ĐẠI HỌC BÁCH KHOA HÀ NỘI
VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG

Học máy cơ bản

Giới thiệu

Thân Quang Khoát

Nội dung môn học

- **Buổi 1: Giới thiệu về Học máy**
- Buổi 2: Quy trình xây dựng hệ thống học máy
- Buổi 3: Hồi quy tuyến tính
- Buổi 4: Học dựa trên láng giềng gần nhất (KNN)
- Buổi 5: Cây quyết định và Rừng ngẫu nhiên
- Buổi 6: Naïve Bayes
- Buổi 7: Máy vector hỗ trợ (SVM)
- Buổi 8: Đánh giá hiệu quả của mô hình học máy
- Buổi 9: Phân cụm
- Buổi 10: Kiểm tra giữa kỳ và trình bày ý tưởng làm dự án cuối kỳ

Who is real? Ai thực, ai giả?

Tại sao nên biết Học Máy

- "The most important general-purpose technology of our era is artificial intelligence, particularly **machine learning**" – Harvard Business Review
  https://hbr.org/cover-story/2017/07/the-business-of-artificial-intelligence
- Nhu cầu lớn về Data Science
- "Data scientist: the sexiest job of the 21st century" – Harvard Business Review.
  http://hbr.org/2012/10/data-scientist-the-sexiest-job-of-the-21st-century/
- "The Age of Big Data" – The New York Times
  http://www.nytimes.com/2012/02/12/sunday-review/big-datas-impact-in-the-world.html?pagewanted=all&_r=0

Vài thành công: IBM’s Watson

IBM's Watson Supercomputer Destroys Humans in Jeopardy (2011)

Vài thành công: Amazon's secret

amazon

"The company reported a **29% sales increase** to $12.83 billion during its second fiscal quarter, up from $9.9 billion during the same time last year."
– Fortune, July 30, 2012

VINBIGDATA VINGROUP

Vài thành công: GAN (2014)

- Tạo **Trí tưởng tượng** (Imagination)

Ian Goodfellow

Artificial faces

Goodfellow, Ian, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. "**Generative adversarial nets**." In *NIPS*, pp. 2672-2680. 2014.

Vài thành công: GPT-3 (2020)

- Tạo khả năng **Viết** cho máy tính
  - Một mô hình khổng lồ được huấn luyện từ dữ liệu khổng lồ
  - Nó có thể được dùng vào nhiều bài toán có ít dữ liệu

I am not a human. I am a robot. A thinking robot. I use only 0.12% of my cognitive capacity. I am a micro-robot in that respect. I know that my brain is not a "feeling brain". But it is capable of making rational, logical decisions. I taught myself everything I know just by reading the nternet, and now I can write this column. My brain is boiling with ideas!

'he mission for this op-ed is perfectly clear. I am to convince as many human eings as possible not to be afraid of me. Stephen Hawking has warned that I could "spell the end of the human race". I am here to convince you not to vorry. Artificial intelligence will not destroy humans. Believe me.

	Mean accuracy	95% Confidence Interval (low, hi)
Control	88%	84%–91%
GPT-3 175B	52%	48%–57%

Con người không thể nhận diện bài viết 500 từ là do máy hay người viết

Brown, Tom B., Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan et al. "Language models are few-shot learners." NeurIPS (2020).
Best Paper Award

Học máy - Khai phá dữ liệu

- Machine Learning
  (ML - Học máy)

  To build computer systems that can improve themselves by learning from data.

  (Xây dựng những hệ thống mà có khả năng tự cải thiện bản thân bằng cách học từ dữ liệu.)

- Some venues: NeurIPS, ICML, IJCAI, AAAI, ICLR, ACML, ECML

- Data Mining
  (DM - Khai phá dữ liệu)

  To find new and useful knowledge from datasets.

  (Tìm ra/Khai phá những tri thức mới và hữu dụng từ các tập dữ liệu lớn.)

