Estimating Information Flow in Deep Neural Networks

Ziv Goldfeld

MIT

56th Allerton Conference on Communication, Control, and Computing Monticello, Illinois, US

October 4th, 2018

Collaborators: E. van den Berg, K. Greenewald, I. Melnyk, N. Nguyen, B. Kingsbury and Y. Polyanskiy

• Unprecedented practical success in hosts of tasks

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?
 - What are properties of learned representations?

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - How fully trained networks process information?

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - How fully trained networks process information?

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

:

Past attempts to understand effectiveness of deep learning

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - ▶ What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

÷

- Past attempts to understand effectiveness of deep learning
 - ▶ Optimization in parameter space [Saxe'14, Choromanska'15, Advani'17]

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - ▶ What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

- Past attempts to understand effectiveness of deep learning
 - Optimization in parameter space [Saxe'14, Choromanska'15, Advani'17]
 - ► Classes of efficiently representable functions [Montufar'14, Poggio'17]

- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

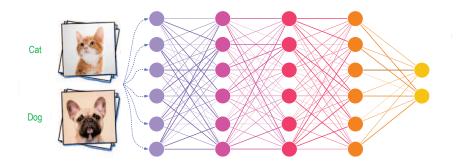
- Past attempts to understand effectiveness of deep learning
 - Optimization in parameter space [Saxe'14, Choromanska'15, Advani'17]
 - ► Classes of efficiently representable functions [Montufar'14, Poggio'17]
 - Information theory [Tishby'17, Saxe'18, Gabrié'18]

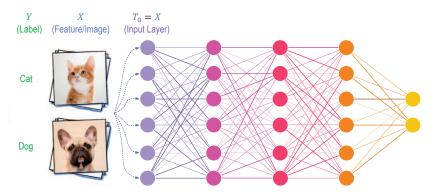
- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - ▶ What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

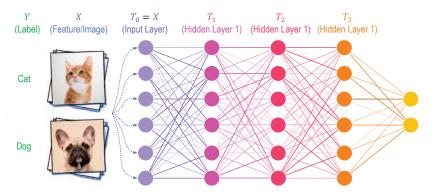
- Past attempts to understand effectiveness of deep learning
 - Optimization in parameter space [Saxe'14, Choromanska'15, Advani'17]
 - ► Classes of efficiently representable functions [Montufar'14, Poggio'17]
 - ▶ Information theory [Tishby'17, Saxe'18, Gabrié'18]

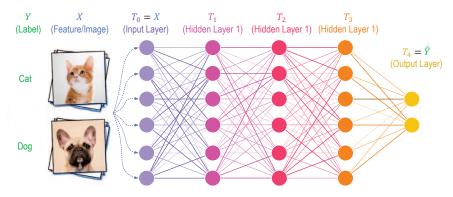
- Unprecedented practical success in hosts of tasks
- Long way to go theory-wise:
 - ▶ What drives the evolution of hidden representations?
 - What are properties of learned representations?
 - ▶ How fully trained networks process information?

- Past attempts to understand effectiveness of deep learning
 - ▶ Optimization in parameter space [Saxe'14, Choromanska'15, Advani'17]
 - ► Classes of efficiently representable functions [Montufar'14, Poggio'17]
 - Information theory [Tishby'17, Saxe'18, Gabrié'18]
- ★ Goal: Explain 'compression' in Information Bottleneck framework

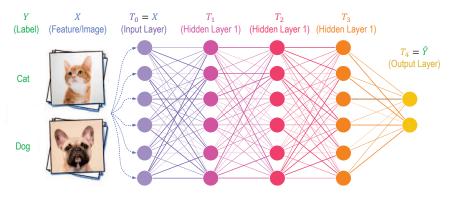




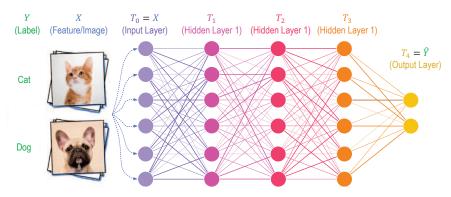




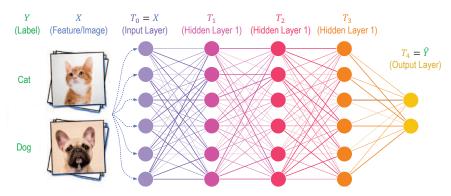
Feedforward DNN for Classification:



• Deterministic DNN: $T_{\ell} = f_{\ell}(T_{\ell-1})$ (MLP: $T_{\ell} = \sigma(W_{\ell}T_{\ell-1} + b_{\ell})$)

