What’s scary about deep learning?

Ju Sun, PhD
Assistant Professor
Department of Computer Science & Engineering
Department of Neurosurgery

March 19, 2021
What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
Brain neural networks

Credit: Max Pixel
Deep neural networks

Brain neural networks

Artificial neural networks

Credit: Max Pixel
Deep neural networks

Brain neural networks

Artificial neural networks

Why called **artificial**?

- (Over-)simplification on neural level
- (Over-)simplification on connection level
Three pillars

data
Three pillars

data
Key ingredients of DL have been in place for 25-30 years:

<table>
<thead>
<tr>
<th>Landmark</th>
<th>Emblem</th>
<th>Epoch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neocognitron</td>
<td>Fukushima</td>
<td>1980</td>
</tr>
<tr>
<td>CNN</td>
<td>Le Cun</td>
<td>mid 1980’s</td>
</tr>
<tr>
<td>Backprop</td>
<td>Hinton</td>
<td>mid 1980’s</td>
</tr>
<tr>
<td>SGD</td>
<td>Le Cun, Bengio etc</td>
<td>mid 1990’s</td>
</tr>
<tr>
<td>Various</td>
<td>Schmidhuber</td>
<td>mid 1980’s</td>
</tr>
<tr>
<td>CTF</td>
<td>DARPA etc</td>
<td>mid 1980’s</td>
</tr>
</tbody>
</table>
Key ingredients of DL have been in place for 25-30 years:

<table>
<thead>
<tr>
<th>Landmark</th>
<th>Emblem</th>
<th>Epoch</th>
</tr>
</thead>
<tbody>
<tr>
<td>Neocognitron</td>
<td>Fukushima</td>
<td>1980</td>
</tr>
<tr>
<td>CNN</td>
<td>Le Cun</td>
<td>mid 1980's</td>
</tr>
<tr>
<td>Backprop</td>
<td>Hinton</td>
<td>mid 1980's</td>
</tr>
<tr>
<td>SGD</td>
<td>Le Cun, Bengio etc</td>
<td>mid 1990's</td>
</tr>
<tr>
<td>Various</td>
<td>Schmidhuber</td>
<td>mid 1980's</td>
</tr>
<tr>
<td>CTF</td>
<td>DARPA etc</td>
<td>mid 1980's</td>
</tr>
</tbody>
</table>

data + specialized hardware + specialized software
What’s good about DL?

DL leads to many things ...

**Revolution:** a great change in conditions, ways of working, beliefs, etc. that affects large numbers of people – *from the Oxford Dictionary*

Terrence Sejnowski (Salk Institute)
DL leads to hope

Academic breakthroughs

image classification
DL leads to hope

Academic breakthroughs

ImageNet Challenge - Classification Error

- NEC-UIUC
- VGRE
- Supervision
- VGG
- Clarifai
- TSM
- Temp-Seg

Word Error Rate

- CTS
- BN

image classification

speech recognition credit: IBM
DL leads to hope

Academic breakthroughs

- **Image classification**
- **Speech recognition**

Go game (2017)

Credit: IBM
DL leads to hope

Academic breakthroughs

- ImageNet Challenge - Classification Error
- Word Error Rate

- **image classification**
- **speech recognition**
  - credit: IBM
- Go game (2017)
- **image generation**
  - credit: I. Goodfellow

- Odena et al 2016
- Miyato et al 2017
- Zhang et al 2018
Commercial breakthroughs ...

self-driving vehicles  credit: wired.com
DL leads to hope

Commercial breakthroughs ...

self-driving vehicles  credit: wired.com  smart-home devices  credit: Amazon
DL leads to hope

Commercial breakthroughs ...

self-driving vehicles  credit: wired.com

smart-home devices  credit: Amazon

healthcare  credit: Google AI
DL leads to hope

Commercial breakthroughs ...

self-driving vehicles  credit: wired.com
smart-home devices  credit: Amazon
healthcare  credit: Google AI
robotics  credit: Cornell U.
DL leads to productivity

Papers are produced at an overwhelming rate
DL leads to productivity

Papers are produced at an overwhelming rate

400 \times 0.8 \times 52/140000 \approx 11.9\%

DL Supremacy!?
DL leads to fame

For conceptual and engineering breakthroughs that have made deep neural networks a critical component of computing.