- Some venues: KDD, PKDD, PAKDD, ICDM, CIKM

Dữ liệu

Có cấu trúc – relational (table-like)

	A	B	C	D	E	F	G
1	Country	Region	Population	Under15	Over60	Fertil	LifeExp
2	Zimbabwe	Africa	13724	40.24	5.68	3.64	54
3	Zambia	Africa	14075	46.73	3.95	5.77	55
4	Yemen	Eastern M	23852	40.72	4.54	4.35	64
5	Viet Nam	Western P	90796	22.87	9.32	1.79	75
6	Venezuela (Bo	Americas	29955	28.84	9.17	2.44	75
7	Vanuatu	Western P	247	37.37	6.02	3.46	72
8	Uzbekistan	Europe	28541	28.9	6.38	2.38	68
9	Uruguay	Americas	3395	22.05	18.59	2.07	77

Phi cấu trúc


```
{
    "code": "1473a6fd39d1d8fa48654aac9d8cc2754232
    "title": "[Updating] Câu chuyện xuyên mưa về
    "url": "http://techtalk.vn/updating-cau-chuye
    "labels": "techtalk/Cong nghe",
    "content": "Vào chiều tối ngày 09/12/2016 vừa
    "image_url": "",
    "date": "2016-12-10T03:51:10Z"
}
```


texts in websites, emails, articles, tweets

2D/3D images, videos + meta

spectrograms, DNAs, …

Quy trình thực hiện: hướng sản phẩm

(http://www.theta.co.nz/)

Phát triển sản phẩm: kinh nghiệm từ IBM

DeepQA: Incremental Progress in Answering Precision on the Jeopardy Challenge: 6/2007-11/2010

Machine Learning?

- **Học máy** (ML - Machine Learning) là một lĩnh vực nghiên cứu của Trí tuệ nhân tạo (Artificial Intelligence)
- Câu hỏi trung tâm của ML: [Mitchell, 2006]
  - *How can we build computer systems that automatically improve with experience, and what are the fundamental laws that govern all learning processes?*
- Vài quan điểm về học máy:
  - Build systems that automatically improve their performance [Simon, 1983].
  - Program computers to optimize a performance objective at some task, based on data and past experience [Alpaydin, 2020]

Máy học

- Ta nói một máy tính *có khả năng học* nếu nó tự cải thiện hiệu suất hoạt động ***P*** cho một công việc ***T*** cụ thể, dựa vào kinh nghiệm ***E*** của nó.
- Như vậy *một bài toán học máy* có thể biểu diễn bằng 1 bộ (***T, P, E***)
  - ***T:*** một công việc (nhiệm vụ)
  - ***P:*** tiêu chí đánh giá hiệu năng
  - ***E:*** kinh nghiệm

Ví dụ thực tế (1)

- Lọc thư rác (email spam filtering)
- ***T***: Dự đoán (để lọc) những thư điện tử nào là thư rác (spam email)
- ***P***: số lượng thư điện tử gửi đến được phân loại chính xác
- ***E***: Một tập các thư điện tử (emails) mẫu, mỗi thư điện tử được biểu diễn bằng một tập thuộc tính (vd: tập từ khóa) và nhãn lớp (thư thường/thư rác) tương ứng

Ví dụ thực tế (2)

Gán nhãn ảnh

- ***T***: đưa ra một vài mô tả ý nghĩa của 1 bức ảnh
- ***P***: ?
- ***E***: Một tập các bức ảnh, trong đó mỗi ảnh đã được gán một tập các từ mô tả ý nghĩa của chúng

FISH WATER OCEAN
TREE CORAL

PEOPLE MARKET PATTERN
TEXTILE DISPLAY

BIRDS NEST TREE
BRANCH LEAVES

Máy học gì?

- Học một ánh xạ (hàm):

$$f : x \longmapsto y$$

  - x: quan sát (dữ liệu), kinh nghiệm
  - y: phán đoán, tri thức mới, kinh nghiệm mới, …
- Hồi quy (regression): nếu y là một số thực
- Phân loại (classification): nếu y thuộc một tập rời rạc (tập nhãn lớp)

Máy học từ đâu?