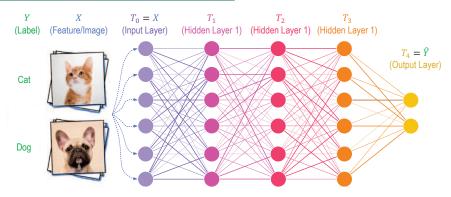


- Deterministic DNN: $T_{\ell} = f_{\ell}(T_{\ell-1})$ (MLP: $T_{\ell} = \sigma(W_{\ell}T_{\ell-1} + b_{\ell})$)
- ullet th Hidden Layer Enc & Dec: $P_{T_\ell|X}$ (enc) and $P_{\hat{Y}|T_\ell}$ (dec)



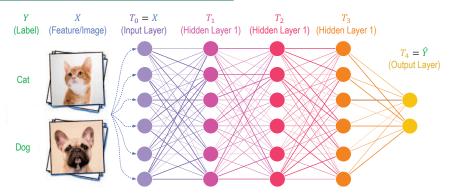
- Deterministic DNN: $T_{\ell} = f_{\ell}(T_{\ell-1})$ (MLP: $T_{\ell} = \sigma(W_{\ell}T_{\ell-1} + b_{\ell})$)
- ullet ℓ th Hidden Layer Enc & Dec: $P_{T_\ell|X}$ (enc) and $P_{\hat{Y}|T_\ell}$ (dec)
- **IB Theory:** Track MI pairs $(I(X;T_{\ell}),I(Y;T_{\ell}))$ (information plane)

Feedforward DNN for Classification:



IB Theory Claim: Training comprises 2 phases

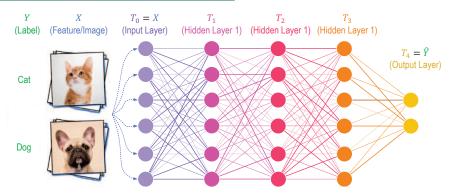
Feedforward DNN for Classification:



IB Theory Claim: Training comprises 2 phases

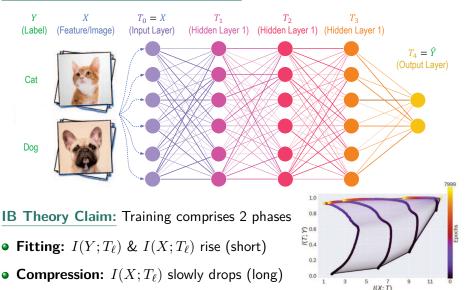
• Fitting: $I(Y;T_{\ell})$ & $I(X;T_{\ell})$ rise (short)

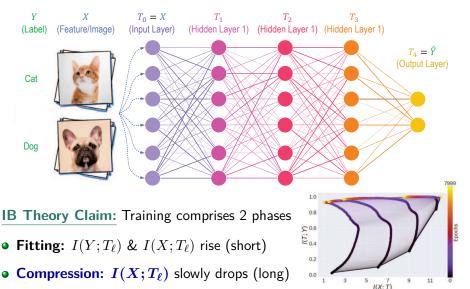
Feedforward DNN for Classification:



IB Theory Claim: Training comprises 2 phases

- Fitting: $I(Y;T_{\ell})$ & $I(X;T_{\ell})$ rise (short)
- Compression: $I(X;T_{\ell})$ slowly drops (long)





Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why?

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

• Continuous X:

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

• Continuous X: $I(X; T_{\ell}) = h(T_{\ell}) - h(T_{\ell}|X)$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

• Continuous
$$X$$
: $I(X;T_{\ell}) = h(T_{\ell}) - h(T_{\ell}|X)$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

• Continuous
$$X$$
: $I(X;T_{\ell}) = h(T_{\ell}) - h(\tilde{f}_{\ell}(X)|X)$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

$$I(X;T_{\ell}) = h(T_{\ell}) - \underbrace{h(\tilde{f}_{\ell}(X)|X)}_{=-\infty}$$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

$$I(X;T_{\ell}) = h(T_{\ell}) - h(\tilde{f}_{\ell}(X)|X) = \infty$$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

- Continuous X: $I(X;T_\ell) = h(T_\ell) h(\tilde{f}_\ell(X)|X) = \infty$
- Discrete X:

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

- Continuous X: $I(X;T_{\ell}) = h(T_{\ell}) h(\tilde{f}_{\ell}(X)|X) = \infty$
- **Discrete** X: The map $X \mapsto T_{\ell}$ is injective*

* For almost all weight matrices and bias vectors

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

- Continuous X: $I(X;T_\ell) = h(T_\ell) h(\tilde{f}_\ell(X)|X) = \infty$
- Discrete X: The map $X \mapsto T_{\ell}$ is injective $\Longrightarrow I(X; T_{\ell}) = H(X)$

* For almost all weight matrices and bias vectors

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

- Continuous X: $I(X;T_\ell) = h(T_\ell) h(\tilde{f}_\ell(X)|X) = \infty$
- Discrete X: The map $X \mapsto T_{\ell}$ is injective $\Longrightarrow I(X; T_{\ell}) = H(X)$

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

- Continuous X: $I(X;T_\ell) = h(T_\ell) h(\tilde{f}_\ell(X)|X) = \infty$
- Discrete X: The map $X \mapsto T_{\ell}$ is injective $\Longrightarrow I(X; T_{\ell}) = H(X)$

Intuition:

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

- Continuous X: $I(X;T_\ell) = h(T_\ell) h(\tilde{f}_\ell(X)|X) = \infty$
- Discrete X: The map $X \mapsto T_{\ell}$ is injective $\Longrightarrow I(X; T_{\ell}) = H(X)$

Intuition: Encoding all info. about X is arbitrarily fine variations of T_ℓ

Observation

Det. DNNs with strictly monotone nonlinearities (e.g., tanh or sigmoid)

 $\implies I(X;T_{\ell})$ is independent of the DNN parameters

Why? Formally...

