# Tensor networks and deep learning 

I. Oseledets<br>Skoltech, INM RAS, Moscow

3 November 2017

## Deep, Deep Trouble

Michael Elad, SIAM News, 01.05.2017

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. I am talking about ... deep learning.

For the sake of brevity, consider the classic image processing task of denoising - removing noise from an image. Researchers developed beautiful and deep mathematical ideas with tools .... In 2012, Harold Burger, Christian Schuler, and Stefan Harmeling decided to throw deep learning into this problem. The end result was a network that performed better than any known image denoising algorithm at that time.

## Deep learning

- The general paradigm is to parametrize your favourite algorithm as a (deep) neural network
- Prepare a training set of true answers
- The problem is non-convex and it is difficult to lie mathematical foundations, i.e. "guarantees" in any form


## Approximation of multivariate functions

Given a training set $\left(x_{i}, y_{i}\right), i=1, \ldots, N, x_{i} \in \mathbb{R}^{d}$ we want to build a model $f(x, w)$

Such that

$$
f\left(x_{i}, w\right)=\hat{y}_{i} \approx y_{i}
$$

in the sense of a certain loss function

$$
\sum_{i=1}^{N} \mathcal{L}\left(\hat{y}_{i}, y_{i}\right) \rightarrow \min
$$

Classification and regression are multivariate function interpolation

## Classification

Suppose that we have a classification problem and a dataset of pairs $\left\{\left(X^{(b)}, y^{(b)}\right)\right\}_{b=1}^{N}$. Let us assume that each object $X^{(b)}$ is represented as a sequence of vectors

$$
X^{(b)}=\left(\mathbf{x}_{1}, \mathbf{x}_{2}, \ldots \mathbf{x}_{d}\right), \quad \mathbf{x}_{k} \in \mathbb{R}^{n}
$$

## Example



## Example

Consider $\left\{f_{\theta_{\ell}}: \mathbb{R}^{n} \rightarrow \mathbb{R}\right\}_{\ell=1}^{m}$, which are organized into a representation map

$$
f_{\theta}: \mathbb{R}^{n} \rightarrow \mathbb{R}^{m} .
$$

A typical choice for such a map is

$$
f_{\theta}(\mathbf{x})=\sigma(A \mathbf{x}+b)
$$

## Connection between tensors and deep learning

Score functions considered in Cohen et. al, 2016 can be written in the form

$$
\begin{gathered}
l_{y}(X)=\left\langle\mathcal{W}_{y}, \Phi(X)\right\rangle \\
\text { where } \\
\Phi(X)^{i_{1} i_{2} \ldots i_{d}}=f_{\theta_{i_{1}}}\left(\mathbf{x}_{1}\right) f_{\theta_{i_{2}}}\left(\mathbf{x}_{2}\right) \ldots f_{\theta_{i_{d}}}\left(\mathbf{x}_{d}\right)
\end{gathered}
$$

## Connection between tensors and deep learning

$$
l_{y}(X)=\left\langle\mathcal{W}_{y}, \Phi(X)\right\rangle
$$

We put low-rank constraints on $\mathcal{W}$ and get different neural networks.

## Canonical format and shallow network

N. Cohen, A. Shashua et. al provided an interpretation of the canonical format as a shallow neural network with a product pooling

$$
A\left(i_{1}, \ldots, i_{d}\right) \approx \sum_{\alpha=1}^{r} U_{1}\left(i_{1}, \alpha\right) U_{2}\left(i_{2}, \alpha\right) \ldots U_{d}\left(i_{d}, \alpha\right)
$$



H-Tucker as a deep neural network with product pooling


## Tensor-train

TT-decomposition is defined as

$$
\begin{gathered}
A\left(i_{1}, \ldots, i_{d}\right)=G_{1}\left(i_{1}\right) \ldots G_{d}\left(i_{d}\right) \\
G_{k}\left(i_{k}\right) \text { is } r_{k-1} \times r_{k}, r_{0}=r_{d}
\end{gathered}
$$

Known for a long time as matrix product state in solid state physics.

## Tensor-train as recurrent neural network

$$
\begin{aligned}
& A\left(i_{1}, \ldots, i_{d}\right)=G_{1}\left(i_{1}\right) \ldots G_{d}\left(i_{d}\right),
\end{aligned}
$$

## Expressive power result

We prove that given a random $d$-dimensional tensor in the TT format with ranks $\mathbf{r}$ and modes $n$, with probability 1 this tensor will have exponentially large CP-rank.

