các điểm dữ liệu trong khoảng của training data, mô hình dự đoán và mô hình thực là khá giống nhau. Tuy nhiên, về phía phải, đa thức bậc 8 cho kết quả hoàn toàn ngược với xu hướng của dữ liệu. Điều tương tự xảy ra trong trường hợp . Đa thức bậc 16 này quá fit dữ liệu trong khoảng đang xét, và quá fit, tức không được mượt trong khoảng dữ liệu training. Việc quá fit trong trường hợp bậc 16 không tốt vì mô hình đang cố gắng mô tả nhiễu hơn là dữ liệu. Hai trường hợp đa thức bậc cao này được gọi là Overfitting.

Về cơ bản, overfitting xảy ra khi mô hình quá phức tạp để mô phỏng training data. Điều này đặc biệt xảy ra khi lượng dữ liệu training quá nhỏ trong khi độ phức tạp của mô hình quá cao.

Một mô hình được coi là tốt **(*fit*)** nếu cả train error và test error đều thấp. Nếu train error thấp nhưng test error cao, ta nói mô hình bị ***overfitting***. Nếu train error cao và test error cao, ta nói mô hình bị ***underfitting***. Nếu train error cao nhưng test error thấp hiện tượng này phải rất may mắn mới xảy ra, hoặc có chỉ khi tập dữ liệu test quá nhỏ.

* + 1. Một số phương pháp tránh overfitting

**Validation/Hold-out**

Phương pháp đơn giản nhất là trích từ tập training data ra một tập con nhỏ và thực hiện việc đánh giá mô hình trên tập con nhỏ này. Tập con nhỏ được trích ra từ training set này được gọi là ***validation set***. Lúc này, training set là phần còn lại của training set ban đầu. Train error được tính trên training set mới này, và có một khái niệm nữa được định nghĩa tương tự như trên validation error, tức error được tính trên tập validation.

Với khái niệm này, ta tìm mô hình sao cho cả train eror và validation error đều nhỏ, qua đó có thể dự đoán được rằng test error cũng nhỏ. Phương pháp thường được sử dụng là sử dụng nhiều mô hình khác nhau. Mô hình nào cho validation error nhỏ nhất sẽ là mô hình tốt.

Thông thường, ta bắt đầu từ mô hình đơn giản, sau đó tăng dần độ phức tạp của mô hình. Tới khi nào validation error có chiều hướng tăng lên thì chọn mô hình ngay trước đó. Chú ý rằng mô hình càng phức tạp, train error có xu hướng càng nhỏ đi.

Hình dưới đây mô tả ví dụ phía trên với bậc của đa thức tăng từ 1 đến 8. Tập validation bao gồm 10 điểm được lấy ra từ tập training ban đầu.



Hình 2.6: Bậc của đa thức

Ta hãy tạm chỉ xét hai đường màu lam và đỏ, tương ứng với train error và validation error. Khi bậc của đa thức tăng lên, train error có xu hướng giảm. Điều này dễ hiểu vì đa thức bậc càng cao, dữ liệu càng được fit. Quan sát đường màu đỏ, khi bậc của đa thức là 3 hoặc 4 thì validation error thấp, sau đó tăng dần lên. Dựa vào validation error, ta có thể xác định được bậc cần chọn là 3 hoặc 4. Quan sát tiếp đường màu lục, tương ứng với test error, thật là trùng hợp, với bậc bằng 3 hoặc 4, test error cũng đạt giá trị nhỏ nhất, sau đó tăng dần lên. Vậy cách làm này ở đây đã tỏ ra hiệu quả.

Việc không sử dụng test data khi lựa chọn mô hình ở trên nhưng vẫn có được kết quả khả quan vì ta giả sử rằng validation data và test data có chung một đặc điểm nào đó. Và khi cả hai đều là unseen data, error trên hai tập này sẽ tương đối giống nhau.

**Cross-validation**

Trong nhiều trường hợp, chúng ta có rất hạn chế số lượng dữ liệu để xây dựng mô hình. Nếu lấy quá nhiều dữ liệu trong tập training ra làm dữ liệu validation, phần dữ liệu còn lại của tập training là không đủ để xây dựng mô hình. Lúc này, tập validation phải thật nhỏ để giữ được lượng dữ liệu cho training đủ lớn. Tuy nhiên, một vấn đề khác nảy sinh. Khi tập validation quá nhỏ, hiện tượng overfitting lại có thể xảy ra với tập training còn lại. Lúc này ta sẽ sử dụng ***cross-validation*** (kiểm định chéo).

Cross validation là một cải tiến của validation với lượng dữ liệu trong tập validation là nhỏ nhưng chất lượng mô hình được đánh giá trên nhiều tập validation khác nhau. Một cách thường đường sử dụng là chia tập training ra tập con không có phần tử chung, có kích thước gần bằng nhau. Tại mỗi lần kiểm thử, được gọi là run, một trong số tập con được lấy ra làm validata set. Mô hình sẽ được xây dựng dựa vào hợp của tập con còn lại. Mô hình cuối được xác định dựa trên trung bình của các train error và validation error. Cách làm này còn có tên gọi ***là k-fold cross validation***.

**Regularization**

Một nhược điểm lớn của cross-validation là số lượng training runs tỉ lệ thuận với . Điều đáng nói là mô hình polynomial như trên chỉ có một tham số cần xác định là bậc của đa thức. Trong các bài toán Machine Learning, lượng tham số cần xác định thường lớn hơn nhiều, và khoảng giá trị của mỗi tham số cũng rộng hơn nhiều, chưa kể đến việc có những tham số có thể là số thực. Như vậy, việc chỉ xây dựng một mô hình thôi cũng là đã rất phức tạp rồi. Có một cách giúp số mô hình cần huấn luyện giảm đi nhiều, thậm chí chỉ một mô hình. Cách này có tên gọi chung là ***regularization***.

Regularization, một cách cơ bản, là thay đổi mô hình một chút để tránh overfitting trong khi vẫn giữ được tính tổng quát của nó (tính tổng quát là tính mô tả được nhiều dữ liệu, trong cả tập training và test). Một cách cụ thể hơn, ta sẽ tìm cách di chuyển nghiệm của bài toán tối ưu hàm mất mát tới một điểm gần nó. Hướng di chuyển sẽ là hướng làm cho mô hình ít phức tạp hơn mặc dù giá trị của hàm mất mát có tăng lên một chút. Một kĩ thuật đơn giản là: **early stopping**.

**Early Stopping**

Trong nhiều bài toán Machine Learning, chúng ta cần sử dụng các thuật toán lặp để tìm ra nghiệm, ví dụ như Gradient Descent. Nhìn chung, hàm mất mát giảm dần khi số vòng lặp tăng lên. Early stopping tức dừng thuật toán trước khi hàm mất mát đạt giá trị quá nhỏ, giúp tránh overfitting. Một kỹ thuật thường được sử dụng là tách từ training set ra một tập validation set như trên. Sau một (hoặc một số, ví dụ 50) vòng lặp, ta tính cả train error và validation error, đến khi validation error có chiều hướng tăng lên thì dừng lại, và quay lại sử dụng mô hình tương ứng với điểm và validation error đạt giá trị nhỏ.



Hình 2.7: Mô hình được xác định tại vòng lặp mà validation error đạt giá trị nhỏ nhất

**Thêm số hạng vào hàm mất mát**

Kỹ thuật regularization phổ biến nhất là thêm vào hàm mất mát một số hạng nữa. Số hạng này thường dùng để đánh giá độ phức tạp của mô hình. Số hạng này càng lớn, thì mô hình càng phức tạp. Hàm mất mát mới này thường được gọi là regularized loss function, thường được định nghĩa như sau:

**Trong đó:**

* được dùng để ký hiệu các biến trong mô hình.
* ký hiệu cho hàm mất mát (loss function).
* là số hạng regularization.
* thường là một số dương để cân bằng giữa hai đại lượng ở vế phải.
  1. Multicollinearity (Đa cộng tuyến)
     1. Giới thiệu

Trong mô hình hồi quy (Linear Regression), nếu các biến độc lập có quan hệ chặt với nhau, các biến độc lập có mối quan hệ tuyến tính, nghĩa là các biến độc lập có tương quan chặt, mạnh với nhau thì sẽ có hiện tượng đa cộng tuyến, đó là hiện tượng các biến độc lập trong mô hình phụ thuộc lẫn nhau và thể hiện được dưới dạng hàm số. Ví dụ có hai biến độc lập A và B, khi A tăng thì B tăng, A giảm thì B giảm…. thì đó là một dấu hiệu của đa cộng tuyến. Nói một cách khác là hai biến độc lập có quan hệ rất mạnh với nhau, đúng ra hai biến này nó phải là 1 biến nhưng thực tế trong mô hình nhà nghiên cứu lại tách làm 2 biến. Hiện tượng đa cộng tuyến vi phạm giả định của mô hình hồi qui tuyến tính cổ điển là các biến độc lập không có mối quan hệ tuyến tính với nhau.