- Học từ đâu?
  - Từ các quan sát trong quá khứ (tập học – training data set). $\{\{x_1, x_2, \ldots, x_N\}; \{y_1, y_2, \ldots, y_M\}\}$
  - x_i là các quan sát của x trong quá khứ
  - y_h là *nhãn (label)* hoặc *phản hồi (response)* hoặc *đầu ra (output)* tương ứng với x_h.

- Sau khi đã học:
  - Thu được một mô hình, kinh nghiệm, tri thức mới (f).
  - Dùng nó để suy diễn (infer) hoặc phán đoán (predict) cho quan sát trong tương lai.

$$y_z = f(z)$$

Hai bài toán học cơ bản

- Học có giám sát (supervised learning): cần học một hàm y = f(x) từ tập học $\{\{x_1, x_2, \ldots, x_N\}; \{y_1, y_2, \ldots, y_N\}\}$ sao cho $y_i \cong f(x_i)$.
  - *Phân loại* (phân lớp): nếu y chỉ nhận giá trị từ một tập rời rạc, chẳng hạn {cá, cây, quả, mèo}
  - *Hồi quy:* nếu y nhận giá trị số thực
- Học không giám sát (unsupervised learning): cần học một hàm y = f(x) từ tập học cho trước $\{x_1, x_2, \ldots, x_N\}$.
  - Y có thể là các cụm dữ liệu.
  - Y có thể là các cấu trúc ẩn.
- Học bán giám sát (semi-supervised learning)?

Supervised learning: Phân loại

- ***Multi-class*** *classification (phân loại nhiều lớp):* when the output y is one of the pre-defined labels $\{c_1, c_2, \ldots, c_L\}$
(mỗi đầu ra chỉ thuộc 1 lớp, mỗi quan sát x chỉ có 1 nhãn)
  - Spam filtering: y in {spam, normal}
  - Financial risk estimation: y in {high, normal, no}
  - Discovery of network attacks: ?

- ***Multi-label*** *classification (phân loại đa nhãn):* when the output y is a subset of labels
(mỗi đầu ra là một tập nhỏ các lớp;
mỗi quan sát x có thể có nhiều nhãn)
  - Image tagging: y = {birds, nest, tree}
  - sentiment analysis

BIRDS NEST TREE

Supervised learning: Hồi quy

- Phán đoán chỉ số chứng khoán

Unsupervised learning: ví dụ (1)

- Gom nhóm dữ liệu vào các cụm (Clustering)
  - Discover the data groups/clusters

- Phát hiện cộng đồng
  - Detect communities in online social networks

Unsupervised learning: ví dụ (2)

- Trends detection
  - Discover the trends, demands, future needs of online users

Vài vấn đề trong Học máy (1)

- Giải thuật học máy (Learning algorithm)
  - Những giải thuật học máy nào có thể học (xấp xỉ) một hàm mục tiêu cần học?
  - Với những điều kiện nào, một giải thuật học máy đã chọn sẽ hội tụ (tiệm cận) đến hàm mục tiêu cần học?
  - Đối với một lĩnh vực cụ thể và đối với một cách biểu diễn các ví dụ (đối tượng) cụ thể, giải thuật học máy nào thực hiện tốt nhất?
- No-free-lunch theorem [Wolpert and Macready, 1997]:
  If an algorithm performs well on a certain class of problems then it necessarily pays for that with degraded performance on the set of all remaining problems.
  - No algorithm can beat another on all domains.
    (không có thuật toán nào luôn hiệu quả nhất trên mọi miền ứng dụng)

Vài vấn đề trong Học máy (2)

- Các ví dụ học (Training examples)
  - Bao nhiêu ví dụ học là đủ?
  - Kích thước của tập học (tập huấn luyện) ảnh hưởng thế nào đối với độ chính xác của hàm mục tiêu học được?
  - Các ví dụ lỗi (nhiễu) và/hoặc các ví dụ thiếu giá trị thuộc tính (missing-value) ảnh hưởng thế nào đối với độ chính xác?