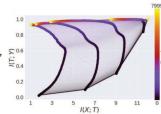
• Continuous *X*:

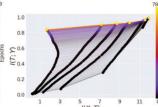
- $I(X;T_{\ell}) = h(T_{\ell}) h(\tilde{f}_{\ell}(X)|X) = \infty$
- Discrete X: The map $X \mapsto T_{\ell}$ is injective $\Longrightarrow I(X; T_{\ell}) = H(X)$

Intuition: Encoding all info. about X is arbitrarily fine variations of T_ℓ

Past Works:

[Schwartz-Ziv&Tishby'17, $\S^{0.6}_{\stackrel{\circ}{\mathfrak{S}}_{0.4}}$ Saxe et al. '18]





ullet Plots via binning-based estimator of $I(X;T_\ell)$, for $X\sim \mathsf{Unif}(\mathsf{dataset})$

• Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$

 \implies Plotted values are $I(X; Bin(T_{\ell}))$

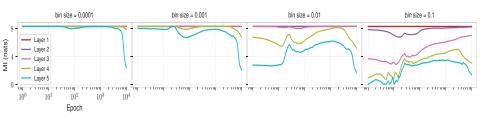
ullet Plots via binning-based estimator of $I(X;T_\ell)$, for $X\sim \mathsf{Unif}(\mathsf{dataset})$

 \implies Plotted values are $I(X; Bin(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$

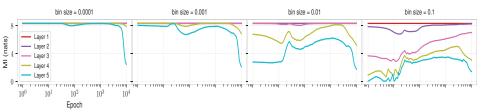
• Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$

 \implies Plotted values are $I(X; \operatorname{Bin}(T_\ell)) \stackrel{??}{pprox} I(X; T_\ell)$ No

- Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$
 - \implies Plotted values are $I(X; \operatorname{Bin}(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$ No!

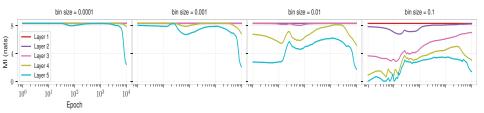


- Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$
 - \implies Plotted values are $I(X; Bin(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$ No!



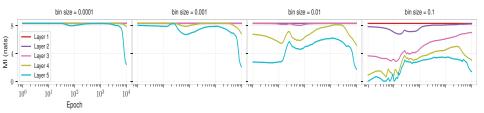
• Smaller bins \implies Closer to truth: $I(X;T_\ell)=\ln(2^{12})\approx 8.31$

- Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$
 - \implies Plotted values are $I(X; \operatorname{Bin}(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$ No!



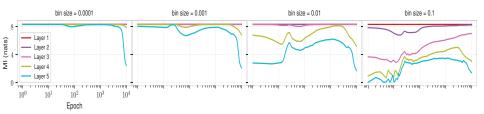
- Smaller bins \implies Closer to truth: $I(X;T_\ell)=\ln(2^{12})\approx 8.31$
- Binning introduces "noise" into estimator (not present in the DNN)

- Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$
 - \implies Plotted values are $I(X; Bin(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$ No!



- Smaller bins \implies Closer to truth: $I(X;T_\ell)=\ln(2^{12})\approx 8.31$
- Binning introduces "noise" into estimator (not present in the DNN)
- Plots showing estimation errors

- Plots via binning-based estimator of $I(X; T_{\ell})$, for $X \sim \mathsf{Unif}(\mathsf{dataset})$
 - \implies Plotted values are $I(X; Bin(T_{\ell})) \stackrel{??}{\approx} I(X; T_{\ell})$ No!