Đa cộng tuyến hoàn hảo:

|  |  |  |
| --- | --- | --- |
| X2 | X3 | X4 |
| 10 | 50 | 52 |
| 15 | 75 | 75 |
| 18 | 90 | 97 |
| 24 | 120 | 129 |

Bảng 2.1: Bảng số giờ học và kết quả

**Nhận Xét:** **X2** và **X3** có mối quan hệ tuyến tính chính xác: **X3** = 5**X2**

* + 1. Cách phát hiện trường hợp đa cộng tuyến

**Có 2 cách:**

* Dựa vào hệ số phóng đại phương sai VIF(Variance Inflation Factor).
* Dựa vào hệ số tương quan,có hay không tương quan tuyến tính mạnh giữa các biến độc lập. Cách làm: xây dựng ma trận hệ số tương quan cặp giữa các biến độc lập và quan sát để nhận diện độ mạnh của các tương quan giữa từng cặp biến số độc lập.
  + 1. Hệ quả của đa cộng tuyến:
* Không ước lượng được mô hình
* Gặp các cảnh báo trong khi xây dựng model
  + 1. Cách giải quyết đa cộng tuyến:

Cách 1: Principal Component Analysis (PCA), dùng kiến thức Eigenvector và Eigenvalue.



Hình 2.8: Cách thức hoạt động của PCA

Cách 2: Partial Least Square Regression (PLSQ)



Hình 2.9: Cách thức hoạt động của PLSQ

Chương 3:  
MỘT SỐ MÔ HÌNH MACHINE LEARNING

1. 1. Linear Regression/Ordinary least squares

Linear hay tuyến tính hiểu một cách đơn giản là thẳng, phẳng. Trong không gian hai chiều, một hàm số được gọi là tuyến tính nếu đồ thị của nó có dạng một đường thẳng. Trong không gian ba chiều, một hàm số được goi là tuyến tính nếu đồ thị của nó có dạng một mặt phẳng. Trong không gian nhiều hơn 3 chiều, khái niệm mặt phẳng không còn phù hợp nữa, thay vào đó, một khái niệm khác ra đời được gọi là siêu mặt phẳng (hyperplane). Các hàm số tuyến tính là các hàm đơn giản nhất, vì chúng thuận tiện trong việc hình dung và tính toán.

* + 1. Giới thiệu

Một căn nhà rộng  , có  phòng ngủ và cách trung tâm thành phố  **km** có giá là bao nhiêu. Giả sử chúng ta đã có số liệu thống kê từ 1000 căn nhà trong thành phố đó, liệu rằng khi có một căn nhà mới với các thông số về diện tích, số phòng ngủ và khoảng cách tới trung tâm, chúng ta có thể dự đoán được giá của căn nhà đó không? Nếu có thì hàm dự đoán  sẽ có dạng như thế nào. Ở đây  là một vector hàng chứa thông tin input,  là một số vô hướng (scalar) biểu diễn output (tức giá của căn nhà trong ví dụ này).

Một cách đơn giản nhất, chúng ta có thể thấy rằng:

* Diện tích nhà càng lớn thì giá nhà càng cao.
* Số lượng phòng ngủ càng lớn thì giá nhà càng cao.
* Càng xa trung tâm thì giá nhà càng giảm.

Một hàm số đơn giản nhất có thể mô tả mối quan hệ giữa giá nhà và 3 đại lượng đầu vào là:

Trong đó,  là các hằng số, còn được gọi là **bias tức hệ số tự do**. Mối quan hệ  bên trên là một mối quan hệ tuyến tính (*linear*). Bài toán chúng ta đang làm là một bài toán thuộc loại regression. Bài toán đi tìm các hệ số tối ưu chính vì vậy được gọi là bài toán Linear Regression.

* + 1. Dạng của Linear Regression

*Trong đó:*

* **w = {}** là vector (cột) cần phải tối ưu.
* là vector (hàng) dữ liệu đầu vào, số **1** được đặt ở đầu để phép tính đơn giản và thuận tiện hơn cho việc tính toán.
  + 1. Sai số dự đoán

Ta mong muốn rằng sự sai khác  giữa giá trị thực  và giá trị dự đoán là nhỏ nhất. Nói cách khác, chúng ta muốn giá trị sau đây càng nhỏ càng tốt:

**=**

Trong đó hệ số để thuận tiện cho việc tính toán (khi tính đạo hàm thì số sẽ bị triệt tiêu). Còn vì , việc ta lấy bình phương cũng là để thuận tiện trong việc đạo hàm.

* + 1. Hàm mất mát (Cost Function /Lost Function)

Điều tương tự xảy ra với tất cả các cặp (input, outcome) với **N** là số dữ liệu quan sát được. Điều chúng ta muốn, tổng sai số là nhỏ nhất, tương đương với việc tìm **w** để hàm số sau đạt giá trị nhỏ nhất:

Hàm số  được gọi là **hàm mất mát** (cost function/loss function) của bài toán Linear Regression. Chúng ta luôn mong muốn rằng sự mất mát (sai số) là nhỏ nhất, điều đó đồng nghĩa với việc tìm vector hệ số  sao cho giá trị của hàm mất mát này càng nhỏ càng tốt. Giá trị của  làm cho hàm mất mát đạt giá trị nhỏ nhất được gọi là điểm tối ưu (optimal point), ký hiệu:

Trước khi đi tìm lời giải, chúng ta đơn giản hóa phép toán trong phương trình hàm mất mát . Đặt là một vector cột chứa tất cả các output của training data. là ma trận dữ liệu đầu vào (mở rộng) mà mỗi hàng của nó là một điểm dữ liệu. Khi đó hàm số mất mát  được viết dưới dạng ma trận đơn giản hơn:

Với là Euclidean norm (chuẩn Euclid, hay khoảng cách Euclid), nói cách khác là tổng bình phương mỗi phần tử của vector z. Tới đây, ta đã có một mạng đơn giản của hàm mất mát được viết như phương trình .

* + 1. Nghiệm trên bài toán Linear Regression

Để tìm nghiệm cho bài toán tối ưu là giải phương trình đạo hàm (gradient) bằng **0**.

Đạo hàm theo của hàm mất mát là:

Phương trình đạo hàm bằng tương đương với:

*Ký hiệu tức là đặt bằng*

Nếu ma trận vuông khả nghịch (non-singular hay invertible) thì phương trình có nghiệm duy nhất: .

Nếu ma trận vuông không khả nghịch (có định thức bằng 0), thì phương trình vô nghiệm hoặc vô số nghiệm. Khi đó ta sẽ xử dụng khái niệm **pseudo inverse** (giả nghịch đảo)  **(A dagger)**. Là trường hợp tổng quát của nghịch đảo khi ma trận không khả nghịch, hoặc không vuông.

Với khái niệm giả nghịch đảo, điểm tối ưu bài toán Linear Regression có dạng:

* + 1. Ví dụ trên Python

Ta sẽ lấy ví dụ đơn giản về giải về việc giải bài toán Linear Regression trong Python. Ta cũng sẽ so sánh nghiệm của bài toán khi giải theo phương trình và nghiệm tìm được khi dùng thư viện ***scikit-learn*** của Python. Để đơn giản ta sẽ dữ liệu với đầu vào chỉ có 1 chiều (1 giá trị).

