

2018 ICML을 통해 살펴보는 AI 연구 동향

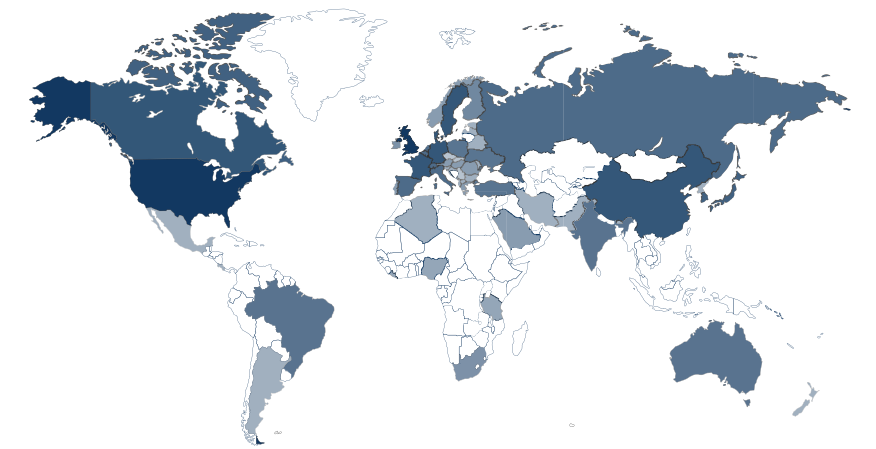
글 | 박찬연 chan.y.park@kc-ml2.com / chan@morulabs.com 대학에서 물리학을 전공하였고, 졸업하기 전 2년여간 웹 프로그래머와 시스템 프로그래머로 일했습니다. 이후 대학원에 진학하여 이론물리학, 그중에서도 끈이론을 전공하였고, 2017년까지는 물리학과 기하학 그리고 프로그래밍에 대한 관심과 경험을 바탕으로 한 연구를 계속했습니다. 그러던 중 머신러닝에서 데이터를 바탕으로 수학적 모델을 세우고 이를 프로그래밍으로 구현하는 흥미로운 일이 많음을 알게 되어 딥러닝 연구에 뛰어들기로 결심합니다. 2018년부터 반도체 제조 솔루션 기업 KC의 Machine Learning Lab(ML2)의 principal research scientist와 스타트업 모루랩스(Moru Labs)의 CTO를 맡아서 여러분들의 도움을 받으며 많은 것을 배우고 있습니다.

ICML(International Conference on Machine Learning)은 머신러닝(machine learning)과 딥러닝(deep learning) 분야에서 NIPS(Neural Information Processing Systems), ICLR(International Conference on Learning Representations)과 함께 전 세계 주요 학회 중 하나입니다. 2018년 ICML은 스웨덴 스톡홀름(Stockholm)에서 7월 10일부터 15일까지 개최되었습니다.

올해 ICML에는 5000여 명이 참가하고 2500편 이상의 논문이 제출되는 등 역대 최대 규모를 기록했습니다. 이는 지난 ICML과 비교하여도 큰 폭으로 증가한 숫자이며, 머신러닝 및 딥러닝에 대한 많은 연구와 관심이 반영된 것으로 볼 수 있습니다. 폭발적으로 늘어난 제출 논문들로 논문 심사 과정에서 논문을 제출하신 분들과 심사하시는 분들 모두 많은 어려움을 겪었다는 이야기도 여러 곳에서 들었습니다.

[그림 1] 연도별, 국가별 ICML 참가자 수^{*1}

5000 registered participants (2300 in 2007, 3200 in 2016, 1600 in 2015)



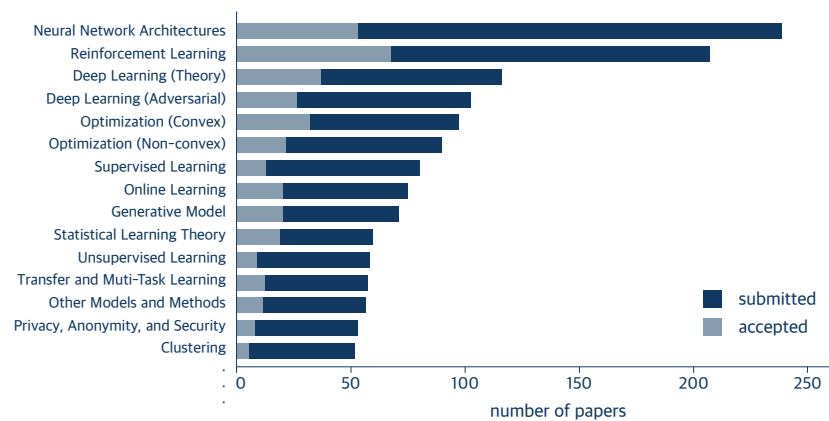
[그림 2] 연도별 제출 및 통과된 논문 수 추이^{*1}



^{*1} 참고 | F. Bach, Opening remarks, ICML 2018

[그림 3]과 같이 제출된 논문을 주제별로 나누어보았을 때, 가장 많이 제출된 분야는 신경망 구조(neural network architecture)이지만 가장 많이 채택된 분야는 강화 학습(reinforcement learning)이라는 점이 흥미롭습니다. 개인적인 추측으로는 새로운 구조(architecture)를 제안하는 연구는 그것이 모델에 대한 이해를 돕거나, 기존의 모델과 비교할 때 명확하게 향상된 성능을 보여주지 않는다면 좋은 연구성과로 받아들여질 수 없다는 점이 그 이유가 아닐까 생각합니다. 또 다른 흥미로운 점은 딥러닝의 이론적인 이해에 대한 연구가 세 번째로 많이 다루어지고 채택된 연구주제라는 것입니다. 머신러닝과 딥러닝을 연구하는 분들께서 현재의 성과에 안주하지 않고 근본적인 딥러닝의 이해에 대해 계속 고민하고, 이를 통해 더욱 큰 발전을 바라고 계신다는 생각이 들었습니다. 마찬가지로 머신러닝의 핵심이라고 할 수 있는 최적화(optimization)도 여전히 중요한 주제로 다루어지고 있다는 점도 눈길을 끌었습니다.