- Smaller bins \implies Closer to truth: $I(X;T_\ell)=\ln(2^{12})\approx 8.31$
- Binning introduces "noise" into estimator (not present in the DNN)
- Plots showing estimation errors
- $igoplus {f Real \ Problem:}\ I(X;T_\ell)$ is meaningless for studying the DNN

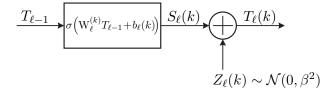
Proposed Fix: Inject (small) Gaussian noise to neurons' output

Proposed Fix: Inject (small) Gaussian noise to neurons' output

• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$

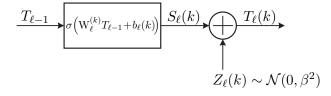
Proposed Fix: Inject (small) Gaussian noise to neurons' output

• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathrm{I})$



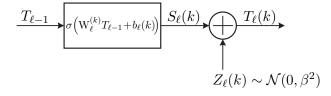
Proposed Fix: Inject (small) Gaussian noise to neurons' output

• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathrm{I})$



Proposed Fix: Inject (small) Gaussian noise to neurons' output

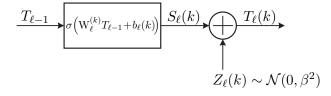
• Formally: $T_\ell = f_\ell(T_{\ell-1}) + Z_\ell$, where $Z_\ell \sim \mathcal{N}(0, \beta^2 \mathrm{I})$



- $\implies X \mapsto T_{\ell}$ is a **parametrized channel** that depends on DNN param.!
 - Operational Perspective:

Proposed Fix: Inject (small) Gaussian noise to neurons' output

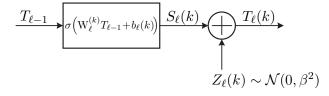
• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathrm{I})$



- Operational Perspective:
 - ▶ Performance & learned representations similar to det. DNNs ($\beta \approx 10^{-1}$)

Proposed Fix: Inject (small) Gaussian noise to neurons' output

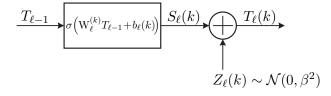
• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$



- Operational Perspective:
 - ▶ Performance & learned representations similar to det. DNNs ($\beta \approx 10^{-1}$)
 - ▶ Noise masks fine variations MI represents relevant/distingishable info.

Proposed Fix: Inject (small) Gaussian noise to neurons' output

• Formally: $T_{\ell} = f_{\ell}(T_{\ell-1}) + Z_{\ell}$, where $Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$



- Operational Perspective:
 - ▶ Performance & learned representations similar to det. DNNs ($\beta \approx 10^{-1}$)
 - ▶ Noise masks fine variations MI represents relevant/distingishable info.
 - ▶ Dropout & quantized DNNs widely used in practice \approx internal noise

• Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1})$

• Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathbf{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_\ell) = h(T_\ell) \frac{1}{m} \sum_{i=1}^m h(T_\ell|X=x_i)$

- Layer ℓ : Denote $S_\ell \triangleq f_\ell(T_{\ell-1}) \implies T_\ell = S_\ell + Z_\ell, \ Z_\ell \sim \mathcal{N}(0, \beta^2 \mathrm{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- **®** Distribution of S_{ℓ} is **extremely** complicated to compute/evaluate

- Layer ℓ : Denote $S_\ell \triangleq f_\ell(T_{\ell-1}) \implies T_\ell = S_\ell + Z_\ell, \ Z_\ell \sim \mathcal{N}(0, \beta^2 \mathrm{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- lacktright Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- \circledast But, $P_{S_{\ell}}$ and $P_{S_{\ell}|X=x_i}$ are easily sampled from via DNN fwd. pass

- Layer ℓ : Denote $S_\ell \triangleq f_\ell(T_{\ell-1}) \implies T_\ell = S_\ell + Z_\ell, \ Z_\ell \sim \mathcal{N}(0, \beta^2 \mathrm{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- ${f \$}$ Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- ${f \$}$ But, P_{S_ℓ} and $P_{S_\ell|X=x_i}$ are **easily** sampled from via DNN fwd. pass
 - ⇒ Estimate MI from samples & Exploit noisy DNN structure

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 I)$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- ${f \$}$ Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- ${f \$}$ But, P_{S_ℓ} and $P_{S_\ell|X=x_i}$ are **easily** sampled from via DNN fwd. pass
 - ⇒ Estimate MI from samples & Exploit noisy DNN structure

Differential Entropy Estimation under Gaussian Convolutions

Estimate h(S+Z) using n i.i.d. samples from $P_S \in \mathcal{F}_d$ (nonparametric class) and knowing that $Z \sim \mathcal{N}(0, \beta^2 \mathbf{I}_d)$ independent of S.

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathbf{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- ${f \$}$ Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- \circledast But, P_{S_ℓ} and $P_{S_\ell|X=x_i}$ are easily sampled from via DNN fwd. pass
 - ⇒ Estimate MI from samples & Exploit noisy DNN structure

Differential Entropy Estimation under Gaussian Convolutions

Estimate h(S+Z) using n i.i.d. samples from $P_S \in \mathcal{F}_d$ (nonparametric class) and knowing that $Z \sim \mathcal{N}(0, \beta^2 \mathbf{I}_d)$ independent of S.