## Lemma

$$
\begin{aligned}
& \text { Let } \mathcal{X}^{i_{1} i_{2} \ldots i_{d}} \text { and } \\
& \operatorname{rank}_{C P} \mathcal{X}=r .
\end{aligned}
$$

Then for any matricization $\mathcal{X}^{(s, t)}$

$$
\operatorname{rank} \mathcal{X}^{(s, t)} \leq r,
$$

where ordinary matrix rank is assumed.

## Theorem

Suppose that $d=2 k$ is even. Define the following set

$$
\begin{gathered}
B=\left\{\mathcal{X} \in \mathcal{M}_{\mathbf{r}}: \operatorname{rank}_{C P} \mathcal{X}<q^{\frac{d}{2}}\right\}, \\
\text { where } q \underset{\text { Then }}{\min \{n, r\}} . \\
\mu(B)=0,
\end{gathered}
$$

where $\mu$ is the standard Lebesgue measure on $\mathcal{M}_{r}$.

## Idea of the proof

We would like to show that that for $s=\{1,3, \ldots d-1\}$,

$$
\begin{gathered}
t=\{2,4, \ldots d\} \text { the following set } \\
B^{(s, t)}=\left\{\mathcal{X} \in \mathcal{M}_{\mathbf{r}}: \operatorname{rank} \mathcal{X}^{(s, t)} \leq q^{\frac{d}{2}}-1\right\} \\
\text { has measure } 0
\end{gathered}
$$

We have

$$
B \subset B^{(s, t)}
$$

$$
\text { so if } \mu\left(B^{(s, t)}\right)=0 \text { then } \mu(B)=0 \text { as well. }
$$

## Idea of the proof

- To show that $\mu\left(B^{(s, t)}\right)=0$ it is sufficient to find at least one $\mathcal{X}$ such that rank $\mathcal{X}^{(s, t)} \geq q^{\frac{d}{2}}$.
- This follows from the fact that $B^{(s, t)}$ is an algebraic subset of the irreducible algebraic variety $\mathcal{M}_{\mathbf{r}}$, so it is either equal to $\mathcal{M}_{r}$ or has measure 0 .


## Example of a tensor

$$
\begin{align*}
& G_{1}^{i_{1} \alpha_{1}}=\delta_{i_{1} \alpha_{1}}, \quad G_{1} \in \mathbb{R}^{1 \times n \times r} \\
& G_{k}^{\alpha_{k-1} i_{k} \alpha_{k}}=\delta_{i_{k} \alpha_{k-1}}, \quad G_{k} \in \mathbb{R}^{r \times n \times 1}, k=2,4,6, \ldots, d-2 \\
& G_{k}^{\alpha_{k-1} i_{k} \alpha_{k}}=\delta_{i_{k} \alpha_{k}}, \quad G_{k} \in \mathbb{R}^{1 \times n \times r}, k=3,5,7, \ldots, d-1 \\
& G_{d}^{\alpha_{d-1} i_{d}}=\delta_{i_{d} \alpha_{d-1}}, \quad G_{d} \in \mathbb{R}^{r \times n \times 1} \tag{1}
\end{align*}
$$

## Connection

Table: Correspondence between languages of Tensor Analysis and Deep Learning.

## Tensor Decompositions

CP-decomposition TT-decomposition HT-decomposition
rank of the decomposition

## Deep Learning

shallow network
RNN
CNN
width of the network

## Expressive power

Table: Comparison of the expressive power of various networks. Given a network, specified in a column, rows correspond to the upper bound on the width of the equivalent network of other type.

TT-Network $(r) \quad$ HT-Network $(r) \quad$ CP-Network $(r)$

| TT-Network | $r$ | $r^{\log _{2} d}$ | $r$ |
| :--- | :---: | :---: | :--- |
| HT-Network | $r^{2}$ | $r$ | $r$ |
| CP-Network | $\geq r^{\frac{d}{2}}$ | $\geq r^{\frac{d}{2}}$ | $r$ |

## Why tensor networks are good

Low-rank tensor decompositions (and problems with them) can be solved using efficient linear algebra tools.

## Simplest tensor network

The simplest tensor network is matrix factorization:

$$
A=U V^{\top}
$$

## Why matrix factorization is great

## $A \approx U V^{\top}$

- Best factorization by SVD
- Riemannian manifold structure
- Nice convex relaxation (nuclear norm)
- Cross approximation / skeleton decomposition


## Cross approximation / skeleton decomposition

One of underestimated matrix facts:
If a matrix is rank $r$, it can be represented as

$$
A=C \widehat{A}^{-1} R
$$

where $C$ are some $r$ columns of $A, R$ are some rows of $A, \widehat{A}$ is a submatrix on the intersection.