[그림 3] 주제별 제출 및 통과된 논문 수^{*1}



이번 ICML에서는 구두 발표(oral presentation)와 워크숍(workshop)의 규모도 굉장하였습니다. 학회 첫날인 7월 10일에는 9개의 튜토리얼(tutorial)이 3개의 동시 세션(parallel session)으로 나누어 진행되었고, 11일부터 13일까지 3일간의 학회 메인 기간 동안에는 매일 200개가 넘는 논문 발표가 10개의 세션에서 동시에 운영되었습니다. 또한 3일간 67개의 워크숍도 개최되면서 상황리에 진행되었습니다. 상황이 이렇다 보니 매일 어떤 세션에 참여할지 결정하는 것도 큰 일이었고, 어떤 결정을 내리던 많은 내용들을 놓칠 수밖에 없어 안타깝기도 하였습니다. 또한 현재의 연구 상황과 앞으로의 연구 방향에 대한 의견을 나누며 연구자분들과 교류하는 데 많은 시간을 할애하다 보니 더 많은 발표에 참석하지 못한 아쉬움도 남았습니다.

올해 ICML의 규모를 고려하여 이 글에서는 모든 내용을 담기보다는, 이번 학회에서 인상 깊었던 발표 내용들을 간단히 정리한 후 이어서 제가 평소 관심을 가지고 있는 연구 주제 중심으로 정리해보고자 합니다. 다행히도 꽤 많은 발표 영상들이 학회 중에 생중계되거나 녹화되어 인터넷에 올라왔습니다. 조만간 모든 발표가 녹화된 영상이 올라온다고 하니, ICML 웹사이트에서 관심 분야의 발표 내용을 확인해보시면 좋을 것 같습니다.^{*2} 그리고 이번 ICML에서 가장 많이 다루어진 주제인 강화 학습 위주로 학회 내용을 정리한 데이빗 아벨(David Abel)의 글^{*3}도 살펴보시길 추천해드립니다.

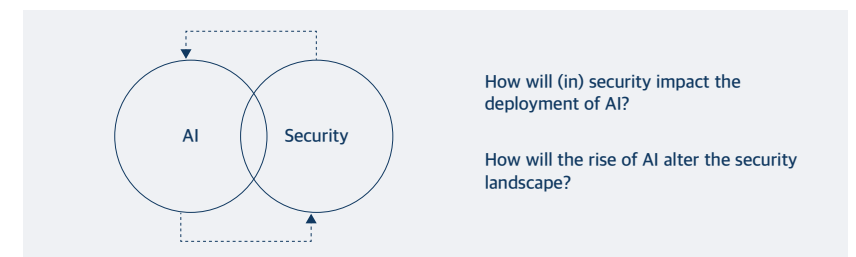
^{*2} 참고 | <https://icml.cc/Conferences/2018/Schedule>
^{*3} 참고 | https://david-abel.github.io/blog/posts/misc/icml_2018.pdf

머신러닝과 보안

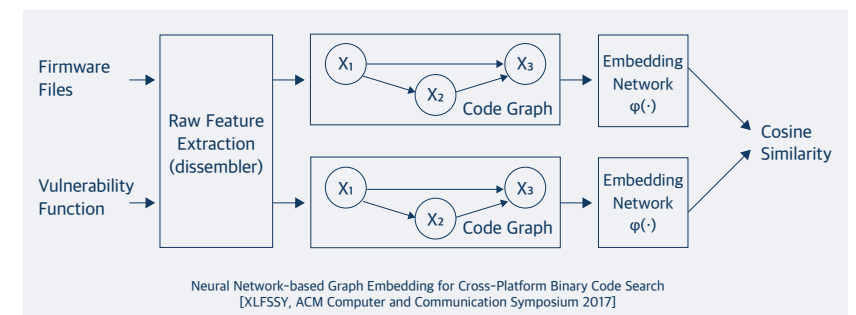
정보기술 기반 산업에서 보안은 언제나 중요하게 생각해야 할 부분입니다. 개인정보 및 사업정보 등 대량의 데이터를 기반으로 하는 데이터 사이언스(data science)와 머신러닝이 더욱 보편화됨에 따라 앞으로 새로운 보안 문제와 대책이 중요하게 다루어질 것으로 생각됩니다. 머신러닝 커뮤니티에서도 이러한 생각을 강조하고 서로 공유하고 있다는 것을 이번 학회를 통해 다시 한 번 느낄 수 있었습니다.