Bài toán dự đoán cân nặng của một bạn trong lớp ĐHCN1A dựa vào chiều cao của bạn ấy (Trên thực tế, tất nhiên là không, vì cân nặng còn phụ thuộc vào nhiều yếu tố khác nữa, thể tích chẳng hạn).

|  |  |  |
| --- | --- | --- |
| Họ và Tên | Chiều Cao | Cân Nặng |
| Trịnh Đình Phúc | 168 | 50 |
| Nguyễn Đình Thái | 169 | 55 |
| Nguyễn Đức Tiến | 180 | 62 |
| Trần Trung Hiếu | 176 | 64 |
| Trịnh Văn Bình | 161 | 53 |
| Lê Thị Hoài Thuận | 163 | 46 |
| Trần Thanh Phương | 172 | 65 |
| Lê Huy Hoàng | 170 | 58 |
| Bùi Lý Hải Đăng | 173 | 73 |
| Huỳnh Diệp Phụng | 163 | 55 |
| Lê Hùng Phú | 173 | 74 |
| Huỳnh Quốc Đạt | 169 | 52 |
| Phạm Hữu Danh | 172 | 71 |
| Nguyễn Duy Thanh Tùng | 172 | **?** |

Bảng 3.1: Bảng cân nặng và chiều cao lớp ĐHCN1A

Để kiểm tra độ chính xác của model tìm được, chúng ta sẽ giữ lại hàng tên “Nguyễn Duy Thanh Tùng” để kiểm thử, các hàng còn lại được sử dụng để huấn luyện (train) model.

**Hiển thị dữ liệu trên đồ thị:**

*#Trước tiên, chúng ta cần có hai thư viện numpy cho đại số tuyến tính và matplotlib cho việc vẽ hình.***import** numpy **as** np  
**import** matplotlib.pyplot **as** plt  
*# chiều cao (cm)*X = np.array([[168,169,180,176,161,163,172,170,173,163,173,169,172]]).T  
*# cân nặng (kg)*y = np.array([[ 50 ,55 ,62, 64, 53 , 46, 65, 58, 73, 55, 74, 52, 71]]).T  
*# Visualize data*plt.plot(X, y, **'ro'**)  
plt.axis([140, 190, 45, 75])  
plt.xlabel(**'Chiều cao (cm)'**)  
plt.ylabel(**'Cân nặng (kg)'**)  
plt.show()

*Kết quả:*



Hình 3.1: Hiển thị dữ liệu về chiều cao & cân nặng trên đồ thị

**Nghiệm theo công thức:**

Công thức: **Cân\_nặng =** **w\_1\*(chiều\_cao) + w\_0**

Tiếp theo, ta sẽ tính toán các hệ số **w\_1** và **w\_0** dựa vào công thức

*# xây dựng X feature & reshape*one = np.ones((X.shape[0], 1))  
Xbar = np.concatenate((one, X), axis = 1)  
*# tính các trọng số A,b,w*A = np.dot(Xbar.T, Xbar) *#np.dot tích trong 2 ma trận*b = np.dot(Xbar.T, y)  
w = np.dot(np.linalg.pinv(A), b) *#pseudo-inverse  
# chuẩn bị cho fitting line*w\_0 = w[0][0]  
w\_1 = w[1][0]  
x0 = np.linspace(145,190,2) *#chia ra 2 khoảng từ 145 đến 190 (vì chiều cao nằm trong khoảng đó)*y0 = w\_0 + w\_1\*x0  
print(**"Phương trình sau khi học được là: y ={}x {}"**.format(w\_1,w\_0))



Hình 3.2: Mô hình Linear Regression sau khi học xong

Nhận xét: từ đồ thị trên ta thấy đường màu xanh nằm khá gần với các đường màu đỏ, tức mô hình Linear Regression hoạt động tốt với tập dữ liệu training. Tiếp theo, ta sẽ dự đoán cân nặng của bạn “Nguyễn Duy Thanh Tùng”.

y1 = w\_1\*172 + w\_0  
print(**"Phương trình sau khi học được là: y ={}x {}"**.format(w\_1,w\_0))  
print( **u'Chiều cao của Thanh Tùng là 172, cân nặng dự đoán: %.2f (kg), cân nặng thực tế là: 60 (kg)'** %(y1) )

*Kết quả:*

Chiều cao của Thanh Tùng là 172, cân nặng dự đoán: 62.16 (kg), cân nặng thực tế là: 60 (kg)

Nhận xét: kết quả dự đoán tương đối chính xác.

* + 1. Hạn chế của Linear Regression

Hạn chế đầu tiên của Linear Regression là nó rất nhạy cảm với nhiễu (sensitive to noise). Trong ví dụ về mối quan hệ giữa chiều cao và cân nặng bên trên, nếu có chỉ một cặp dữ liệu nhiễu (155 cm, 80kg) thì kết quả sẽ sai khác đi rất nhiều. Xem hình dưới đây:



Hình 3.3: Ảnh hưởng của Outliers

Vì vậy, trước khi thực hiện Linear Regression, các nhiễu (outlier) cần phải được loại bỏ. Bước này được gọi là tiền xử lý (pre-processing).

Hạn chế thứ hai của Linear Regression là nó không biễu diễn được các mô hình phức tạp. Mặc dù trong phần trên, chúng ta thấy rằng phương pháp này có thể được áp dụng nếu quan hệ giữa outcome và input không nhất thiết phải là tuyến tính, nhưng mối quan hệ này vẫn đơn giản nhiều so với các mô hình thực tế, những mô hình có các hàm như **.**

* 1. Gradient Decent

Trong Machine Learning nói riêng và Toán Tối Ưu nói chung, ta thường xuyên phải tìm giá trị nhỏ nhất (hoặc đôi khi là lớn nhất) của một hàm số nào đó. Ví dụ như các hàm mất mát trong Linear Regression và K-means Clustering. Nhìn chung, việc tìm global minimum của các hàm mất mát trong Machine Learning là rất phức tạp, thậm chí là bất khả thi. Thay vào đó, người ta thường cố gắng tìm các điểm local minimum, và ở một mức độ nào đó, coi đó là nghiệm cần tìm của bài toán.



Hình 3.4: Biểu diễn các điểm local và global

Các điểm local minimum là nghiệm của phương trình đạo hàm bằng 0. Nếu bằng một cách nào đó có thể tìm được toàn bộ (hữu hạn) các điểm cực tiểu, ta chỉ cần thay từng điểm local minimum đó vào hàm số rồi tìm điểm làm cho hàm có giá trị nhỏ nhất. Tuy nhiên, trong hầu hết các trường hợp, việc giải phương trình đạo hàm bằng 0 là bất khả thi. Nguyên nhân có thể đến từ sự phức tạp của dạng của đạo hàm, từ việc các điểm dữ liệu có số chiều lớn, hoặc từ việc có quá nhiều điểm dữ liệu.

Hướng tiếp cận phổ biến nhất là xuất phát từ một điểm mà chúng ta coi là gần với nghiệm của bài toán, sau đó dùng một phép toán lặp để tiến dần đến điểm cần tìm, tức đến khi đạo hàm gần với 0. Gradient Descent (GD) – Đạo hàm ngược và các biến thể của nó là một trong những phương pháp được dùng nhiều nhất.

* + 1. Gradient Decent cho hàm một biến

****

Hình 3.5: Parapol của hàm f(x)

Giả sử là điểm ta tìm được sau vòng lặp **t**. Ta cần tìm một thuật toán để đưa về càng gần càng tốt.