## Maximum-volume principle

Goreinov, Tyrtyshnikov, 2001 have shown:
If $\widehat{A}$ has maximal volume, then

$$
\left\|A-A_{\text {skel }}\right\|_{C} \leq(r+1) \sigma_{r+1}
$$

Way to compare submatrices!

## Riemannian framework

Low-rank matrices form a manifold Standard: $F(X)=F\left(U V^{\top}\right) \rightarrow \min$


Riemannian:

## Riemannian word embedding

Example: Riemannian Optimization for Skip-Gram Negative Sampling A Fonarev, O Hrinchuk, G Gusev, P Serdyukov arXiv:1704.08059, ACL 2017.

We treated SGNS as implicit matrix factorization and solved in using Riemannian optimization.

## Negative sampling

Words and context (nearby words)

$$
\begin{gathered}
X=W C^{T}=\left(x_{w c}\right), x_{w c}=\langle\mathrm{w}, \mathrm{c}\rangle \\
\mathcal{M}_{d}=\left\{X \in \mathbb{R}^{n \times m}: \operatorname{rank}(X)=d\right\} \\
F(X)=\sum_{w \in V_{W}} \sum_{c \in V_{C}}\left(\# ( w , c ) \left(\log \sigma\left(x_{w c}\right)+\right.\right. \\
\left.\left.+k \frac{\#(w) \#(c)}{|D|} \log \sigma\left(-x_{w c}\right)\right)\right) \rightarrow \max _{X \in \mathcal{M}_{d}}
\end{gathered}
$$

## Results

|  |  |  |  |  |  |
| :---: | :---: | :---: | :---: | :---: | :---: |
| SGD-SGNS | usa |  |  |  |  |
| Neighbors | Dist. | SVD-SPPMI | RO-SGNS |  |  |
| akron | 0.536 | wisconsin | 0.700 | georgia | 0.707 |
| midwest | 0.535 | delaware | 0.693 | delaware | 0.706 |
| burbank | 0.534 | ohio | 0.691 | maryland | 0.705 |
| nevada | 0.534 | northeast | 0.690 | illinois | 0.704 |
| arizona | 0.533 | cities | 0.688 | madison | 0.703 |
| uk | 0.532 | southwest | 0.684 | arkansas | 0.699 |
| youngstown | 0.532 | places | 0.684 | dakota | 0.690 |
| utah | 0.530 | counties | 0.681 | tennessee | 0.689 |
| milwaukee | 0.530 | maryland | 0.680 | northeast | 0.687 |
| headquartered | 0.527 | dakota | 0.674 | nebraska | 0.686 |

Table: Examples of the semantic neighbors for "usa".

## Tensor factorization

## Tensor factorization: we want numerical tools of the same quality

## Classical attempt

Matrix case:

$$
A(i, j)=\sum_{\alpha=1}^{r} U(i, \alpha) V(j, \alpha)
$$

CP-decomposition:

$$
A(i, j, k)=\sum_{\alpha=1}^{r} U(i, \alpha) V(j, \alpha) W(k, \alpha)
$$

Tucker decomposition:

$$
A(i, j, k)=\sum_{\alpha, \beta, \gamma=1}^{r} G(\alpha, \beta, \gamma) U(i, \alpha) V(j, \beta) W(k, \gamma)
$$

## CP-decomposition has bad properties!

- Best rank- $r$ approximation may not exist
- Algorithms may converge very slowly (swamp behaviour)
- No finite-step completion procedure.


## Example where CP decomposition is not known

Consider a $9 \times 9 \times 9$ tensor A with slices

$$
A_{i}=E_{i} \otimes I_{3}, \quad i=1, \ldots, 9
$$

and $E_{3}$ has only one identity element.
It is known that CP-rank of A is $\leq 23$ and $\geq 20$.

## Example where CP decomposition does not exist

Consider

$$
T=a \otimes b \otimes \ldots \otimes b+\ldots+b \otimes \ldots \otimes a
$$

Then,
$P(t)=\otimes_{k=1}^{d}(b+t a), \quad P^{\prime}(0)=T=\frac{P(h)-P(0)}{h}+\mathcal{O}(h)$.
Can be approximated with rank-2 with any accuracy, but no exact decomposition of rank less than $d$ exist!

## Our idea

Our idea was to build tensor decompositions using well-established matrix tools.