먼저 기조연설 중 하나였던 다운 송(Dawn Song)의 ‘AI and Security: Lessons, Challenges and Future Directions(인공지능과 보안: 레슨, 도전 과제 및 향후 방향)’에서는 다양한 예제를 통해 새로운 머신러닝 기술이 기존의 보안 문제에 어떤 도움을 줄 수 있으며, 또한 머신러닝 기술의 발달과 함께 어떠한 새로운 보안 문제가 등장할 수 있는지에 대해서 다루었습니다. 딥러닝을 이용한 사물인터넷(IoT) 디바이스의 취약성 발견과 시각 인식 시스템을 적대적으로 공격하는 기법인 적대적 공격(adversarial attack) 등이 그 예입니다. 제시된 문제점 중 가장 마음에 와 닿았던 것은, 만일 머신러닝 모델들의 학습 능력이 데이터를 모두 기억할 수 있을 정도로 뛰어나다면, 머신러닝 모델의 입력값을 적절히 조절하여 그에 해당하는 출력값을 통해 학습된 데이터를 볼 수 있을까라는 것이었습니다. 머신러닝 모델, 그중에서도 특히 딥러닝 모델들이 데이터를 어떻게 처리하고 저장하는지에 대한 이해는 아직 부족하고 이와 관련된 연구도 아직 활발하게 진행 중입니다. 특히 딥러닝 모델들의 경우 산술적으로는 모든 데이터를 기억할 수 있을 정도로 큰 학습 능력을 가지고 있다는 것과 몇몇 모델들의 경우에는 실제로 기억에 의한 학습이 많은 부분을 차지한다는 것을 고려해봤을 때, 의료 정보나 신용정보와 같은 민감한 개인정보를 다루는 머신러닝 모델의 보안성은 매우 중요한 주제입니다.

[그림 4] AI와 보안^{*4}



[그림 5] 딥러닝을 이용한 사물인터넷 디바이스의 취약성 찾기^{*4}



^{*4} 참고 | AI and Security: Lessons, Challenges and Future Directions, D. Song, ICML 2018

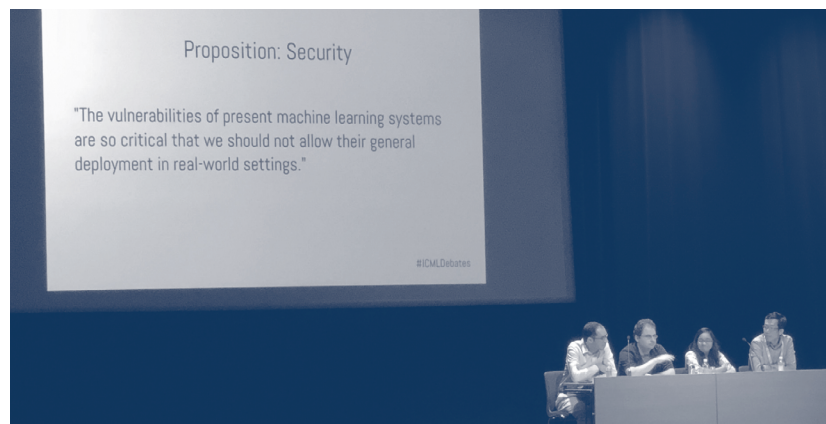
[그림 6] 딥러닝을 적대적으로 이용한 사례^{*4}

이번 ICML의 최우수 논문 중 하나^{*5}도 보안과 관련된 것이었습니다. 특히 논문 내용 외에 발표 내용 중 “보안 문제를 방어하는 연구를 하고 싶다면 먼저 최신 보안 방어 시스템을 공격하는 연구를 해봐야 한다”는, 다시 말해 해커의 자세를 가져야 한다는 이야기가 가장 인상 깊었습니다. 또한 딥러닝 모델 해커들이 방어 방법에 대한 연구논문을 모두 읽고 이해한 후 그 취약성을 공격할 것이라는 가정 하에 보안 방어 연구를 진행해야 한다는 지적도 설득력 있게 다가왔습니다.

보안 연구자가 가져야 할 마음가짐^{*6}

The threat model MUST assume the attacker has read the paper and knows the defender is using those techniques to defend.

토요일에 열린 워크숍 중 하나^{*7}에서는 머신러닝과 관련된 여러 주제들에 관해 토론을 하는 자리가 마련되었습니다. 그중 보안과 관련해서 주된 논점 중 하나는 우리가 한정된 연구자원을 첨단 머신러닝 기술 개발에 투입하는 것이 옳은가, 아니면 연구의 시작부터 보안을 강화하는 데에 투입해야 하는가에 대한 것이었습니다. 물론 한 번의 토론으로 결론이 날 수 있는 주제가 아니라 머신러닝 커뮤니티가 지속적으로 함께 고민해보아야 할 문제입니다만, 이렇게 모두가 문제의식을 공유하고 그에 대해 의견을 주고받고 있다는 점이 머신러닝 커뮤니티가 건강하다는 증거가 아닐까 생각되었습니다.

[그림 7] 머신러닝과 보안에 관한 토론^{*8}

^{*5} 논문 | Athalye, A., Carlini, N., Wagner, D. (2018). Obfuscated Gradients Give a False Sense of Security: Circumventing Defenses to Adversarial Examples. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:274-283

^{*6} 참고 | Carlini, N., Best Paper Session 1, ICML 2018

^{*7} 참고 | <https://www.machinelearningdebates.com>

^{*8} 참고 | <https://twitter.com/LaflammeSteph>

공정한 머신러닝

머신러닝으로 학습된 모델은 데이터가 반영하는 현재 사회의 편견(bias)까지도 배우기 때문에 그에 따르는 사회적 영향을 고려해야 합니다. 이는 딥러닝의 혁신적인 발전으로 머신러닝 모델이 많은 데이터를 학습하는 것이 쉬워졌을 때부터 중요하게 생각되어 왔습니다.