Từ hình trên ta thấy: Nếu đạo hàm của hàm số tại thì nằm về bên phải so với (và ngược lại). Để điểm tiếp theo gần với hơn, chúng ta cần di chuyển về phía bên trái, tức về phía âm. Nói cách khác, ta cần di chuyển ngược dấu với đạo hàm

*Trong đó:*

* *là một đại lượng ngược dấu với đạo hàm*
* *càng xa về phía bên phải thì* *càng lớn hơn 0 (và ngược lại). Vậy, lượng di chuyển , một cách trực quan nhất, là tỉ lệ thuận với*

Từ 2 nhận xét trên cho ta một cách cập nhật đơn giản:

*Trong đó: (đọc là eta) là một số dương được gọi là learning rate (tốc độ học). Dấu trừ thể hiện việc chúng ta phải đi ngược với đạo hàm.*

**Ví dụ đơn giản với Python:**

Xét hàm số với đạo hàm  **2x + 5cos(x).** Giả sử bắt đầu từ một điểm nào đó, tại vòng lặp thứ **,** chúng ta sẽ cập nhật như sau:

Các hàm số:

* **Grad\_Fx** để tính đạo hàm
* **Cost** để tính giá trị của hàm số. Hàm này không sử dụng trong thuật toán nhưng thường được dùng để kiểm tra việc tính đạo hàm của đúng không hoặc để xem giá trị của hàm số có giảm theo mỗi vòng lặp hay không.
* Hàm **Gradient\_Decent** là phần chính thực hiện thuật toán Gradient Desent nêu phía trên. Đầu vào của hàm số này là learning rate () và điểm bắt đầu. Thuật toán dừng lại khi đạo hàm có độ lớn đủ nhỏ

Các điểm khởi tạo khác nhau là và

**import** numpy **as** np  
  
**def** grad\_Fx(x):  
 **return** 2\*x+ 5\*np.cos(x)**def** cost(x):  
 **return** x\*\*2 + 5\*np.sin(x)  
**def** Gradient\_Decent(eta, x0):  
 x = [x0]  
 **for** it **in** range(100):  
 x\_new = x[-1] - eta\*grad\_Fx(x[-1])  
 **if** abs(grad\_Fx(x\_new)) < 1e-3: *#Thuật toán dừng lại khi đạo hàm có độ lớn đủ nhỏ (0.001)* **break** x.append(x\_new)  
 **return** (x, it)  
(x1, it1) = Gradient\_Decent(.1, -5) *# đầu vào, learning rate = 0.1, điểm bắt đầu bằng -5*(x2, it2) = Gradient\_Decent(.1, 5) *# đầu vào, learning rate = 0.1, điểm bắt đầu bằng 5*print(**'với x1 = %f, cost = %f, hội tụ sau %d bước lặp'**%(x1[-1], cost(x1[-1]), it1))  
print(**'với x2 = %f, cost = %f, hội tụ sau %d bước lặp'**%(x2[-1], cost(x2[-1]), it2))

*Kết quả:*

với x1 = -1.110667, cost = -3.246394, hội tụ sau 11 bước lặp

với x2 = -1.110341, cost = -3.246394, hội tụ sau 29 bước lặp

**Vậy là với các điểm ban đầu khác nhau, thuật toán của chúng ta tìm được nghiệm gần giống nhau, mặc dù với tốc độ hội tụ khác nhau. Dưới đây là hình ảnh minh họa thuật toán GD cho bài toán này.

Hình 3.6: Minh họa thuật toán Gradient Decent – Bước 1

Hình 3.7: Minh họa thuật toán Gradient Decent – Bước 2





Hình 3.8: Minh họa thuật toán Gradient Decent – Bước 3



Hình 3.9: Minh họa thuật toán Gradient Decent – Bước 4

Hình 3.10: Minh họa thuật toán Gradient Decent – Bước 5

Từ hình minh họa trên ta thấy rằng ở hình bên trái, tương ứng với , nghiệm hội tụ nhanh hơn, vì điểm ban đầu gần với nghiệm hơn. Hơn nữa, với ở hình bên phải, đường đi của nghiệm có chứa một khu vực có đạo hàm khá nhỏ gần điểm có hoành độ bằng 2. Điều này khiến cho thuật toán “la cà” ở đây khá lâu. Khi vượt qua được điểm này thì mọi việc diễn ra rất tốt đẹp.

Nhận xét:

* Với các điểm ban đầu khác nhau, thuật toán tìm được nghiệm gần giống nhau, mặc dù với tốc độ hội tụ khác nhau.
* Tốc độ hội tụ của GD không những phụ thuộc vào điểm khởi tạo ban đầu mà còn phụ thuộc vào learning rate.

Việc lựa chọn learning rate rất quan trọng trong các bài toán thực tế. Việc lựa chọn giá trị này phụ thuộc nhiều vào từng bài toán và phải làm một vài thí nghiệm để chọn ra giá trị tốt nhất. Ngoài ra, tùy vào một số bài toán, GD có thể làm việc hiệu quả hơn bằng cách chọn ra learning rate phù hợp hoặc chọn learning rate khác nhau ở mỗi vòng lặp

* + 1. Gradient Decent cho hàm nhiều biến

Giả sử ta cần tìm global minimum cho hàm trong đó **θ** (theta) là một vector, thường được dùng để ký hiệu tập hợp các tham số của một mô hình cần tối ưu (trong Linear Regression thì các tham số chính là hệ số). Đạo hàm của hàm số đó tại một điểm **θ** bất kỳ được ký hiệu là (hình tam giác ngược đọc là *nabla*). Tương tự như hàm 1 biến, thuật toán GD cho hàm nhiều biến cũng bắt đầu bằng một điểm dự đoán **,** sau đó, ở vòng lặp thứ , quy tắc cập nhật là:

* + 1. Stopping Criteria (điều kiện dừng)

Khi nào thì chúng ta biết thuật toán đã hội tụ và dừng lại?

Trong thực nghiệm, có một vài phương pháp như dưới đây:

* Giới hạn số vòng lặp: đây là phương pháp phổ biến nhất và cũng để đảm bảo rằng chương trình chạy không quá lâu. Tuy nhiên, một nhược điểm của cách làm này là có thể thuật toán dừng lại trước khi đủ gần với nghiệm.
* So sánh gradient của nghiệm tại hai lần cập nhật liên tiếp, khi nào giá trị này đủ nhỏ thì dừng lại. Phương pháp này cũng có một nhược điểm lớn là việc tính đạo hàm đôi khi trở nên quá phức tạp (ví dụ như khi có quá nhiều dữ liệu).
* So sánh giá trị của hàm mất mát của nghiệm tại hai lần cập nhật liên tiếp, khi nào giá trị này đủ nhỏ thì dừng lại. Nhược điểm của phương pháp này là nếu tại một thời điểm, đồ thị hàm số có dạng bẳng phẳng tại một khu vực nhưng khu vực đó không chứa điểm local minimum (khu vực này thường được gọi là saddle points), thuật toán cũng dừng lại trước khi đạt giá trị mong muốn.
* Trong SGD và mini-batch GD, cách thường dùng là so sánh nghiệm sau một vài lần cập nhật.
  + 1. Biến thể của Gradient Descent
       1. Batch Gradient Descent

Thuật toán Gradient Descent còn được gọi là Batch Gradient Descent. Batch ở đây được hiểu là tất cả, tức khi cập nhật , chúng ta sử dụng tất cả các điểm dữ liệu .

Cách làm này có một vài hạn chế đối với cơ sở dữ liệu quá lớn. Việc phải tính toán lại đạo hàm với tất cả các điểm này sau mỗi vòng lặp trở nên cồng kềnh và không hiệu quả.

* + - 1. Stochastic Gradient Descent(SGD)

Trong thuật toán này, tại 1 thời điểm, ta chỉ tính đạo hàm của hàm mất mát dựa trên chỉ một điểm dữ liệu rồi cập nhật dựa trên đạo hàm này. Việc này được thực hiện với từng điểm trên toàn bộ dữ liệu, sau đó lặp lại quá trình trên. Thuật toán rất đơn giản này trên thực tế lại làm việc rất hiệu quả.

Mỗi lần duyệt một lượt qua tất cả các điểm trên toàn bộ dữ liệu được gọi là một epoch. Với GD thông thường thì mỗi epoch ứng với 1 lần cập nhật . Với SGD thì mỗi epoch ứng với lần cập nhật với lần cập nhật với là số điểm dữ liệu. Nhìn vào một mặt, việc cập nhật từng điểm một như thế này có thể làm giảm đi tốc độ thực hiện 1 epoch. Nhưng nhìn vào một mặt khác, SGD chỉ yêu cầu một lượng epoch rất nhỏ (thường là 10 cho lần đầu tiên, sau đó khi có dữ liệu mới thì chỉ cần chạy dưới một epoch là đã có nghiệm tốt). Vì vậy SGD phù hợp với các bài toán có lượng cơ sở dữ liệu lớn và các bài toán yêu cầu mô hình thay đổi liên tục, tức online learning.