## Reshaping tensor into matrix

Let reshape an $n \times n \times \ldots \times n$ tensor into a $n^{d / 2} \times n^{d / 2}$ matrix $A$ :

$$
\mathbb{A}(\mathcal{J}, \mathcal{J})=A\left(i_{1} \ldots i_{k} ; i_{k+1} \ldots i_{d}\right)
$$

and compute low-rank factorization of $\mathbb{A}$ :

$$
\mathbb{A}(\mathcal{J}, \mathcal{J}) \approx \sum_{\alpha=1}^{r} U(\mathcal{J}, \alpha) V(\mathcal{J}, \alpha)
$$

## Recursion

If we do it recursively, we get $r^{\log d}$ complexity If we do it smart, we get $d n r^{3}$ complexity:

- Tree-Tucker format (Oseledets, Tyrtyshnikov, 2009)
- H-Tucker format (Hackbusch, Kuhn, Grasedyck, 2011)
- Simple but powerful version: Tensor-train format (Oseledets, 2009)


## Properties of the TT-format

- TT-ranks are ranks of matrix unfoldings
- We can do basic linear algebra
- We can do rounding
- We can recover a low-rank tensor from $\mathcal{O}\left(d n r^{2}\right)$ elements
- Good for rank-constrained optimization
- There are classes of problems where $r_{k} \sim \log ^{s} \varepsilon^{-1}$
- We have MATLAB, Python and Tensorflow toolboxes!


## TT-ranks are matrix ranks

$$
\begin{gathered}
\text { Define unfoldings: } \\
A_{k}=A\left(i_{1} \ldots i_{k} ; i_{k+1} \ldots i_{d}\right), n^{k} \times n^{d-k} \text { matrix }
\end{gathered}
$$

## TT-ranks are matrix ranks

Define unfoldings:
$A_{k}=A\left(i_{1} \ldots i_{k} ; i_{k+1} \ldots i_{d}\right), n^{k} \times n^{d-k}$ matrix Theorem: there exists a TT-decomposition with TT-ranks

$$
r_{k}=\operatorname{rank} A_{k}
$$

## TT-ranks are matrix ranks

The proof is constructive and gives the TT-SVD algorithm!

## TT-ranks are matrix ranks

No exact ranks in practice - stability estimate!

## TT-ranks are matrix ranks

Physical meaning of ranks of unfoldings is entanglement: we split the system into two halves, and if rank is 1, they are independent.

## Approximation theorem

$$
\begin{gathered}
\text { If } A_{k}=R_{k}+E_{k},\left\|E_{k}\right\|=\varepsilon_{k} \\
\qquad\|\mathrm{~A}-\mathrm{TT}\|_{F} \leq \sqrt{\sum_{k=1}^{d-1} \varepsilon_{k}^{2}}
\end{gathered}
$$

## TT-SVD

Suppose, we want to approximate:

$$
A\left(i_{1}, \ldots, i_{d}\right) \approx G_{1}\left(i_{1}\right) G_{2}\left(i_{2}\right) G_{3}\left(i_{3}\right) G_{4}\left(i_{4}\right)
$$

1. $A_{1}$ is an $n_{1} \times\left(n_{2} n_{3} n_{4}\right)$ reshape of A .
2. $U_{1}, S_{1}, V_{1}=\operatorname{SVD}\left(A_{1}\right), U_{1}$ is $n_{1} \times r_{1}$ - first core
3. $A_{2}=S_{1} V_{1}^{*}, A_{2}$ is $r_{1} \times\left(n_{2} n_{3} n_{4}\right)$.

Reshape it into a $\left(r_{1} n_{2}\right) \times\left(n_{3} n_{4}\right)$ matrix
4. Compute its SVD:
$U_{2}, S_{2}, V_{2}=\operatorname{SVD}\left(A_{2}\right)$,
$U_{2}$ is $\left(r_{1} n_{2}\right) \times r_{2}$ - second core, $V_{2}$ is $r_{2} \times\left(n_{3} n_{4}\right)$
5. $A_{3}=S_{2} V_{2}^{*}$,
6. Compute its SVD:
$U_{3} S_{3} V_{3}=\operatorname{SVD}\left(A_{3}\right), U_{3}$ is $\left(r_{2} n_{3}\right) \times r_{3}, V_{3}$ is
$r_{3} \times n_{4}$

## Fast and trivial linear algebra

Addition, Hadamard product, scalar product, convolution All scale linear in $d$

## Fast and trivial linear algebra

$$
\begin{gathered}
C\left(i_{1}, \ldots, i_{d}\right)=A\left(i_{1}, \ldots, i_{d}\right) B\left(i_{1}, \ldots, i_{d}\right) \\
C_{k}\left(i_{k}\right)=A_{k}\left(i_{k}\right) \otimes B_{k}\left(i_{k}\right), \\
\text { ranks are multiplied }
\end{gathered}
$$

## Tensor rounding

A is in the TT-format with suboptimal ranks. How to reapproximate?