한편 딥러닝이 주목받기 이전부터 사회과학 분야의 연구자들은 적극적으로 데이터 기반의 머신러닝 방법론을 받아들였습니다. 예를 들어 과거에는 공공 데이터로서 공개된 많은 정부 문서들이 사회과학 연구자들에게는 아주 귀중한 자료임에도 양이 워낙 방대하여 그 자료들을 연구에 활용하는 데 어려움을 겪었습니다. 그러나 이제는 LDA(latent dirichlet allocation)와 같은 자연어 처리 모델이 개발된 덕분에 연구 주제와 관련된 문서를 찾아내기가 훨씬 수월해졌습니다. 이와 같이 머신러닝을 활용한 다양하고 흥미로운 사회과학 연구에 대해서는 2016년 SciPy(Scientific Python Conference)의 기조 연설 중 하나였던 한나 월러크(Hanna Wallach)의 ‘Machine Learning for Social Science(사회과학 부문의 머신러닝)’^{*9}에서 살펴볼 수 있습니다. 또한 계량경제학이나 미시경제학을 연구하는 많은 분들도 사회과학과 수학, 그리고 데이터 사이언스가 만나는 지점에서 다양한 활동을 하면서 머신러닝과 딥러닝의 발전으로 많은 혜택을 보게 되었습니다. 그리고 2008년 미국 대통령 선거에서 데이터를 기반으로 한 선거전 전략이 화두로 떠오르면서^{*10} 정치학에서도 머신러닝과 데이터 사이언스의 중요성은 더욱 커지고 있습니다.

머신러닝 발전이 사회에 어떠한 영향을 미치며, 특히 그중에서 좋지 않은 영향을 줄이는 방법에 대한 주제는 머신러닝 커뮤니티 내에서만 연구하기에는 어려운 주제입니다. 따라서 전통적으로 사회과학의 여러 주제에 대해 깊은 관심과 고민을 가지고 있던 연구 커뮤니티와의 협력이 중요합니다. 이번 ICML의 또 다른 최우수 논문 중 하나^{*11}도 정량적으로 머신러닝의 공정함에 대해서 생각해보는 연구였습니다. ‘Fairness, Accountability, and Transparency in Machine Learning(머신러닝의 공정성, 책임성 및 투명성)’이라는 주제로 워크숍도 개최되어 앞으로 사회과학과 머신러닝의 조화롭고 생산적인 협력을 기대할 수 있게 되었습니다.

빅데이터와 베이지안 추론

GPGPU(General-purpose computing on graphics processing units)의 발전과 그에 따른 딥러닝의 르네상스가 찾아오기 전까지 머신러닝의 최전선은 베이지안 추론(Bayesian inference)이었다고 해도 무방합니다. 베이지안 추론 기반의 머신러닝은 상대적으로 적은 수의 데이터를 가지고도 해당 분야의 전문 지식까지 포함하는 좋은 모델을 만들 수 있다는 장점이 있지만, 많은 데이터를 효율적으로 처리하기 어렵다는 단점도 가지고 있습니다. 하지만 그 장점들 때문에 여전히 외행성 발견, 중력파 검출과 같은 과학 연구와 비행기 잔해 탐색, 교통량 분석, 무담보 소액대출(microcredit), 야생동물 보호, 제트엔진 분석 등 산업의 많은 분야에서 중요하게 활용되고 있습니다([그림 8] 참고). 이번 학회의 튜토리얼 중 하나인 브로데릭(Broderick)의 ‘Variational Bayes and Beyond: Bayesian Inference for Big Data’가 바로 이러한 베이지안 추론을 빅데이터 영역에 활용하는 방안을 연구한 것이었습니다. 특히 발표의 주된 내용은

^{*9} 참고 | <https://youtu.be/oqfKz-PP9FU>

^{*10} 참고 | <https://fivethirtyeight.com/tag/2008-presidential-election>

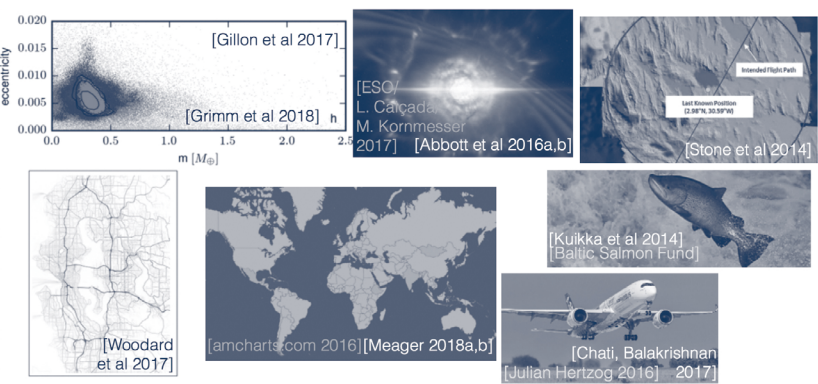
^{*11} 논문 | Liu, L.T., Dean, S., Rolf, E., Simchowitz, M. & Hardt, M. (2018). Delayed Impact of Fair Machine Learning. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:3150-3158

근사적인 베이지안 추론 대신, 효과적인 데이터 샘플링을 통해 베이지안 추론을 하는 방법론에 대한 것이었습니다.