Turing Award 2018  credit: ACM.org
Citation: For conceptual and engineering breakthroughs that have made deep neural networks a critical component of computing.
DL leads to frustration

esp. for academic researchers ...

It’s working amazingly well, but we don’t understand why

Deep, Deep Trouble

Deep Learning’s Impact on Image Processing, Mathematics, and Humanity

By Michael Elad

I am really confused. I keep changing my opinion on a daily basis, and I cannot seem to settle on one solid view of this puzzle. No, I am not talking about world politics or the current U.S. president, but rather something far more critical to humankind, and more specifically to our existence and work as engineers and researchers. I am talking about...deep learning.

While you might find the above statement rather bombastic and overstated, deep learning indeed raises several critical questions we must address. In the following paragraphs, I hope to expose one key conflict related to the emergence of this field, which is relevant to researchers in the image processing community.

First, a few words about deep learning to put our discussion into perspective. Neural networks have been around for decades, proposing a universal learning mechanism that could, in principle, fit to any learnable data source. In its feed-forward architecture, layers of perceptrons—also referred to as neurons—first perform weighted averaging...
DL leads to new sciences

- chemistry
- astronomy
- applied math
- social science
DL leads to money

- Funding
- Investment
- Job opportunities
A brief history of AI

- First Computer (ENIAC)
- First NN
- Symbolic AI
- Birth of AI
- 1st AI Winter (1974)
- 2nd AI Winter
- Machine Learning
- Turing Test
- Perceptron
- Expert System
- 1950
- 1970
- 1980
- 1990
- 2010
- Deep Learning, Data Science
- Now
- 2030
- ?
Outline

What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
Elon Musk says full self-driving Tesla tech 'very close'

9 July 2020

Tesla will be able to make its vehicles completely autonomous by the end of this year, founder Elon Musk has said.
Elon Musk says full self-driving Tesla tech 'very close'

Tesla will be able to make its vehicles completely autonomous by the end of this year, founder Elon Musk has said.

BBC.com
How it works?
How robust?
How robust?

FOOLING THE AI

Deep neural networks (DNNs) are brilliant at image recognition — but they can be easily hacked.

These stickers made an artificial-intelligence system read this stop sign as ‘speed limit 45’.
Robustness to natural variations?

<table>
<thead>
<tr>
<th>Method</th>
<th>Reference</th>
<th>Standalone?</th>
<th>mCE</th>
<th>Clean Error</th>
</tr>
</thead>
<tbody>
<tr>
<td>DeepAugment+AugMix</td>
<td>Hendrycks et al.</td>
<td>No</td>
<td>53.6%</td>
<td>24.2%</td>
</tr>
<tr>
<td>Assemble-ResNet50</td>
<td>Lee et al.</td>
<td>No</td>
<td>56.5%</td>
<td>17.90%</td>
</tr>
<tr>
<td>ANT (3x3)</td>
<td>Rusak and Schott et al.</td>
<td>Yes</td>
<td>63%</td>
<td>23.9%</td>
</tr>
</tbody>
</table>
What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
Put DL into good use

solve difficult scientific and engineering problems

chemistry

applied math

astronomy

social science
Inverse problems: given $f$ and $y = f(x)$, estimate $x$
Inverse problems: given $f$ and $y = f(x)$, estimate $x$
Inverse problems: given \( f \) and \( y = f(x) \), estimate \( x \)
Inverse problems: given $f$ and $y = f(x)$, estimate $x$
**Inverse problems:** given $f$ and $y = f(x)$, estimate $x$

Symmetries/ill-posedness in practical problems
Lots of suboptimal practical usage...

**e.g., phase retrieval:** given $Y = |\mathcal{F}(X)|^2$, recover $X$
What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
I heard reiteration of the following claim: Complex theories do not work; simple algorithms do.

I would like to demonstrate that in the area of science a good old principle is valid:

Nothing is more practical than a good theory.

— Vladimir N Vapnik, who invented support vector machines and statistical learning theory
(Fourier) phase retrieval:

For a complex signal $x \in \mathbb{C}^n$, given $|F x|^2$, recover $x$. 
Insights from randomness?

(Fourier) phase retrieval:

For a complex signal $x \in \mathbb{C}^n$, given $|\mathcal{F}x|^2$, recover $x$.