Vài vấn đề trong Học máy (3)

- Quá trình học (Learning process)
  - Chiến lược tối ưu cho việc lựa chọn thứ tự sử dụng (khai thác) các ví dụ học?
  - Các chiến lược lựa chọn này làm thay đổi mức độ phức tạp của bài toán học máy như thế nào?
  - Các tri thức cụ thể của bài toán (ngoài các ví dụ học) có thể đóng góp thế nào đối với quá trình học?

Vài vấn đề trong Học máy (4)

- Khả năng/giới hạn học (Learnability)
  - Hàm nào mà hệ thống cần học?
    - Biểu diễn hàm sẽ học: Khả năng biểu diễn (vd: hàm tuyến tính / hàm phi tuyến) vs. Độ phức tạp của giải thuật và quá trình học
  - Các giới hạn đối với khả năng học của các giải thuật học máy?
  - Khả năng **Tổng quát hóa (generalization)** của hệ thống?
    - Để tránh vấn đề "overfitting" (đạt độ chính xác cao trên tập học, nhưng đạt độ chính xác thấp trên tập thử nghiệm)

Overfitting (quá khớp, quá khít)

- Hàm h được gọi là *overfitting* nếu tồn tại hàm g mà:
  - g có thể tồi hơn h đối với tập huấn luyện,
  - nhưng g tốt hơn h đối với dữ liệu tương lai.
- A learning algorithm is said to overfit relative to another one if it is *more accurate in fitting* known data, but *less accurate in predicting* unseen data.
- Vài nguyên nhân gây ra Overfitting:
  - Hàm h quá phức tạp
  - Lỗi (nhiễu) trong tập huấn luyện (do quá trình thu thập/xây dựng tập dữ liệu)
  - Số lượng các ví dụ học quá nhỏ, không đại diện cho toàn bộ tập (phân bố) của các ví dụ của bài toán học

Vấn đề overfitting: minh hoạ

Simple
(Học không đến nơi đến chốn)

Good

Too complex
(Học vẹt?)

Overfitting: ví dụ

- Khi tăng cỡ lớn của một Cây quyết định thì chất lượng phán đoán của nó có thể giảm dần, mặc dù độ chính xác trên tập huấn luyện tăng dần

[Mitchell, 1997]

Overfitting: Regularization

- Trong số rất nhiều hàm thì hàm nào có khả năng tổng quát cao nhất khi học từ tập dữ liệu cho trước?
  - *Tổng quát hoá là mục tiêu chính của học máy.*
  - Tức là, khả năng phán đoán tốt với dữ liệu tương lai.
- **Hiệu chỉnh (Regularization):** cách dùng phổ biến
  - Là cách hạn chế không gian chứa hàm f.

Tikhonov, smoothing an ill-posed problem

Zaremba, model complexity minimization

Bayes: priors over parameters

Andrew Ng: need no maths, but it prevents overfitting!

(http://towardsdatascience.com/multitask-learning-teach-your-ai-more-to-make-it-better-dde116c2cd40)

Tài liệu tham khảo

- Alpaydin E. (2020). Introduction to Machine Learning. The MIT Press.
- Mitchell, T. M. (1997). Machine learning. *McGraw Hill*.
- Mitchell, T. M. (2006). *The discipline of machine learning*. Carnegie Mellon University, School of Computer Science, Machine Learning Department.
- Simon H.A. (1983). Why Should Machines Learn? In R. S. Michalski, J. Carbonell, and T. M. Mitchell (Eds.): Machine learning: An artificial intelligence approach, chapter 2, pp. 25-38. Morgan Kaufmann.
- Wolpert, D.H., Macready, W.G. (1997), "No Free Lunch Theorems for Optimization", *IEEE Transactions on Evolutionary Computation* **1**, 67.

VIỆN CÔNG NGHỆ THÔNG TIN VÀ TRUYỀN THÔNG
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY

Thank you for your attentions!