[그림 8] 베이지안 추론의 다양한 활용*12

Bayesian inference

- Analysis goals: Point estimates, coherent uncertainties
- Interpretable, complex, modular; expert information



기조연설 발표자 중 한 분인 웰링(Welling)도 베이지안 추론을 딥러닝에 적용하는 것과 관련해 많은 연구를 진행하신 바 있습니다. 기조연설의 주제는 'Intelligence per Kilowatthour'로, 현재의 딥러닝 연구 결과가 실제로 활용되기 위해서는 지금보다 에너지를 훨씬 적게 사용하는 방법론이 필요하다는, 그러한 방법론의 예로 베이지안 추론을 이용하여 모델의 크기를 줄이는 연구에 대한 내용을 다루었습니다.

딥러닝의 이론적 이해

기존의 결정론적(deterministic)인 컴퓨터 알고리즘이나 자료구조(data structure)가 최근의 딥러닝 모델들과 다른 점 중 하나는 딥러닝 모델들의 작동에 대한 이론적인 이해가 부족하다는 것입니다. 다시 말하면 어떤 딥러닝 모델의 학습 능력이 뛰어난지, 어느 정도의 학습 능력을 가지고 있으며 어떻게 학습하지 않은 영역으로 일반화를 할 수 있는지, 어떤 구조를 가져야 주어진 데이터로 학습이 가능한지를 이해하지 못하고 있다는 것입니다.

그러한 질문에 대한 이론적인 이해를 위해서는 단순하지만 명확하게 수학적으로 정의될 수 있는 문제를 찾아서 정량적으로 질문에 대한 답을 구하려는 연구가 필요합니다. 이번 ICML에서 발표된 연구 내용 중 그 예를 찾아보자면*13, 두 가지 분류(binary classification)를 위해 학습된 신경망(neural network)이 모든 가까운 최소값들(local minima)에서 학습오차(training error)가 '0'이 되기 위한 조건에 대한 것입니다. 연구 결과로 나온 이를 충족시키는 조건은 1) 활성화 함수(activation function)가 증가하는 순볼록(strictly convex) 형태를 가지며, 2) 신경망은 1개의 숨겨진 층(hidden layer)을 가지거나 또는 쇼트컷 커넥션(shortcut connection)을 가지는 다층

네트워크(multi-layered network)이어야 하고, 3) 손실 함수(loss function)가 힌지 로스(hinge loss)를 매끄럽게 만든 형태여야 한다는 것입니다. 하지만 최근에 널리 사용되는 깊은 신경망(deep neural network)의 경우 위의 조건을 만족하는 경우는 없습니다. 이는 간단명료한 결론을 내릴 수 있는 문제를 만들 경우 그 대상에 포함되는 모델들이 toy model이 되는 경우가 많다는 현재의 딥러닝의 이론적인 이해 한계를 보여주고 있습니다.

또 다른 예*14는 'tropical geometry'의 풍부한 기하학적인 구조를 활용해 깊은 신경망을 이해하려는 연구로, ReLU(rectified linear unit) 활성화를 가지고 가중치(weight parameter)들이 정수(integer)로 주어지는 피드포워드 망(feed-forward network)과 'tropical rational map'의 상관관계를 보여줬습니다. 하지만 위의 조건을 만족시키는 깊은 신경망 역시 실제로 활용되고 있는 모델들과 비교했을 때 매우 단순한 경우에 국한됩니다.

이번 ICML의 튜토리얼 중 하나인 산지브 아로라(Sanjeev Arora)의 'Toward Theoretical Understanding of Deep Learning(딥러닝의 이론적 이해를 위해)'에서도 현재의 딥러닝에 대한 이론적인 이해가 앞서 말한 것과 같이 매우 제한적이라는 것을 이야기하고 있습니다. 물론 위와 같은 연구들이 향후에 중요한 이론적인 연구 결과가 나올 수 있는 원천이 될 수 있음을 인지하고 있어야 합니다. 동시에 튜토리얼에서는 단순히 발표된 모델의 구조를 이해하려고 하는 연구에 그치지 않고, 더 나아가 주어진 데이터를 효율적으로 학습할 수 있는 모델의 구조와 이를 가능하게 하는 최적화 방법을 먼저 제시할 수 있도록 노력해야 한다는 점이 강조되었습니다. 마무리 즈음에는 라그랑지안(Lagrangian)이나 해밀토니안(Hamiltonian)을 이용한 변분법(calculus of variation)의 사용과 같이 물리학에서 비롯된 직관(insight)의 역할이 중요할 수 있다는 점이 언급되어서, 물리학을 전공한 사람의 입장에서 반갑기도 했습니다.

딥러닝의 표현 학습

딥러닝이 지금과 같은 성공을 거둘 수 있었던 이유는, 연구자가 직접 특징(feature)을 선택하거나 생성해야 했던 이전 머신러닝 모델의 학습과는 다르게 역전파(backpropagation)를 이용해 모델이 직접 특징을 생성하고 연구자는 모델의 구조(architecture)와 학습목표(objective function) 설계에 집중할 수 있는 환경이 만들어졌기 때문입니다. 따라서 이렇게 학습된 특징이 사람이 이해할 수 있도록 의미를 가지는 표현(representation)과 어떻게 대응될 수 있는지에 대한 연구도 활발히 진행되고 있습니다.