## Tensor rounding

$\varepsilon$-rounding can be done in $\mathcal{O}\left(d n r^{3}\right)$ operations

## Cross approximation

Recall the cross approximation
Rank- $r$ matrix can be recovered from $r$ columns and $r$ rows


## TT-cross approximation

Tensor with TT-ranks $r_{k} \leq r$ can be recovered from $\mathcal{O}\left(d n r^{2}\right)$ elements.

There are effective algorithms for computing those points in active learning fashion.

They are based on the computation of maximum-volume submatrices.

## Making everything a tensor: the QTT

Let $f(x)$ be a univariate function (say, $f(x)=\sin x$ ).
Let $v$ be a vector of values on a uniform grid with $2^{d}$ points.
Transform $v$ into a $2 \times 2 \times \ldots \times 2 d$-dimensional tensor.
Compute TT-decomposition of it!
And this is the QTT-format

## Making everything a tensor: the QTT

If $f(x)$ is such that

$$
f(x+y)=\sum_{\alpha=1}^{r} u_{\alpha}(x) v_{\alpha}(y)
$$

then QTT-ranks are bounded by $r$
Corollary:

- $f(x)=\exp (\lambda x)$
- $f(x)=\sin (\alpha x+\beta)$
- $f(x)$ is a polynomial
- $f(x)$ is a rational function


## Optimization with low-rank constraints

Tensors can be given implicitly as a solution of a certain optimization

$$
F(X) \rightarrow \min , \quad r_{k} \leq r
$$

The set of low-rank tensors is non-convex, but has efficient Riemannian structure and many fabulous unstudied geometrical properties.

## Software

- http://github.com/oseledets/TT-Toolbox - MATLAB
- http://github.com/oseledets/ttpy - Python
- https://github.com/Bihaqo/t3f - Tensor Train in Tensorflow (Alexander Novikov)


## Application of tensors

- High-dimensional, smooth functions
- Computational chemistry (electronic and molecular computations, spin systems)
- Parametric PDEs, high-dimensional uncertainty quantification
- Scale-separated multiscale problems
- Recommender systems
- Compression of convolutional layers in deep neural networks
- TensorNet (Novikov et. al) - very compact dense layers


## Type of problems we can solve

- Active tensor learning by the cross method
- Solution of high-dimensional linear systems: $A(X)=F$
- Solution of high-dimensional eigenvalue problems $A(X)=\lambda X$
- Solution of high-dimensional time-dependent problems $\frac{d A}{d t}=F(A)$ (very efficient integrator).


## Examples

Some examples of using tensor methods from different areas.

## Vibrational states

## Realistic Hamiltonian of $\mathrm{CH}_{3} \mathrm{CN}$

[P. Thomas, T. Carrington, 2015]

$$
\begin{aligned}
\mathcal{A}=\frac{1}{2} \sum_{i=1}^{12} \omega_{i}\left(-\frac{\partial^{2}}{\partial q_{i}^{2}}\right. & \left.+q_{i}^{2}\right)+\frac{1}{6} \sum_{i=1}^{12} \sum_{j=1}^{12} \sum_{k=1}^{12} \phi_{i j k}^{(3)} q_{i} q_{j} q_{k} \\
+ & \frac{1}{24} \sum_{i=1}^{12} \sum_{j=1}^{12} \sum_{k=1}^{12} \sum_{l=1}^{12} \phi_{i j k l}^{(4)} q_{i} q_{j} q_{k} q_{l}
\end{aligned}
$$

TT-rank $=[1,5,9,14,21,25,26,24,18,15,8,5,1]$

## Block eigensolvers in the the TT-format



Figure: The $E_{\text {ref }}$ are energies obtained by Smolyak quadratures [Carrington, 2011]. H-RRBPM method [Carrington, 2015].
M. Rakhuba and I. Oseledets. Calculating vibrational spectra of molecules using tensor train decomposition J. Chem. Phys. 145, 124101 (2016)