Generalized phase retrieval:

For a complex signal $x \in \mathbb{C}^n$, given $|Ax|^2$ where $A$ contains randomness, recover $x$. 
(Fourier) phase retrieval:

For a complex signal $x \in \mathbb{C}^n$, given $|F_x|^2$, recover $x$.

Generalized phase retrieval:

For a complex signal $x \in \mathbb{C}^n$, given $|Ax|^2$ where $A$ contains randomness, recover $x$.

coded-diffraction
CDI [Candès et al., 2015]
Insights from the Gaussian case?

\[ y = |a_i^* x| \text{ for } i = 1, \ldots, m \text{ where } a_i \text{'s complex Gaussian vectors} \]
Insights from the Gaussian case?

\[ y = |a_i^* x| \text{ for } i = 1, \ldots, m \text{ where } a_i \text{'s complex Gaussian vectors} \]

- many beautiful mathematical results [Chi et al., 2018, Fannjiang and Strohmer, 2020]
Insights from the Gaussian case?

\[ y = |a_i^* x| \] for \( i = 1, \ldots, m \) where \( a_i \)'s complex Gaussian vectors

- many beautiful mathematical results [Chi et al., 2018, Fannjiang and Strohmer, 2020]

Example 1: a beautiful init + local descent result
Insights from the Gaussian case?

\[ y = |a_i^* x| \text{ for } i = 1, \ldots, m \text{ where } a_i \text{'s complex Gaussian vectors} \]

- many beautiful mathematical results [Chi et al., 2018, Fannjiang and Strohmer, 2020]

**Example 2: my own results**

\[
\min_{z \in \mathbb{C}^n} f(z) = \frac{1}{2m} \sum_{k=1}^{m} \left(y_k^2 - |a_k^* z|^2\right)^2.
\]

**Theorem ([Sun et al., 2016])**

When \( a_k \)'s generic and \( m \) large, with high probability

all local minimizers are global, all saddles are nice.
I was happy until ...
I was happy until ...
I find it interesting people have tried to analyze Gaussian phase retrieval. —Fineup
Take-home messages

I find it interesting people have tried to analyze Gaussian phase retrieval. —Fineup

Beautiful mathematical results gathered so far
[Chi et al., 2018, Fannjiang and Strohmer, 2020]

James R Fienup
(U. Rochester)
Take-home messages

I find it interesting people have tried to analyze Gaussian phase retrieval. —Fineup

Beautiful mathematical results gathered so far [Chi et al., 2018, Fannjiang and Strohmer, 2020]

But we made little progress in solving Fourier PR

James R Fienup
(U. Rochester)
Theories for DL?

COLLOQUIUM ON THE SCIENCE OF DEEP LEARNING

Theoretical issues in deep networks

Tomaso Poggio, Andrzej Banburski, and Qianli Liao
+ See all authors and affiliations

PNAS December 1, 2020 117 (48) 30039-30045; first published June 9, 2020; https://doi.org/10.1073/pnas.1907369117

Edited by David L. Donoho, Stanford University, Stanford, CA, and approved May 1, 2020 (received for review June 3, 2019)

Abstract

While deep learning is successful in a number of applications, it is not yet well
CS18980: Topics in modern machine learning (Fall 2021)

—put classic statistical learning theory in the context of modern deep learning, and put deep learning in the context of classic statistical learning theory

- Approximation theory for DL
- Optimization & Generalization
  - Classic theory: uniform convergence, VC-dim, Radamachar complexity, PAC-Bayesian bound, margin-based (½)
  - DL: implicit regularization, objection to implicit regularization, double descent
    - Understanding Deep Learning (Still) Requires Rethinking Generalization https://dl.acm.org/doi/pdf/10.1145/3446776
  - Generative prior: DIP and variants
  - Neural tangent kernels, lazy training
  - Robustness, interpretability, explainability, fairness, privacy, causality
  - Learning with imbalance and label noise
  - Learning with symmetries --- input (invariance & equivariance) & output
  - Landscape analysis (Batch normalization)
    - Why Flatness Correlates With Generalization For Deep Neural Networks https://arxiv.org/abs/2103.06219
  - Transfer learning & Domain adaptation
  - Self-supervised learning (contrastive learning)
  - Generative models (Normalization flow, GANs & VAE)
  - Use DL for solving hard problems (Maxcut, combinatorial problems, FPR)
  - 2nd order methods for DL (classification, inverse problems, etc)

- Scattering transform
- Randomized numerical linear algebra & concentration of measure: dimension reduction, sketched-based optimization

CSCI 8980 Notes (2021 Fall)
Outline

What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
We’re running short of doctors!