지금까지 CNN(convolutional neural network)과 같은 딥러닝 모델은 유클리드 공간(Euclidean space)에 규칙적으로 배열된 데이터를 학습하는 데에 큰 성공을 거뒀습니다. 하지만 중요한 자료구조 중 하나인 그래프나 3차원 공간에 정의된 2차원 곡면과 같은 비유클리드 공간에 정의된 데이터의 학습, 또는 이러한 공간을 딥러닝 표현(representation learning) 학습에 사용하기 위해서는 비유클리드 기하학을 이용하여 이전의 모델을 확장하는 연구가 필요합니다. 이러한 주제를 다루는 연구를 아울러서 기하학적 딥러닝(geometric deep learning)이라고 부르며*15, 이번 ICML에서는 기하학적인 딥러닝 연구 중 계층구조(hierarchical structure)를

*12 참고 | T. Broderick, Variational Bayes and Beyond: Bayesian Inference for Big Data, ICML 2018. (http://www.tamarabroderick.com/files/broderick_tutorial_2018_icml_part_i.pdf)
*13 논문 | LIANG, S., Sun, R., Li, Y. & Srikant, R. (2018). Understanding the Loss Surface of Neural Networks for Binary Classification. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:2835-2843

*14 논문 | Zhang, L., Naitzat, G. & Lim, L. (2018). Tropical Geometry of Deep Neural Networks. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:5824-5832
*15 논문 | Bronstein, M. M., Bruna, J., Lecun, Y., Szlam, A., & Vandergheynst, P. (2017). Geometric Deep Learning: Going beyond Euclidean data. IEEE Signal Processing Magazine, 34(4), 18-42. doi:10.1109/msp.2017.2693418

가지는 데이터를 쌍곡기하학(hyperbolic geometry)에 임베딩(embedding)하는 것과 관련된 논문 두 편이 발표되었습니다.

그중 하나는 쌍곡기하학을 이용한 딥러닝의 첫 연구^{*16}에 이은 후속 연구^{*17}로, 쌍곡선 공간(hyperbolic space)의 푸앵카레 모델(Poincare model)을 사용하여 이루어진 이전의 모델링 방식을 로렌츠 모델(Lorentz model)을 이용하는 방식으로 변경하여 더욱 효율적인 리만 최적화(Riemannian optimisation)를 이끌어내는 것을 제안했습니다.

다른 하나^{*18}는 쌍곡선 기하학에서의 함축 콘(entailment cone)을 닫힌 형태(closed form)로 정의하고 이를 이용하여 방향성 비순환 그래프(directed acyclic graph)의 효율적인 임베딩을 보여준 연구였습니다. 또한 그래프를 다루기 위해 사용되는 딥러닝 모델 중 하나인 그래프 합성곱 네트워크(graph convolutional network)를 개선하기 위한 연구^{*19}^{*20}와 실제 데이터와 유사한 그래프를 생성하기 위한 심층 생성 모델(deep generative model)에 대한 연구^{*21}^{*22}도 흥미로웠습니다.

기하학의 아이디어를 활용한 표현학습의 또 다른 연구로는 모델이 특징의 대칭성을 유지하고 학습하도록 해서 더 적은 수의 특징으로도 더 많은 정보를 학습할 수 있도록 하는 방법이 있습니다. 여기에서 핵심이 되는 개념인 등변(equivariance)은 수학적으로는 다음과 같이 정의됩니다.

$$\phi(Tg\mathbf{x})=T'g\phi(\mathbf{x})$$

여기에서 ϕ 는 깊은 신경망 전체 혹은 일부에 해당하는 비선형함수(non-linear function), $\mathbf{x}$ 는 그 함수의 입력값(input), g 는 입력 공간(input space)의 대칭 그룹(symmetry group)인 G 의 원소, 그리고 T_g 는 그에 해당하는 변형(transformation)입니다. 위와 같은 등변식이 최대한 유지되도록 하면서 모델을 설계하려는 연구^{*23}^{*24}가 다양하게 진행되고 있으며, 한편으로는 이론적인 이해를 위해 미분기하학(differential geometry)에서 널리 사용되는 principal G-bundle을 이용한 연구^{*25}도 진행되고 있다는 사실 또한 이번 ICML의 ‘Towards learning with limited labels: Equivariance, Invariance, and Beyond’ 워크숍에서도 알 수 있었습니다. 아직은 이러한 연구들이 시작 단계에 불과하지만 앞으로의 발전이 기대되는 연구들이라고 생각합니다.

생성 모델(generative model)의 경우 잠재적 공간(latent space)에서의 표현을 이해하는 것이 중요한데, 그러기 위해서는 표현의 얽힘(entanglement) 문제를 해결하는 것이 필요합니다. 이번 ICML에서는 이를 위해 새로운 학습방법^{*26} 및 모델의 구조^{*27}, 그리고 새로운 학습목표^{*28}를 제시한 연구 결과들이 발표되었습니다. 또한 ‘Theoretical Foundations and Applications of Deep Generative Models’이라는 주제로 열린 워크숍에서도 현재 진행 중인 관련 연구들이 대거 소개되었습니다.

경험적인 해법을 머신러닝으로 대체하기

경험적인 해법(heuristic)은 여행하는 판매원 문제(travelling salesperson problem)와 같이 정확한 답을 찾기가 어려운 문제의 답을 현실적인 제약조건 안에서 찾기 위해 컴퓨터 알고리즘과 자료구조에서 자주 사용되는 방법입니다. 큰 의미에서 보면 알고리즘과 자료구조의 설계 자체도 주어진 문제를 해결하기 위해 연구자들이 이전까지의 경험과 문제에 대한 직관을 바탕으로 이끌어낸 경험적인 해법이라고 할 수 있을 것입니다.