Results [ZG-Greenewald-Polyanskiy'18]:

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathbf{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- ${f \$}$ Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- ${f \$}$ But, P_{S_ℓ} and $P_{S_\ell|X=x_i}$ are **easily** sampled from via DNN fwd. pass
 - ⇒ Estimate MI from samples & Exploit noisy DNN structure

Differential Entropy Estimation under Gaussian Convolutions

Estimate h(S+Z) using n i.i.d. samples from $P_S \in \mathcal{F}_d$ (nonparametric class) and knowing that $Z \sim \mathcal{N}(0, \beta^2 \mathbf{I}_d)$ independent of S.

Results [ZG-Greenewald-Polyanskiy'18]:

lacktriangle Sample complexity is exponential in d

- Layer ℓ : Denote $S_{\ell} \triangleq f_{\ell}(T_{\ell-1}) \implies T_{\ell} = S_{\ell} + Z_{\ell}, \ Z_{\ell} \sim \mathcal{N}(0, \beta^2 \mathbf{I})$
- Assume: $X \sim \mathsf{Unif}(\mathcal{X})$, where $\mathcal{X} \triangleq \{x_i\}_{i=1}^m$ is empirical dataset
- Mutual Information: $I(X;T_{\ell}) = h(T_{\ell}) \frac{1}{m} \sum_{i=1}^{m} h(T_{\ell}|X=x_i)$
- lacktrightarrow Distribution of S_ℓ is **extremely** complicated to compute/evaluate
- \circledast But, P_{S_ℓ} and $P_{S_\ell|X=x_i}$ are **easily** sampled from via DNN fwd. pass
 - ⇒ Estimate MI from samples & Exploit noisy DNN structure

Differential Entropy Estimation under Gaussian Convolutions

Estimate h(S+Z) using n i.i.d. samples from $P_S \in \mathcal{F}_d$ (nonparametric class) and knowing that $Z \sim \mathcal{N}(0, \beta^2 \mathbf{I}_d)$ independent of S.

Results [ZG-Greenewald-Polyanskiy'18]:

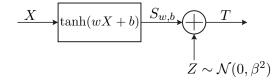
- ightharpoonup Sample complexity is exponential in d
- ▶ Absolute-error minimax risk is $O((\log n)^{d/4}/\sqrt{n})$ (all const. explicit)

$\overline{I(X;T_\ell)}$ Dynamics - Illustrative Minimal Example

Single Neuron Classification:

$I(X;T_\ell)$ Dynamics - Illustrative Minimal Example

Single Neuron Classification:



Single Neuron Classification:

• Input: $X \sim \text{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$ $\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$, $\mathcal{X}_1 \triangleq \{3\}$

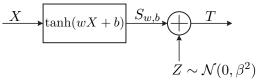
$$\frac{X}{\operatorname{tanh}(wX+b)} \xrightarrow{S_{w,b}} \frac{T}{I}$$

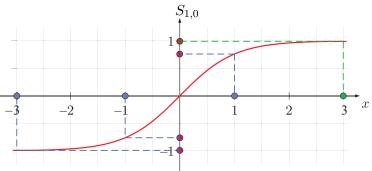
$$Z \sim \mathcal{N}(0, \beta^2)$$

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

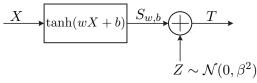


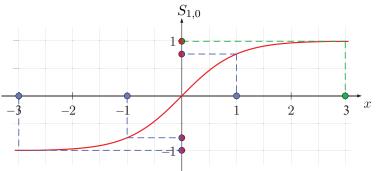


Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$



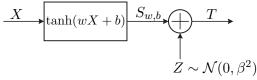


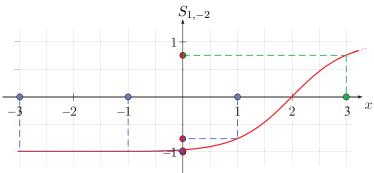
R Move \tanh center x = 2 (\iff b = -2)

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

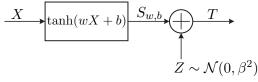


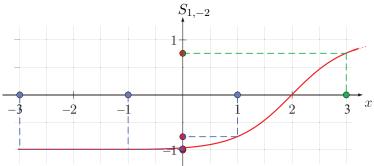


Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$



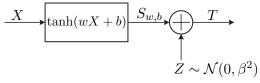


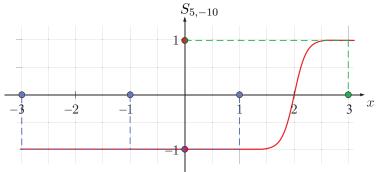
8 Sharpen \tanh transition (\iff increase w and keep b=-2w)

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

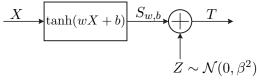


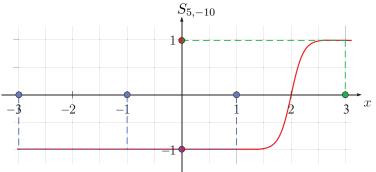


Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$$
 , $\mathcal{X}_{1} \triangleq \{3\}$





✓ Correct classification performance

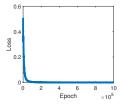
Single Neuron Classification:

