November 18, 2020

Introduction and plan

I will be going back and forth between multiple decks. I will also try a live demo which as you know, will certainly not work the one time I will want it to. There is an added problem of Teams and how it handles changes to the screen. So a few glitches but please bear with me.

Lack of blackboard for math compounded with remote presentation - feel free to ask questions. Ambitious agenda so I might not be able to get to all questions but will try. w.

Objective

The objective of this session is not to make you experts in AI or machine learning or deep neural networks. This is just to give you a flavor, an idea of what people mean when they use these terms. I will briefly address data issue but I strongly suspect that I won't be doing it justice.

I do not have an end point. There are a few items that I do wish to cover. I will let the discussion and drinks drive the agenda beyond that.

Notes about sections

Support vector machines I was all into support vector machines in 2008 - 2009. Neural networks were relegated to the backwaters of machine learning community.

Logistic planning 1991 Gulf war crisis - US forces deployed Dynamic analysis and replanning tool (DART) for transportation. They estimated that this single instance more than paid for DARPA's 30-year investment in AI.

Graphs Talk about max flow and min cut problem.

Convolution network

Discuss why architecture matters.

- Exploit relationships better
- Numerical stability/ease of computation.

ImageNet challenge

- Describe the challenge
- Start taking about what happened in 2012

Transfer learning

Motivation

- People not only build models but also make the trained weights available. We will see a little bit of pytorch code. Data, fine tuning and execution all reused.
- We may not have enough data to train a deep model.
- Our task can exploit features detected by an existing pretrained model.

Adversarial example

- Start with Rohan's work
- Introduce adversarial network
- Discuss stop sign, trucks with LCDs

References

[1] V. Dumoulin and F. Visin, "A guide to convolution arithmetic for deep learning," 2018.

[2] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, vol. 86, pp. 2278–2324, Nov 1998.

[3] I. Goodfellow, J. Shlens, and C. Szegedy, "Explaining and harnessing adversarial examples," in *International Conference on Learning Representations*, 2015.

[4] A. Kurakin, I. Goodfellow, and S. Bengio, "Adversarial examples in the physical world," *ICLR Workshop*, 2017.

[5] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. The MIT Press, 2016.

[6] I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to sequence learning with neural networks," in *Advances in Neural Information Processing Systems 27* (Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, eds.), pp. 3104–3112, Curran Associates, Inc., 2014.

[7] S. J. Russell and P. Norvig, *Artificial Intelligence: a modern approach*. Pearson, 3 ed., 2009.