따라서 머신러닝의 발전과 함께 이전의 경험적인 해법을 학습된 모델로 대체하려고 하는 시도는 자연스러운 연구 방향이라고 할 수 있습니다. 이는 알고리즘이나 자료구조를 설계할 때 문제를 해결하기 위한 세부적인 논리적 설계를 고민하기보다는 어떠한 학습 목표를 설정하는 것이 좋은지를 고민할 수 있게 함으로써, 경험적 해법을 이끌어내기 위해 필요하게 마련인 시행착오(trial and error)에 투입되는 시간과 노력을 줄이거나 효율적으로 활용할 수 있기 때문입니다.

이러한 연구 방향 중 흥미로웠던 결과는 구글(Google)이 이끌었던 두 개의 연구였는데, 그중 하나는 강화 학습을 통해 딥러닝 모델의 산출 그래프(computational graph)를 여러 GPU node에 배분하는 것을 최적화하여 전체 실행 시간을 단축하는 것이었습니다.^{*29} 또한 파일 시스템(file system)과 데이터베이스에서 널리 사용되는 B트리(B-tree) 구조와 같은 색인구조(index structure)를 학습된 모델로 대체하는 연구 결과도 흥미로웠습니다.^{*30} 특히 두 번째 연구의 경우, 기존의 색인구조와 학습된 색인구조(learned index structure)의 장단점을 비교하고, 이 둘을 함께 사용하는 구조를 제안함으로써 기존의 자료구조를 학습된 모델을 이용하여 점진적으로 발전시킬 수 있는 방법을 제시했다는 점이 인상적입니다.

지난 6월 26일, 구글의 제프 딘(Jeff Dean)이 구글 서울 캠퍼스에 방문했을 때 위의 두 연구들에 대한 질문을 할 수 있는 기회가 있었습니다. 저의 첫 번째 질문은 “경험적인 해법을 학습 모델로 대체할 수 있는 또 다른 연구 방향으로 어떤 것이 있을까?”였는데, “현재의 컴퓨터 시스템의 소프트웨어와 하드웨어에 다수의 경험적인 해법들이 포함되어 있기 때문에 이를 학습된 모델로 대체하여 성능을 향상시킬 만한 연구 방향 또한 많이 있을 것이고, 그중에서 캐시 정책(cache policy)과 관련된 연구가 흥미로울 것”이라는 답을 들었습니다. 단일 CPU 코어(CPU core)의 클럭(clock)을 증가시키는 것이 현실적으로 어려워진 지금의 상황에서 시스템의 성능을 크게 좌우하는 메모리 계층 구조(memory hierarchy)를 개선하는 것은 지연(latency) 및 OS 보안 커널(OS kernel security)과 같이 여러 가지 어려움이 예상되더라도 확실히 큰 성능 향상을 기대할 수 있는 연구 방향입니다. 이번 ICML에서는 구글에서 진행 중인 관련 연구가 발표되었는데^{*31}, 캐시 예측(cache prediction)을 N-gram 문제로 보고 LSTM(long short-term memory)을 이용하여 캐시 미스 주소(cache miss address)의 차이(delta)를 입력 데이터로 모델을 학습하는 구조를 제안했습니다. 이 연구는 발표자 스스로도 말했던 것처럼 해답보다는 질문을 많이 얻게 된 연구였습니다. 하지만 한편으로 이 연구는 딥러닝과 하드웨어의 결합이라는 새로운 방향을 제시한 흥미로운 연구라고 생각합니다.

머신러닝과 하드웨어를 접목하는 연구는 2001년에 신경망(neural network)과 의사결정 나무(decision tree)를 이용한 분기 예측(branch prediction)에 대한 연구^{*32}와 2008년에 진행됐던 강화 학습을 이용하여 DRAM 메모리 제어기(DRAM memory controller)를 개선하는

^{*16} 논문 | Nickel, M., Kiela, D., Poincare Embeddings for Learning Hierarchical Representations, NIPS 2017
^{*17} 논문 | Nickel, M. & Kiela, D., (2018). Learning Continuous Hierarchies in the Lorentz Model of Hyperbolic Geometry. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:3779-3788
^{*18} 논문 | Ganev, O., Becigneul, G. & Hofmann, T., (2018). Hyperbolic Entailment Cones for Learning Hierarchical Embeddings. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:1646-1655
^{*19} 논문 | Chen, J., Zhu, J. & Song, L., (2018). Stochastic Training of Graph Convolutional Networks with Variance Reduction. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:942-950
^{*20} 논문 | Xu, K., Li, C., Tian, Y., Sonobe, T., Kawarabayashi, K. & Jegelka, S., (2018). Representation Learning on Graphs with Jumping Knowledge Networks. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:5453-5462
^{*21} 논문 | Bojchevski, A., Shchur, O., Zugner, D. & Gunnemann, S., (2018). NetGAN: Generating Graphs via Random Walks. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:610-619
^{*22} 논문 | You, J., Ying, R., Ren, X., Hamilton, W. & Leskovec, J., (2018). GraphRNN: Generating Realistic Graphs with Deep Auto-regressive Models. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:5708-5717
^{*23} 논문 | T.S. Cohen, M. Welling, Group Equivariant Convolutional Networks. Proceedings of the International Conference on Machine Learning (ICML), 2016
^{*24} 논문 | Sabour, S., Frosst, N., Hinton, G.E. (2017). Dynamic Routing Between Capsules. NIPS 2017
^{*25} 논문 | T.S. Cohen, M. Geiger, M. Weiler, The Quite General Theory of Equivariant Convolutional Networks (forthcoming), 2018
^{*26} 논문 | Kamnitsas, K., Castro, D., Folgoc, L.L., Walker, I., Tanno, R., Rueckert, D., Glocker, B., Criminisi, A. & Nori, A. (2018). Semi-Supervised Learning via Compact Latent Space Clustering. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:2459-2468
^{*27} 논문 | Parascandolo, G., Kilbertus, N., Rojas-Carulla, M. & Scholkopf, B., (2018). Learning Independent Causal Mechanisms. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:4036-4044
^{*28} 논문 | Kim, H. & Mnih, A., (2018). Disentangling by Factorising. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:2649-2658