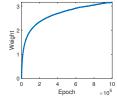
• Input: $X \sim \mathsf{Unif} \big(\mathcal{X}_{-1} \cup \mathcal{X}_1 \big)$

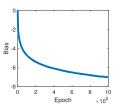
$$\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$$
 , $\mathcal{X}_{1} \triangleq \{3\}$

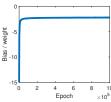
 $\begin{array}{c|c}
X & \tanh(wX+b) & S_{w,b} & T \\
\downarrow & & \downarrow \\
Z \sim \mathcal{N}(0, \beta^2)
\end{array}$

• Empirical Results:



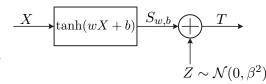






Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$ $\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$, $\mathcal{X}_1 \triangleq \{3\}$

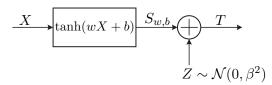


Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

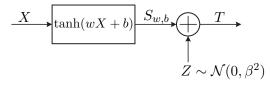
$$I(X;T) = I(X;S_{w,b} + Z)$$



Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

$$\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$$
 , $\mathcal{X}_1 \triangleq \{3\}$



$$I(X;T) = I(X; S_{w,b} + Z) = I(\tanh(wX + b); S_{w,b} + Z)$$

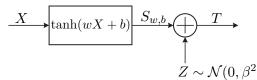
Single Neuron Classification:

• Input: $X \sim \text{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$ $\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$, $\mathcal{X}_1 \triangleq \{3\}$

$$I(X;T) = I(X;S_{w,b} + Z) = I(\tanh(wX+b);S_{w,b} + Z) = I(S_{w,b};S_{w,b} + Z)$$

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$ $\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$, $\mathcal{X}_1 \triangleq \{3\}$



• Mutual Information:

$$I(X;T) = I(X;S_{w,b} + Z) = I(\tanh(wX + b); S_{w,b} + Z) = I(S_{w,b}; S_{w,b} + Z)$$

$$\mathcal{S}_{w,b} \triangleq \{ \tanh(-3w+b), \tanh(-w+b), \tanh(w+b), \tanh(3w+b) \}$$

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$ $\mathcal{X}_{-1} \triangleq \{-3, -1, 1\}$, $\mathcal{X}_1 \triangleq \{3\}$

$$\begin{array}{c}
X \longrightarrow \tanh(wX+b) & S_{w,b} \longrightarrow & T \\
\downarrow & & \downarrow \\
Z \sim \mathcal{N}(0, \beta)
\end{array}$$

• Mutual Information:

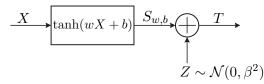
$$I(X;T) = I(X; S_{w,b} + Z) = I(\tanh(wX+b); S_{w,b} + Z) = I(S_{w,b}; S_{w,b} + Z)$$

$$\mathcal{S}_{w,b} \triangleq \{ \tanh(-3w+b), \tanh(-w+b), \tanh(w+b), \tanh(3w+b) \} \longrightarrow \{ \pm 1 \}$$

Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

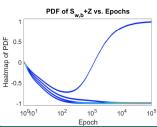
$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$



• Mutual Information:

$$I(X;T) = I(X;S_{w,b} + Z) = I(\tanh(wX+b);S_{w,b} + Z) = I(S_{w,b};S_{w,b} + Z)$$

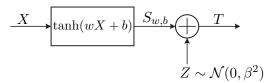
$$S_{w,b} \triangleq \{ \tanh(-3w+b), \tanh(-w+b), \tanh(w+b), \tanh(3w+b) \} \longrightarrow \{\pm 1\}$$



Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

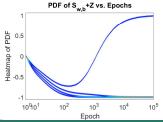
$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

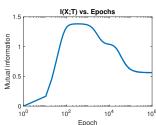


• Mutual Information:

$$I(X;T) = I(X;S_{w,b} + Z) = I(\tanh(wX+b);S_{w,b} + Z) = I(S_{w,b};S_{w,b} + Z)$$

$$S_{w,b} \triangleq \{ \tanh(-3w+b), \tanh(-w+b), \tanh(w+b), \tanh(3w+b) \} \longrightarrow \{\pm 1\}$$

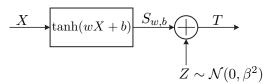




Single Neuron Classification:

• Input: $X \sim \mathsf{Unif}(\mathcal{X}_{-1} \cup \mathcal{X}_1)$

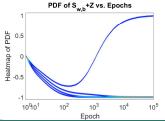
$$\mathcal{X}_{-1}\triangleq\{-3,-1,1\}$$
 , $\mathcal{X}_{1}\triangleq\{3\}$

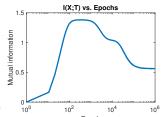


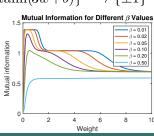
• Mutual Information:

$$I(X;T) = I(X;S_{w,b} + Z) = I(\tanh(wX+b);S_{w,b} + Z) = I(S_{w,b};S_{w,b} + Z)$$

$$\mathcal{S}_{w,b} \triangleq \big\{ \tanh(-3w+b), \tanh(-w+b), \tanh(w+b), \tanh(3w+b) \big\} \longrightarrow \{\pm 1\}$$







Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

• Binary Classification: 12-bit input & 12–10–7–5–4–3–2 MLP arch.

Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

• **Binary Classification:** 12-bit input & 12–10–7–5–4–3–2 MLP arch.

• Noise std.: Set to $\beta=0.1$

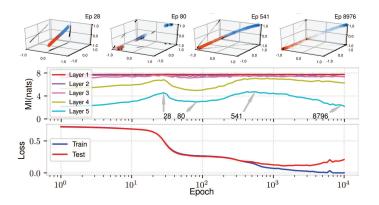
Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

• **Binary Classification:** 12-bit input & 12–10–7–5–4–3–2 MLP arch.

• Noise std.: Set to $\beta=0.1$

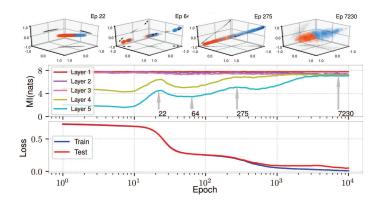
Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

- **Binary Classification:** 12-bit input & 12–10–7–5–4–3–2 MLP arch.
- Noise std.: Set to $\beta = 0.1$



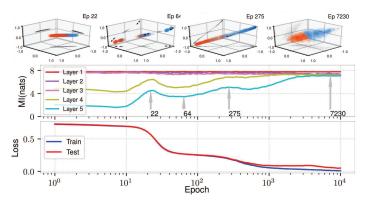
Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

- **Binary Classification:** 12-bit input & 12–10–7–5–4–3–2 MLP arch.
- Noise std.: Set to $\beta = 0.1$



Noisy version of DNN from [Schwartz-Ziv&Tishby'17]:

- **Binary Classification:** 12-bit input & 12–10–7–5–4–3–2 MLP arch.
- Noise std.: Set to $\beta = 0.1$



 \implies Compression of $I(X;T_{\ell})$ driven by clustering of representations

• $I(X;T_{\ell})$ is constant

ullet $I(X;T_\ell)$ is constant \implies Doesn't measure clustering

- ullet $I(X;T_\ell)$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):

- ullet $I(X;T_\ell)$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)

- ullet $I(X;T_\ell)$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_\ell)$ and $H(\mathsf{Bin}(T_\ell))$ highly correlated!*

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_\ell)$ and $H(\mathsf{Bin}(T_\ell))$ highly correlated!*
- Det. DNNs: $H(Bin(T_{\ell}))$ compresses (resolution wrt bins size)

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_\ell)$ and $H(\mathsf{Bin}(T_\ell))$ highly correlated!*
- Det. DNNs: $H(Bin(T_{\ell}))$ compresses (resolution wrt bins size)
- **Representation** Past Works: Estimated $I(X; T_{\ell})$ by $I(X; Bin(T_{\ell}))$

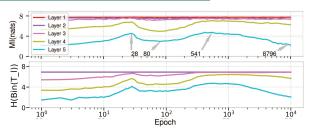
- ullet $I(X;T_\ell)$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ► Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_\ell)$ and $H(\mathsf{Bin}(T_\ell))$ highly correlated!*
- Det. DNNs: $H(Bin(T_{\ell}))$ compresses (resolution wrt bins size)
- *** Past Works:** Estimated $I(X; T_{\ell})$ by $I(X; Bin(T_{\ell})) = H(Bin(T_{\ell}))$

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - ▶ Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_{\ell})$ and $H(\mathsf{Bin}(T_{\ell}))$ highly correlated!*
- **Det. DNNs:** $H(Bin(T_{\ell}))$ compresses (resolution wrt bins size)
- **8** Past Works: Estimated $I(X; T_{\ell})$ by $I(X; Bin(T_{\ell})) = H(Bin(T_{\ell}))$
 - X Incapable of accurately estimating MI values

- \bullet $I(X;T_{\ell})$ is constant \implies Doesn't measure clustering
- Alternative measures for clustering (det. and noisy DNNs):
 - Scatter plots (up to 3D layers)
 - Within-class & In-between-class pairwise distance distribution
 - ▶ Binned entropy $H(Bin(T_{\ell}))$
- Noisy DNNs: $I(X;T_{\ell})$ and $H(\mathsf{Bin}(T_{\ell}))$ highly correlated!*
- **Det. DNNs:** $H(Bin(T_{\ell}))$ compresses (resolution wrt bins size)
- **8** Past Works: Estimated $I(X; T_{\ell})$ by $I(X; Bin(T_{\ell})) = H(Bin(T_{\ell}))$
 - X Incapable of accurately estimating MI values
 - ✓ Still, simple to compute & follows MI in tracking clustering!