* + 1. Thứ tự lựa chọn điểm dữ liệu

Một điểm cần lưu ý đó là: sau mỗi epoch, ta cần shuffle (xáo trộn) thứ tự của các dữ liệu để đảm bảo tính ngẫu nhiên. Việc này cũng ảnh hưởng tới hiệu năng của SGD.

Một cách toán học, quy tắc cập nhật của SGD là:

*Trong đó: là hàm mất mát với chỉ 1 cặp điểm dữ liệu (input, label) là .*

* 1. K-Means
     1. Giới thiệu

Trong thuật toán K-means clustering, chúng ta không biết nhãn (label) của từng điểm dữ liệu. Mục đích là làm thể nào để phân dữ liệu thành các cụm (cluster) khác nhau sao cho dữ liệu trong cùng một cụm có tính chất giống nhau.

* + 1. Ví dụ

Một công ty muốn tạo ra những chính sách ưu đãi cho những nhóm khách hàng khác nhau dựa trên sự tương tác giữa mỗi khách hàng với công ty đó (số năm là khách hàng, số tiền khách hàng đã chi trả cho công ty, độ tuổi, giới tính, thành phố, nghề nghiệp,…). Giả sử công ty đó có rất nhiều dữ liệu của rất nhiều khách hàng nhưng chưa có cách nào chia toàn bộ khách hàng đó thành một số nhóm/cụm khác nhau. Lúc đó ta có thể sử dụng các phương pháp phân cụm, ví dụ như K-means.

Ý tưởng đơn giản nhất về cluster (cụm) là tập hợp các điểm ở gần nhau trong một không gian nào đó (không gian này có thể có rất nhiều chiều trong trường hợp thông tin về một điểm dữ liệu là rất lớn). Hình bên dưới là một ví dụ về 3 cụm dữ liệu.



Hình 3.11: Bài toán phân cụm với 3 cluster

Giả sử mỗi cluster có một điểm đại diện (center) màu vàng. Và những điểm xung quanh mỗi center thuộc vào cùng nhóm với center đó. Một cách đơn giản nhất, xét một điểm bất kỳ, ta xét xem điểm đó gần với center nào nhất thì nó thuộc về cùng nhóm với center đó.

* + 1. Phân tích mặt toán học

Giả sử có điểm dữ liệu là và là số cluster chúng ta muốn phân chia. Chúng ta cần tìm các center và label của mỗi điểm dữ liệu.

Với mỗi điểm dữ liệu đặt là label vector của nó, trong đó nếu được phân vào cluster thì và . Điều này có nghĩa là có đúng một phần tử của vector là bằng 1 (tương ứng với cluster của) các phần tử còn lại bằng 0. Ví dụ: nếu một điểm dữ liệu có label vector là thì nó thuộc vào cluster 1, là thì nó thuộc vào cluster 2,...Cách mã hóa label của dữ liệu như thế này được gọi là biểu diễn **one-hot-encoding**.

Ràng buộc của có thể viết dưới dạng toán học như sau:

* + 1. Thuật toán

**Đầu vào:** Dữ liệu  và số lượng cluster cần tìm .

**Đầu ra:** Các center và label vector cho từng điểm dữ liệu .

1. Chọn điểm bất kỳ làm các ***center*** ban đầu.
2. Phân mỗi điểm dữ liệu vào ***cluster*** có ***center*** gần nó nhất.
3. Nếu việc gán dữ liệu vào từng cluster ở bước 2 không thay đổi so với vòng lặp trước nó thì ta dừng thuật toán.
4. Cập nhật ***center*** cho từng ***cluster*** bằng cách lấy trung bình cộng của tất các các điểm dữ liệu đã được gán vào ***cluster*** đó sau bước 2.
5. Quay lại bước 2.
   * 1. Hàm mất mát và bài toán tối ưu

Nếu ta coi center là center (hoặc representative) của mỗi cluster và ước lượng tất cả các điểm được phân vào cluster này bởi thì một điểm dữ liệu được phân vào cluster sẽ bị sai số là **( )**. Chúng ta mong muốn sai số này có giá trị tuyệt đối nhỏ nhất nên sai số này có giá trị tuyệt đối nhỏ nhất nên ta sẽ tìm cách để đại lượng sau có giá trị nhỏ nhất:

Hơn nữa, vì được phân vào cluster nên . Khi đó, biểu thức bên trên sẽ được viết lại là:

Sai số cho toàn dữ liệu sẽ là:

*Trong đó,* *lần lượt là các ma trận được tạo bởi label vector của mỗi điểm dữ liệu và center của mỗi cluster. là hàm số mất mát với ràng buộc như trong phương trình .*

Tóm lại, chúng ta cần tối ưu bài toán sau:

* + 1. Thuật toán tối ưu hàm mất mát

Một cách đơn giản để giải bài toán là xen kẽ giải và khi biến còn lại được cố định. Đây là một thuật toán lặp, cũng là kỹ thuật phổ biến khi giải bài toán tối ưu. Ta sẽ lần lượt giải quyết hai bài toán sau đây:

* + - 1. Cố định M, tìm Y

Giả sử đã tìm được cluster cho từng điểm, hãy tìm center mới cho mỗi cluster để hàm mất mát đạt giá trị nhỏ nhất.

Một khi chúng ta đã xác định được label vector cho từng điểm dữ liệu, bài toán tìm center cho mỗi cluster được rút gọn thành:

**=**

Chỉ có một phần tử của vector label bằng 1 nên bài toán **(7)** có thể tiếp tục viết dưới dạng đơn giản hơn:

Vì chính là bình phương khoảng cách tính từ điểm tới center , ta có thể kết luận rằng mỗi điểm thuộc vào cluster có center gần nó nhất. Từ đó ta có thể dễ dàng suy ra label vector của từng điểm dữ liệu.

* + - 1. Cố định Y, tìm M

Giá sử ta đã xác định được label vector vector cho từng điểm dữ liệu, bài toán tìm center cho mỗi cluster được rút gọn lại thành:

Tới đây, ta có thể tìm nghiệm bằng phương pháp giải đạo hàm bằng 0, vì hàm cần tối ưu là một hàm liên tục và có đạo hàm xác định tại mọi điểm. Và quan trọng hơn, hàm này là hàm convex (lồi) theo nên chúng ta sẽ tìm được giá trị nhỏ nhất và điểm tối ưu tương ứng.

Đặt là hàm bên trong dấu , ta có đạo hàm:

Giải phương trình đạo hàm bằng 0 ta có:

Ta thấy là trung bình cộng của các điểm trong cluster

* 1. Logistic Regression
     1. Giới thiệu

Mục tiêu của hồi qui Logistic là nghiên cứu mối tương quan giữa một (hay nhiều) yếu tố nguy cơ (risk factor) và đối tượng phân tích (outcome). Chẳn hạn như đối với nghiên cứu mối tương quan giữa thói quen hút thuốc lá và nguy cơ mắc ung thư phổi thì yếu tố nguy cơ ở đây là thói quen hút thuốc lá và đối tượng phân tích ở đây là nguy cơ mắc ung thư phổi. Trong hồi qui logistic thì các đối tượng nghiên cứu thường được thể hiện qua các biến số nhị phân (binary) như xảy ra/ không xảy ra ; chết/sống ; có/không,… còn các yếu tố nguy cơ có thể được thể hiện qua các biến số liên tục (tuổi, huyết áp,…) hoặc các biến nhị phân (giới tính) hay các biến thứ bậc (thu nhập : cao, trung bình, thấp).

* + 1. Ví dụ

Một nhóm 20 sinh viên dành thời gian trong khoảng từ 0 đến 6 giờ cho việc ôn thi. Thời gian ôn thi này ảnh hưởng đến xác suất sinh viên vượt qua kỳ thi như thế nào?