## Orbital-free DFT solver

Orbital-free DFT equation
Nonlinear eigenvalue problem:
$\left(-\frac{1}{2} \Delta+C_{F} \phi^{4 / 3}-\sum_{\alpha} \frac{Z_{\alpha}}{\left|\mathrm{r}-\mathrm{R}_{\alpha}\right|}+\int_{\mathbb{R}^{3}} \frac{\phi^{2}\left(\mathrm{r}^{\prime}\right)}{\left|\mathrm{r}-\mathrm{r}^{\prime}\right|} d \mathrm{r}^{\prime}+V_{x c}\left(\phi^{2}\right)\right) \phi=\mu \phi$

- For regular clusters of molecules density is of low QTT rank
- Standard iteration (SCF) in tensor formats is as difficult as initial problem $\Longrightarrow$ preconditioned gradient descent
- Derivative-free formulas to control accuracy


## Some results about DL

- Generalization properties of DNN
- Adversarial examples


## Generalization properties

Work by Daniil Merkulov on experimental study of generalization properties of DNN.
"Understanding Deep Learning requires rethinking generalization" - Chiyuan Zhang et al. 2016

We have firstly investigated behaviour of our simple CNN in terms of robustness to shuffling of the labels. Here, we just corrupted part of labels by defining any random number between 0 and 9 randomly.


## There are "sad" local minima on loss surfaces of NN





## Properties of "sad" points (obtained so far)

$>$ Even $l_{2}$ regularization won't hide them if we try to find them relatively far from initial point.
They are unstable (if we start stochastic algorithm with them, it will jump from such local minimum)

Training from BAD weights. 10000 iter; Test accuracy: 0.977



Robustness of learning algorithms to the noise in labels have the same form for different learning models



## Adversarial examples (joint with Valentin Khrulkov)

Suppose that we have a standard feed-forward DNN which takes a vector $x$ as the input, and outputs a vector of probabilities $p(x)$ for class labels. Our goal is given parameters $q \geq 1$ and $L>0$ produce a vector $\varepsilon$ such that

$$
\max p(x) \neq \quad \max p(x+\varepsilon), \quad\|\varepsilon\|_{q}=L
$$

for as many $x$ in a dataset as possible. Efficiency of the given universal adversarial perturbation $\varepsilon$ for the dataset $X$ of the size $N$ is called the fooling rate and is defined as

$$
\frac{|\{x \in X: \quad \max p(x) \neq \quad \max p(x+\varepsilon)\}|}{N} .
$$

## Our construction

Let us denote the outputs of the $i$-th hidden layer of the network by $f_{i}(x)$. Then we have

$$
f_{i}(x+\varepsilon)-f_{i}(x) \approx J_{i}(x) \varepsilon
$$

where

$$
J_{i}(x)=\left.\frac{\partial f_{i}}{\partial x}\right|_{x}
$$

Thus, for any $q$

$$
\begin{equation*}
\left\|f_{i}(x+\varepsilon)-f_{i}(x)\right\|_{q} \approx\left\|J_{i}(x) \varepsilon\right\|_{q} \tag{2}
\end{equation*}
$$

## Generalized singular values

$$
y=\quad \max \frac{\|A y\|_{q}}{\|y\|_{p}} .
$$

We can use generalized power method to compute it.

## Singular vectors



Figure: Universal adversarial perturbations constructed using various layers of various DNNs

## Fooling rates

| Layer name | block2_pool | block3_conv1 | block3_conv2 | block3_conv3 |
| :--- | ---: | ---: | ---: | ---: |
| Singular value | 1165.74 | 2200.08 | 3146.66 | 6282.64 |
| Fooling rate | $\mathbf{0 . 5 2}$ | 0.39 | 0.50 | 0.50 |

Table: Fooling rates for VGG-16

| Layer name | block2_pool | block3_conv1 | block3_conv2 | block3_conv3 |
| :--- | ---: | ---: | ---: | ---: |
| Singular value | 784.82 | 1274.99 | 1600.77 | 3063.72 |
| Fooling rate | $\mathbf{0 . 6 0}$ | 0.33 | 0.50 | 0.52 |

Table: Fooling rates for VGG-19

| Layer name | conv1 | res3c_branch2a | bn5a_branch2c | activation_8 |
| :--- | ---: | ---: | ---: | ---: |
| Singular value | 59.69 | 19.21 | 138.81 | 15.55 |
| Fooling rate | $\mathbf{0 . 4 4}$ | 0.35 | 0.34 | 0.34 |

Table: Fooling rates for ResNet50