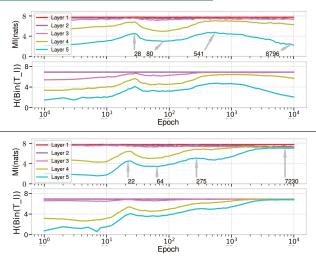
Circling back to Deterministic DNNs (Cntd.)

Comparing to Previously Shown MI Plots:



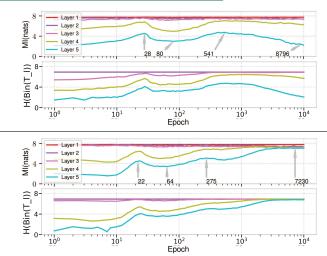
Circling back to Deterministic DNNs (Cntd.)

Comparing to Previously Shown MI Plots:



Circling back to Deterministic DNNs (Cntd.)

Comparing to Previously Shown MI Plots:



⇒ Past works we not showing MI but clustering (via binned-MI)!

• Reexamined Information Bottleneck Compression:

- Reexamined Information Bottleneck Compression:
 - lacksquare I(X;T) fluctuations in det. DNNs are theoretically impossible

Reexamined Information Bottleneck Compression:

- ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
- lacktriangle Yes, past works presented I(X;T) dynamics during training

- Reexamined Information Bottleneck Compression:
 - ▶ *I*(*X*; *T*) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs

- Reexamined Information Bottleneck Compression:
 - ▶ *I*(*X*; *T*) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - Toolkit for accurate MI estimation over this framework

- Reexamined Information Bottleneck Compression:
 - ▶ *I*(*X*; *T*) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - Toolkit for accurate MI estimation over this framework
 - ▶ Clustering of the learned representations is the source of compression

- Reexamined Information Bottleneck Compression:
 - lacksquare I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ▶ Toolkit for accurate MI estimation over this framework
 - Clustering of the learned representations is the source of compression
 - lackbox Methods to track clustering in det. DNNs (incl. $Hig(\mathsf{Bin}(T_\ell)ig)ig)$

- Reexamined Information Bottleneck Compression:
 - ▶ *I*(*X*; *T*) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ▶ Toolkit for accurate MI estimation over this framework
 - ▶ Clustering of the learned representations is the source of compression
 - lackbox Methods to track clustering in det. DNNs (incl. $Hig(\mathsf{Bin}(T_\ell)ig)ig)$
- **③** Det. DNNs cluster representations

- Reexamined Information Bottleneck Compression:
 - ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ► Toolkit for accurate MI estimation over this framework
 - Clustering of the learned representations is the source of compression
 - lacksquare Methods to track clustering in det. DNNs (incl. $Hig(\mathsf{Bin}(T_\ell)ig)ig)$
- **③ Det. DNNs cluster representations** ⇒ Clarify past observations

- Reexamined Information Bottleneck Compression:
 - ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangle Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ► Toolkit for accurate MI estimation over this framework
 - ▶ Clustering of the learned representations is the source of compression
 - ▶ Methods to track clustering in det. DNNs (incl. $H(Bin(T_{\ell}))$)
- **♦ Det. DNNs cluster representations** ⇒ Clarify past observations
- Future Research:

- Reexamined Information Bottleneck Compression:
 - ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ► Toolkit for accurate MI estimation over this framework
 - ▶ Clustering of the learned representations is the source of compression
 - ▶ Methods to track clustering in det. DNNs (incl. $H(Bin(T_{\ell}))$)
- lacktriangledown **Det. DNNs cluster representations** \Longrightarrow Clarify past observations
- Future Research:
 - ► Curse of dimensionality: How to track clustering in high-dimensions?

- Reexamined Information Bottleneck Compression:
 - ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangleright Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ► Toolkit for accurate MI estimation over this framework
 - ▶ Clustering of the learned representations is the source of compression
 - ▶ Methods to track clustering in det. DNNs (incl. $H(Bin(T_{\ell}))$)
- **③ Det. DNNs cluster representations** ⇒ Clarify past observations
 - Future Research:
 - Curse of dimensionality: How to track clustering in high-dimensions?
 - Is compression necessary? Desirable?

- Reexamined Information Bottleneck Compression:
 - ightharpoonup I(X;T) fluctuations in det. DNNs are theoretically impossible
 - lacktriangle Yes, past works presented I(X;T) dynamics during training
- Noisy DNN Framework: Studying IT quantities over DNNs
 - ► Toolkit for accurate MI estimation over this framework
 - Clustering of the learned representations is the source of compression
 - ▶ Methods to track clustering in det. DNNs (incl. $H(Bin(T_{\ell}))$)
- ★ Det. DNNs cluster representations ⇒ Clarify past observations
- Future Research:
 - ► Curse of dimensionality: How to track clustering in high-dimensions?
 - Is compression necessary? Desirable?
 - ▶ Build on findings to improve DNN training alg. and architectures