Kết quả thu được như sau:

|  |  |  |  |
| --- | --- | --- | --- |
| Số giờ học | Kết quả | Số giờ học | Kết quả |
| 0.5 | 0 | 2.75 | 1 |
| 0.75 | 0 | 3 | 0 |
| 1 | 0 | 3.25 | 1 |
| 1.25 | 0 | 3.5 | 0 |
| 1.5 | 0 | 4 | 1 |
| 1.75 | 0 | 4.25 | 1 |
| 1.75 | 1 | 4.5 | 1 |
| 2 | 0 | 4.75 | 1 |
| 2.25 | 1 | 5 | 1 |
| 2.5 | 0 | 5.5 | 1 |

Bảng 3.2: Bảng số giờ học và kết quả

Mặc dù có một chút bất công khi học 3.5 giờ thì trượt, còn học 1.75 giờ thì lại đỗ, nhìn chung, học càng nhiều thì khả năng đỗ càng cao.

Biểu diễn các điểm này trên đồ thị:

Hình 3.12: Kết quả thi dựa trên số giờ học

* + 1. Mô hình Logistic Regression

Đầu ra dự đoán của logistic regression thường được viết chung dưới dạng:

*Trong đó: được gọi là logistic function. Một số activation cho mô hình tuyến tính được cho trong hình dưới đây:*



Hình 3.13: Một số loại Activation Function

* **Đường màu vàng**:

Biểu diễn linear regression. Đường này không bị chặn nên không phù hợp cho bài toán này. Khi áp dụng mô hình linear regression như hình dưới đây và lấy mốc 0.5 để phân lớp, toàn bộ sinh viên thi trượt vẫn được dự đoán là trượt, nhưng rất nhiều sinh viên thi đỗ cũng được dự đoán là trượt (nếu ta coi điểm x màu xanh lục là ngưỡng cứng để đưa ra kết luận). Rõ ràng đây là một mô hình không tốt.



Hình 3.14: Mô tả Linear Regression không phù hợp

* **Đường màu đỏ:**

Rõ ràng là khi sử dụng ngưỡng cứng ở đây vì dữ liệu ở đây không tách biệt tuyến tính (linearly separable).

* **Các đường màu xanh:**

Hai đường màu xanh lá và xanh dương hợp với bài toán của ta hơn, chúng có 1 vài tính chất quan trọng sau:

* + Là hàm số liên tục nhận giá trị thực, bị chặn trong khoảng .
  + Nếu coi điểm có tung độ là 1/2 làm điểm phân chia thì các điểm càng xa điểm này về phía bên trái có giá trị càng gần 0. Ngược lại, các điểm càng xa điểm này về phía phải có giá trị càng gần 1. Điều này khớp với nhận xét rằng học càng nhiều thì xác suất đỗ càng cao và ngược lại.
  + Mượt (smooth) nên có đạo hàm mọi nơi, có thể được lợi trong việc tối ưu.
    1. Sigmoid Function

Đây là hàm được sử dụng nhiều nhất, vì nó bị chặn trong khoảng .

* + 1. Tanh Function (Hyperpolic Tangent)

Hàm số này nhận giá trị trong khoảng **,** với khoảng hàm có dạng:

* 1. Artificial Neural Network (ANN)
     1. Kiến trúc tổng quát của một ANN

Mạng Neuron nhân tạo (Artificial Neural Network- ***ANN***) là mô hình xử lý thông tin được mô phỏng dựa trên hoạt động của hệ thống thần kinh của sinh vật, bao gồm số lượng lớn các Neuron được gắn kết để xử lý thông tin. ANN giống như bộ não con người, được học bởi kinh nghiệm (thông qua huấn luyện), có khả năng lưu giữ những kinh nghiệm hiểu biết (tri thức) và sử dụng những tri thức đó trong việc dự đoán các dữ liệu chưa biết (unseen data).

Hình 3.15: Kiến trúc tổng quát của một mạng Neuron nhân tạo

Processing Elements (PE): Các PE của ANN gọi là Neuron, mỗi Neuron nhận các dữ liệu vào (Inputs) xử lý chúng và cho ra một kết quả (output) duy nhất. Kết quả xử lý của một Neuron có thể làm Input cho các Neuron khác

Kiến trúc chung của một ANN gồm 3 thành phần đó là Input Layer, Hidden Layer và Output Layer.

Trong đó, lớp ẩn (Hidden Layer) gồm các Neuron, nhận dữ liệu input từ các Neuron ở lớp (Layer) trước đó và chuyển đổi các input này cho các lớp xử lý tiếp theo. Trong một ANN có thể có nhiều Hidden Layer.

* + 1. Quá trình xử lý thông tin của một ANN

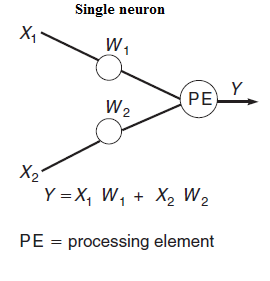
Hình 3.16: Quá trình xử lý thông tin của một ANN

**Inputs**: Mỗi Input tương ứng với 1 thuộc tính (attribute) của dữ liệu (patterns).

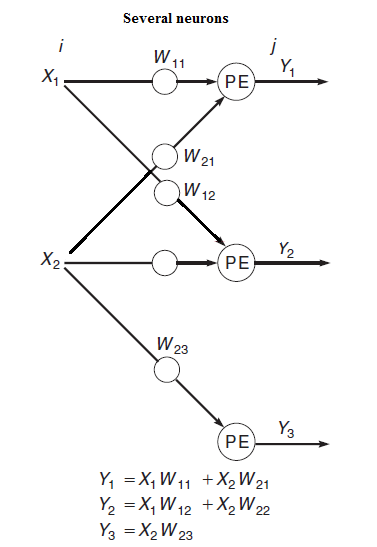
**Output**: Kết quả của một ANN là một giải pháp cho một vấn đề.

**Connection Weights** (Trọng số liên kết) : Đây là thành phần rất quan trọng của một ANN, nó thể hiện mức độ quan trọng (độ mạnh) của dữ liệu đầu vào đối với quá trình xử lý thông tin (quá trình chuyển đổi dữ liệu từ Layer này sang layer khác). Quá trình học (Learning Processing) của ANN thực ra là quá trình điều chỉnh các trọng số (Weight) của các input data để có được kết quả mong muốn.

**Summation Function** (Hàm tổng): Tính tổng trọng số của tất cả các input được đưa vào mỗi Neuron (phần tử xử lý PE). Hàm tổng của một Neuron đối với **n** input được tính theo công thức sau:



Hình 3.17: Hàm tổng của một neuron



Hình 3.18: Hàm tổng của nhiều neuron

* + 1. Transfer function

Hàm tổng (Summation Function) của một Neuron cho biết khả năng kích hoạt (Activation) của neuron đó còn gọi là internal activation. Các Neuron này có thể sinh ra một output hoặc không trong ANN (nói cách khác rằng có thể output của 1 Neuron có thể được chuyển đến layer tiếp trong mạng Neuron theo hoặc không). Mối quan hệ giữa Internal Activation và output được thể hiện bằng hàm chuyển đổi (Transfer Function).



Hình 3.19: Hàm chuyển đổi giữa internal activation và output

Việc lựa chọn Transfer Function có tác động lớn đến kết quả của ANN. Hàm chuyển đổi phi tuyến được sử dụng phổ biến trong ANN là sigmoid (logical activation) function.

*Trong đó:*

* *: hàm chuyển đổi*
* *: hàm tổng*

Kết quả xử lý tại các Neuron (Output) đôi khi rất lớn, vì vậy transfer function được sử dụng để xử lý output này trước khi chuyển đến layer tiếp theo. Đôi khi thay vì sử dụng Transfer Function người ta sử dụng giá trị ngưỡng (Threshold value) để kiểm soát các output của các neuron tại một layer nào đó trước khi chuyển các output này đến các Layer tiếp theo. Nếu output của một neuron nào đó nhỏ hơn Threshold thì nó sẻ không được chuyển đến Layer tiếp theo.

* + 1. Quá trình học (Learning Processing) của ANN

Supervised learning: Quá trình Training được lặp lại cho đến kết quả (output) của ANN đạt được giá trị mong muốn (Desired value) đã biết. Điển hình cho kỹ thuật này là mạng Neuron lan truyền ngược (Backpropagation).