^{*29} 논문 | Mirhoseini, A., Pham, H., Le, Q.V., Steiner, B., Larsen, R., Zhou, Y., Kumar, N., Norouzi, M., Bengio, S. & Dean, J., (2017). Device Placement Optimization with Reinforcement Learning. Proceedings of the 34th International Conference on Machine Learning, in PMLR 70:2430-2439
^{*30} 논문 | Kraska, T., Beutel, A., Chi, E. H., Dean, J., Polyzotis, N. (2018). The Case for Learned Index Structures. In Proceedings of the 2018 International Conference on Management of Data (SIGMOD '18). ACM, New York, NY, USA, 489-504. DOI: https://doi.org/10.1145/3183713.3196909
^{*31} 논문 | Hashemi, M., Swersky, K., Smith, J., Ayers, G., Litz, H., Chang, J., Kozyrakis, C. & Ranganathan, P., (2018). Learning Memory Access Patterns. Proceedings of the 35th International Conference on Machine Learning, in PMLR 80:1919-1928
^{*32} 논문 | Jimenez, D. A., Lin, C. Dynamic branch prediction with perceptrons. In HPCA, pp. 197-206, 2001

연구^{*33}에서 볼 수 있는 것처럼 최근 딥러닝이 발전되기 전부터 활발하게 진행되고 있었습니다. 딥러닝 모델의 발전이 하드웨어 분야에도 적용된다면 이전의 연구에서 한발 더 나아갈 수 있는 계기가 될 것입니다.

이렇게 머신러닝과 컴퓨터 하드웨어를 함께 고민하는 연구에 대해 최근 많은 관심이 모이고 있습니다. 구글에서 발표한 TPU(tensor processing unit)와 같은 특정 도메인 아키텍처(domain-specific architecture)도 이러한 연구 중 하나라고 할 수 있습니다. 제프 딘에게 이와 관련하여 “TPU처럼 머신러닝 모델을 위한 또 다른 하드웨어 개발 방향은 어떤 것이 있을까?”라는 두 번째 질문을 했을 때, “TPU와 같이 범용성과 특수성을 모두 갖고 있는 또 다른 응용 분야를 찾기가 당장은 어려워 보이나, 데이터 센터에서 사용되고 있는 TPU와 같은 선형대수가속기(linear algebra accelerator)를 저전력 종단 장치(edge device)에서 사용할 수 있도록 하는 것을 생각해볼 수 있을 것”이라는 답을 들을 수 있었는데, 이 역시 최근 구글에서 발표한 에지 TPU(Edge TPU)^{*34}를 염두에 둔 발언이 아니었을까 생각합니다.

머신러닝을 이용해 경험적인 해법을 개선하는 방법 중 하나로, 경험적인 해법을 차선택(sub-optimal expert)으로 생각하고 이를 뛰어넘는 주체(agent)를 학습하는 모방 학습(imitation learning)을 고려해볼 수 있습니다. 이번 ICML의 한 튜토리얼^{*35}에서 다뤄진 모방학습의 다양한 연구와 그 응용은 강화 학습과 상호 보완적인 역할을 통해 경험적인 해법을 향상시킬 수 있는 머신러닝 모델의 개발에 대한 기대를 높였습니다.

마치며

학회에 참석하면 즐거운 일 중 하나는 비슷한 관심사를 가진 새로운 분들을 만나볼 수 있다는 것입니다. 하지만 큰 규모의 학회장에서는 아는 사람을 찾기도 쉽지 않은데요, 이번 ICML에서는 학회에서 제공한 편리한 모바일 앱을 통해 다양한 모임방이 열려서 그러한 어려움을 덜 수 있었습니다. 이번 ICML에 참석한 물리학 전공자 혹은 물리학에 관심이 많은 머신러닝 연구자들은 모바일 앱을 이용하여 의견도 교환하고 함께 점심 모임을 가지기도 하였습니다.

제가 참석했던 2016년도 ICML과 비교해볼 때, 올해의 ICML은 새로운 돌파구를 여는 연구 성과보다는 머신러닝 분야의 성숙된 분위기를 반영하는 데에 더욱 중점을 둔 것같이 여겨졌습니다. 올해 주요 학회 중 하나인 NIPS도 이와 같은 모습을 이어갈지, 아니면 깜짝 놀랄 만한 새로운 연구 결과가 공개될지 사뭇 기대가 됩니다.

^{*33} 논문 | Ipek, E., Mutlu, O., Martinez, J. F., Caruana, R., Self-Optimizing Memory Controllers: A Reinforcement Learning Approach, 2008 International Symposium on Computer Architecture, Beijing, 2008, pp.39~50. doi: 10.1109/ISCA.2008.21

^{*34} 참고 | <https://cloud.google.com/edge-tpu>

^{*35} 참고 | Imitation Learning, Y. Yue and H. M. Le, ICML 2018



〈2018 ICML을 통해 살펴보는 AI 연구 동향〉브런치로 연결되는 QR 코드입니다.