### Projected Physician Shortages by 2033

<table>
<thead>
<tr>
<th>Medical Areas</th>
<th>Shortage Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary care</td>
<td>Between 21,400 and 55,200 physicians</td>
</tr>
<tr>
<td>Nonprimary care specialties</td>
<td>Between 33,700 and 86,700 physicians</td>
</tr>
<tr>
<td>- Surgical specialties</td>
<td>Between 17,100 and 28,700 physicians</td>
</tr>
<tr>
<td>- Medical specialties</td>
<td>Between 9,300 and 17,800 physicians</td>
</tr>
<tr>
<td>- Other specialties (i.e., pathology, radiology, psychiatry)</td>
<td>Between 17,100 and 41,900 physician</td>
</tr>
</tbody>
</table>

Source: Assoc. American Medical Colleges
Perils and promise

Perils

- **Small** datasets (sometimes)
- **Unbalanced** datasets (almost always)
- **Noisy** datasets (almost always)
Perils and promise

Perils

- **Small** datasets (sometimes)
- **Unbalanced** datasets (almost always)
- **Noisy** datasets (almost always)

Promise

- Confined domain

- Robustness — noise less wild
What we’re up to

COVID-19 Diagnosis and Prognosis (deployed in 12 M Health Fairview H’s)

Collaborative/federated learning for medical imaging

Fracture detection in critical/trauma care
What’s good about deep learning?

Why are self-driving cars not delivered?

Are we making the best use of deep learning?

What about understanding DL?

Why AI for healthcare now?

Research of the SUN group
{machine learning, data sciences, optimization, computer vision, image/signal processing, imaging, healthcare...}

- **Representation Learning**: learn efficient representation for data
- **Computation**: compute with, often optimize with, massive amounts of data
- **Theory insights**: whenever possible/necessary
SUN group at UMN

- foundations of machine/deep learning & computer vision
  * robustness in recognition
  * novel applications and limitations
  * fast computation and theoretical insights

– application of CV and DL in healthcare
  * diagnosis and analysis of glioblastoma via brain MRI
  * fracture/COVID 19 detection from chest X-rays/CT
  * federated learning
- foundations of machine/deep learning & computer vision
  * robustness in recognition
  * novel applications and limitations
  * fast computation and theoretical insights
- application of CV and DL in healthcare
  * diagnosis and analysis of gliobastoma via brain MRI
  * fracture/COVID 19 detection from chest X-rays/CT
  * federated learning
CSCI8980: Topics in modern machine learning (Fall 2021)

—put classic statistical learning theory in the context of modern deep learning, and put deep learning in the context of classic statistical learning theory

- Approximation theory for DL
- Optimization & Generalization
  - Classic theory: uniform convergence, VC-dim, Radamachar complexity, PAC-Bayesian bound, margin-based (¼)
  - DL: implicit regularization, objection to implicit regularization, double descent
    - Understanding Deep Learning (Still) Requires Rethinking Generalization https://dl.acm.org/doi/pdf/10.1145/3446776
  - Generative prior: DIP and variants
  - Neural tangent kernels, lazy training
  - Robustness, interpretability, explainability, fairness, privacy, causality
  - Learning with imbalance and label noise
  - Learning with symmetries --- input (invariance & equivariance) & output
  - Landscape analysis (Batch normalization)
    - Why Flatness Correlates With Generalization For Deep Neural Networks https://arxiv.org/abs/2103.06219
- Transfer learning & Domain adaptation
- Self-supervised learning (contrastive learning)
- Generative models (Normalization flow, GANs & VAE)
- Use DL for solving hard problems (Maxcut, combinatorial problems, FPR)
- 2nd order methods for DL (classification, inverse problems, etc)

- Scattering transform
- Randomized numerical linear algebra & concentration of measure: dimension reduction, sketched-based optimization
- Graph neural networks/NN on non-Euclidean spaces