Hình 3.20: Quá trình học của ANN

1. Tính giá trị output .
2. So sánh output với giá trị mong muốn (desired value).
3. Nếu chưa đạt được giá trị mong muốn thì hiệu chỉnh trọng số (weights) và tính lại output
   * 1. Nguyên tắc huấn luyện (Training Protocols)

Mạng Neuron có 3 cách huấn luyện chính đó là batch training, stochastic training và on-line training. Đối với on-line training thì các trọng số của mạng (weights) được cập nhật ngay lập tức sau khi một input pattern được đưa vào mạng. Stohastic training cũng giống như on-line training nhưng việc chọn các input patterns để đưa vào mạng từ training set được thực hiện ngẫu nhiên (random). Batch training thì tất cả các input patterns được đưa vào mạng cùng lúc và sau đó cập nhật các trọng số mạng đồng thời. Ưu điểm của on-line training là tiết kiệm bộ nhớ vì không cần lưu lại số lượng lớn các input patterns trong bộ nhớ.

Trong quá trình huấn luyện mạng, thuật ngữ “epoch” được dùng để mô tả quá trình khi tất cả các input patterns của training set được đưa để huấn luyện mạng. Nói cách khách 1 epoch được hoàn thành khi tất cả các dữ liệu trong training set được đưa vào huấn luyện mạng. Vì vậy số lượng “epoch” xác định số lần mạng được huấn luyện (hay số lần đưa tất cả các dữ liệu trong training set vào mạng).

Chương 4:  
ĐÁNH GIÁ MÔ HÌNH (MODEL EVALUATION)

* 1. Giới Thiệu

Khi xây dựng một mô hình Machine Learning, chúng ta cần một phép đánh giá để xem mô hình sử dụng có hiệu quả không và để so sánh khả năng của các mô hình. Có rất nhiều cách đánh giá một mô hình phân lớp. Tuỳ vào những bài toán khác nhau mà chúng ta sử dụng các phương pháp khác nhau. Các phương pháp thường được sử dụng là: Accuracy score, Confusion matrix, ROC curve, Area Under the Curve, Precision and Recall, F1 score.

* 1. Accuracy

Cách đơn giản và hay được sử dụng nhất là accuracy (độ chính xác). Cách đánh giá này đơn giản tính tỉ lệ giữa số điểm được dự đoán đúng và tổng số điểm trong tập dữ liệu kiểm thử.

* 1. Confusion Matrix (CM)

Cách tính sử dụng Accuracy như ở trên chỉ cho chúng ta biết được bao nhiêu phần trăm lượng dữ liệu được phân loại đúng mà không chỉ ra được cụ thể mỗi loại được phân loại như thế nào, lớp nào được phân loại đúng nhiều nhất, và dữ liệu thuộc lớp nào thường bị phân loại nhầm vào lớp khác. Để có thể đánh giá được các giá trị này, chúng ta sử dụng một ma trận được gọi là confusion matrix.

Về cơ bản, confusion matrix thể hiện có bao nhiêu điểm dữ liệu thực sự thuộc vào một class, và được dự đoán là rơi vào một class. Để hiểu rõ hơn, hãy xem bảng dưới đây:



Bảng 4.1: Bảng Confusion Matrix

Có tổng cộng 165 điểm dữ liệu. Chúng ta xét ma trận tạo bởi các giá trị tại vùng 2x2 trung tâm của bảng. Ma trận thu được được gọi là Confusion Matrix. Nó là một ma trận vuông với kích thước mỗi chiều bằng số lượng lớp dữ liệu. Giá trị tại hàng thứ i, cột thứ j là số lượng điểm lẽ ra thuộc vào class i nhưng lại được dự đoán là thuộc vào class j. Như vậy, nhìn vào hàng thứ nhất (0), ta có thể thấy được rằng trong số 60 điểm thực sự thuộc lớp 0, chỉ có một điểm được phân loại đúng, điểm còn lại bị phân loại nhầm vào lớp 1.

Chúng ta có thể suy ra ngay rằng tổng các phần tử trong toàn ma trận này chính là số điểm trong tập kiểm thử. Các phần tử trên đường chéo của ma trận là số điểm được phân loại đúng của mỗi lớp dữ liệu. Từ đây có thể suy ra accuracy chính bằng tổng các phần tử trên đường chéo chia cho tổng các phần tử của toàn ma trận. Đoạn code dưới đây mô tả cách tính confusion matrix:

**import** numpy **as** np  
**def** confusion\_matrix(y\_true,y\_pred): *# xây dựng hàm tính ma trận* N= np.unique(y\_true).shape[0] *#tính số lớp của ma trận* cm = np.zeros((N,N)) *#khởi tạo ma trận 0 NxN lớp* **for** i **in** range(y\_true.shape[0]): *# lấy từng phần tử trong ma trận y\_true* cm[y\_true[i],y\_pred[i]] +=1  
 **return** cm  
  
y\_true = np.array([0, 0, 0, 0, 1, 1, 1, 2, 2, 2])  
y\_pred = np.array([0, 1, 0, 2, 1, 1, 0, 2, 1, 2])  
cnf\_matrix = confusion\_matrix(y\_true, y\_pred) *#gọi hàm*print(**'Confusion matrix là :'**)  
print(cnf\_matrix)  
*#Độ chính xác Accuracy được tính bằng tổng các thành phần trên đường chéo chính chia cho tổng các thành phần trên ma trận*print(**'\nĐộ chính xác Accuracy: {}%'**.format(int(np.diagonal(cnf\_matrix).sum()/cnf\_matrix.sum()\*100)))

*Kết quả:*

Confusion matrix là:

[[ 2. 1. 1.]

[ 1. 2. 0.]

[ 0. 1. 2.]]

Độ chính xác Accuracy: 60%

Cách biểu diễn trên đây của confusion matrix còn được gọi là unnormalized confusion matrix, tức CM chưa chuẩn hoá. Để có cái nhìn rõ hơn, ta có thể dùng normalized confuion matrix, tức CM được chuẩn hoá. Để có normalized confusion matrix, ta lấy mỗi hàng của unnormalized confusion matrix sẽ được chia cho tổng các phần tử trên hàng đó. Như vậy, ta có nhận xét rằng tổng các phần tử trên một hàng của normalized confusion matrix luôn bằng 1. Điều này thường không đúng trên mỗi cột. Dưới đây là cách tính normalized confusion matrix:

normalized\_confusion\_matrix = cnf\_matrix/cnf\_matrix.sum(axis=1,keepdims=**True**)  
print(**"Normalized confusion matrix là:\n {}"**.format(normalized\_confusion\_matrix))

*Kết quả:*

Normalized confusion matrix là:

[[ 0.5 0.25 0.25 ]

[ 0.33333333 0.66666667 0. ]

[ 0. 0.33333333 0.66666667]]

* 1. True/False Positive/Negative

Cách đánh giá này thường được áp dụng cho các bài toán phân lớp có hai lớp dữ liệu. Cụ thể hơn, trong hai lớp dữ liệu này có một lớp nghiêm trọng hơn lớp kia và cần được dự đoán chính xác. Ví dụ, trong bài toán xác định có bệnh ung thư hay không thì việc không bị sót (miss) quan trọng hơn là việc chẩn đoán nhầm âm tính thành dương tính. Trong bài toán xác định có mìn dưới lòng đất hay không thì việc bỏ sót nghiêm trọng hơn việc báo động nhầm rất nhiều. Hay trong bài toán lọc email rác thì việc cho nhầm email quan trọng vào thùng rác nghiêm trọng hơn việc xác định một email rác là email thường.

Trong những bài toán này, người ta thường định nghĩa lớp dữ liệu quan trọng hơn cần được xác định đúng là lớp Positive (P-dương tính), lớp còn lại được gọi là Negative (N-âm tính). Ta định nghĩa True Positive (TP), False Positive (FP), True Negative (TN), False Negative (FN) dựa trên confusion matrix chưa chuẩn hoá như sau:

|  |  |  |
| --- | --- | --- |
|  | Predicted as Positive | Predicted as Negative |
| Actual: Positive | True Positive (TP) | False Negative (FN) |
| Actual: Negative | False Positive (FP) | True Negative (TN) |

Bảng 4.2: Bảng True/False Positive/Negative

Người ta thường quan tâm đến **TPR, FNR, FPR, TNR** (R - Rate) dựa trên normalized confusion matrix như sau:

|  |  |  |
| --- | --- | --- |
|  | Predicted as Positive | Predicted as Negative |
| Actual: Positive | TPR = TP/(TP + FN) | FNR = FN/(TP + FN) |
| Actual: Negative | FPR = FP/(FP + TN) | TNR = TN/(FP + TN) |

Bảng 4.3: Bảng Normalized Confusion Matrix

**False Positive Rate** còn được gọi là **False Alarm Rate** (tỉ lệ báo động nhầm), **False Negative Rate** còn được gọi là **Miss Detection Rate** (tỉ lệ bỏ sót). Trong bài toán dò mìn, thà báo nhầm còn hơn bỏ sót, tức là ta có thể chấp nhận **False Alarm Rate** cao để đạt được **Miss Detection Rate** thấp.

**Chú ý:**

* Việc biết một cột của **confusion matrix** này sẽ suy ra được cột còn lại vì tổng các hàng luôn bằng 1 và chỉ có hai lớp dữ liệu.
* Với các bài toán có nhiều lớp dữ liệu, ta có thể xây dựng bảng **True/False Positive/Negative** cho mỗi lớp nếu coi lớp đó là lớp Positive, các lớp còn lại gộp chung thành lớp Negative.
  1. Receiver operating characteristic curve (ROC)

Nếu bây giờ ta coi lớp **1** là lớp **Positive**, lớp **0** là lớp **Negative**, làm thế nào để tăng mức độ báo nhầm (**FPR**) để giảm mức độ bỏ sót (**FNR**). Chú ý rằng tăng **FNR** đồng nghĩa với việc giảm **TPR** vì tổng của chúng luôn bằng 1.

Một kỹ thuật đơn giản là ta thay giá trị ***threshold*** từ 0.5 xuống một số nhỏ hơn. Chẳng hạn nếu chọn ***threshold*** = 0.3, thì mọi điểm được dự đoán có xác suất đầu ra lớn hơn 0.3 sẽ được dự đoán là thuộc lớp Positive. Nói cách khác, tỉ lệ các điểm được phân loại là **Positive** sẽ tăng lên, kéo theo cả **False Positive Rate** và **True Positive Rate** cùng tăng lên (cột thứ nhất trong ma trận tăng lên). Từ đây suy ra cả **FNR** và **TNR** đều giảm.

Ngược lại, nếu ta muốn bỏ sót còn hơn báo nhầm, tất nhiên là ở mức độ nào đó, như bài toán xác định email rác chẳng hạn, ta cần tăng ***threshold*** lên một số lớn hơn 0.5. Khi đó, hầu hết các điểm dữ liệu sẽ được dự đoán thuộc lớp **0**, tức **Negative**, và cả **TNF** và **FNR** đều tăng lên, tức **TPR** và **FPR** giảm xuống.

Như vậy, ứng với mỗi giá trị của ***threshold***, ta sẽ thu được một cặp (**FPR**, **TPR**). Biểu diễn các điểm (**FPR**, **TPR**) trên đồ thị khi thay đổi ***threshold*** từ 0 tới 1 ta sẽ thu được một đường được gọi là **Receiver Operating Characteristic curve** hay **ROC curve**. (Chú ý rằng khoảng giá trị của ***threshold*** không nhất thiết từ 0 tới 1 trong các bài toán tổng quát. Khoảng giá trị này cần được đảm bảo có trường hợp **TPR/FPR** nhận giá trị lớn nhất hay nhỏ nhất mà nó có thể đạt được).



Hình 4.1: Ví dụ về đường ROC

* 1. Area Under the Curve

Dựa trên đường cong **ROC**, ta có thể chỉ ra rằng một mô hình có hiệu quả hay không. Một mô hình hiệu quả khi có **FPR** thấp và **TPR** cao, tức tồn tại một điểm trên đường cong **ROC** gần với điểm có toạ độ **(0, 1)** trên đồ thị (góc trên bên trái). Curve (đường cong) càng gần thì mô hình càng hiệu quả.

Có một thông số nữa dùng để đánh giá được gọi là **Area Under the Curve** hay **AUC**. Đại lượng này chính là diện tích nằm dưới **ROC** **curve** màu cam. Giá trị này là một số dương nhỏ hơn hoặc bằng 1. Giá trị này càng lớn thì mô hình càng tốt.

* 1. Precision và Recall

Với bài toán phân loại mà tập dữ liệu của các lớp là chênh lệch nhau rất nhiều, có một phép đó hiệu quả thường được sử dụng là **Precision-Recall**.

Trước hết xét bài toán phân loại nhị phân. Ta cũng coi một trong hai lớp là **positive**, lớp còn lại là **negative**.

Xét hình 3 dưới đây:



Hình 4.2: Cách tính Precision và Recall

Với một cách xác định một lớp là positive, Precision được định nghĩa là tỉ lệ số điểm true positive trong số những điểm được phân loại là positive (TP + FP).

Recall được định nghĩa là tỉ lệ số điểm true positive trong số những điểm thực sự là positive (TP + FN).

Một cách toán học, Precison và Recall là hai phân số có tử số bằng nhau nhưng mẫu số khác nhau:

Có thể nhận thấy rằng TPR và Recall là hai đại lượng bằng nhau. Ngoài ra, cả Precision và Recall đều là các số không âm nhỏ hơn hoặc bằng một.

Precision cao đồng nghĩa với việc độ chính xác của các điểm tìm được là cao. Recall cao đồng nghĩa với việc True Positive Rate cao, tức tỉ lệ bỏ sót các điểm thực sự positive là thấp.

* 1. Residual sum of squares (RSS)

Trong thống kê, residual sum of squares (RSS) hoặc the sum of squared residuals (SSR) hoặc the sum of squared errors of prediction (SSE), là tổng số dư bình phương (độ lệch giữa giá trị dự đoán và giá trị thực tế của dữ liệu). Đây là thước đo sự khác biệt giữa dữ liệu thực và mô hình ước tính. Nếu giá trị RSS nhỏ thì có nghĩa là độ **fit** (khít) giữa mô hình dự đoán và mô hình ước tính cao. Nó được dùng như một tiêu chí tối ưu trong việc lựa chọn tham số và lựa chọn mô hình.



KẾT LUẬN

* 1. Những phần đã làm hoàn thành
* Đã ứng dụng quy trình khai phá dữ liệu và lấy được insights của dữ liệu đối với 3 dạng bài toán: Regression, Classification và Clustering.
* Đã thực hiện Tuning Model để đạt kết quả chính xác cao nhất.
* Đã thực hiện đánh giá mô hình qua nhiều phương pháp.
* Đã xây dựng Data Story một cách mạch lạc và trực quan.
  1. Đánh giá ưu nhược điểm

|  |  |  |
| --- | --- | --- |
|  | Ưu điểm | Nhược điểm |
| Đối với bài toán Regression | Cho kết quả dự đoán cao | Rất nhạy cảm với nhiễu, dễ bị Overfitting |
| Đối với bài toán Classification | Cho kết quả phân loại tốt | Thời gian huấn luyện lâu (SVM) |
| Đối với bài toán Clustering | Thời gian huấn luyện nhanh | Khó khăn trong việc Feature Selection |

* 1. Phương hướng phát triển

Sử dụng các phương pháp và mô hình Machine Learning mới để đem lại độ chính xác cao hơn. Ví dụ như các thuật toán Ensemble: Boosting, AdaBoost, Random Forest. Đổi lại, đòi hỏi phần cứng hệ thống cao hơn, thời gian train lâu hơn.

TÀI LIỆU THAM KHẢO

[1]. Vũ Hữu Tiệp, Machine Learning Cơ Bản

[2]. Ông Xuân Hồng, Machine Learning Ông Xuân Hồng

[3]. Christopher Bishop, Pattern Recognition and Machine Learning

[4]. Jason Brownlee, Machine Learning Mastery

[5]. Andrew Ng, Machine Learning Course

[6]. Andrew Ng, Deep Learning Course

[7]. Kirill Eremenko, Super Data Science

[8]. Grant Sanderson, 3Blue1Brown Course