## Learning to Explain:

## An Information-Theoretic Perspective on Model Interpretation

Jianbo Chen*2 Le Song ${ }^{\ddagger} \ddagger$ § ${ }^{\ddagger}$ Martin J. Wainwright* Michael I. Jordan*<br>University of California, Berkeley*, Georgia Institute of Technology ${ }^{\frac{\ddagger}{4}}$, Ant Financial ${ }^{\S}$

## Motivation

Application of machine learning
Medicine
Financial markets
Criminal justice


Complex models:
Deep neural networks Random forests
Kernel methods


## Problem

Instancewise Feature Selection:

1. Given a machine learning model, one asks for the importance score of each feature on the prediction of a given instance.
2. Feature importance is allowed to vary across instances

## 



Existing Work and Properties
Training: Require training in advance.
Efficiency: Scalable to large data sets
Additive: Approximated by an additive model locally
Model-agnostic: Generic to black-box models.

|  | Training | Efficiency | Additive | Model-agnostic |
| :---: | :---: | :---: | :---: | :---: |
| Parzen (Baehrens et al., 2010) | Yes | High | Yes | Yes |
| Salient Map (Simonyan et al., 2013) | No | High | Yes | No |
| LRP (Bach et al., 2015) | No | High | Yes | No |
| LIME (Ribeiro et al., 2016) | No | Low | Yes | Yes |
| DeepLIFT (Shrikumar et al., 2017) | No | High | Yes | No |
| Kernel SHAP (Lundberg \& Lee, 2017) | No | Low | Yes | Yes |
| IG (Sundararajan et al., 2017) | No | Medium | Yes | No |
| L2X | Yes | High | No | Yes |

## Notations

Input $x \in \mathbb{R}^{d}$.
Model $(Y \mid x) \sim \mathbb{P}_{m}(\cdot \mid x)$,
S: A feature subse $(-x)$.
S : A feature subset of size $k$
$\rho_{k}$ : All subsets of size
Explainer $\mathcal{E}: \mathbb{P}(S \mid x)$.
$X_{s}$ : The sub-vector of chosen features.


## Framework

Objective: Maximize the mutual information between selected features and theresponse variable, over the explainer $\mathcal{E}$

$$
\max I\left(X_{S} ; Y\right) \text { subject to } \quad S \sim \mathcal{E}(X) \text {. }
$$

An information-theoretic interpretation: Define

$$
\mathcal{E}^{*}(x):=\arg \min _{S} \underbrace{\mathbb{E}_{m}\left[\left.\log \frac{1}{\mathbb{P}_{m}\left(Y \mid x_{S}\right)} \right\rvert\, x\right]}_{\begin{array}{c}
\text { Expected length of encoded message. } \\
\text { for the target model using } \mathbb{P}_{m}(Y \mid Y s)
\end{array}} .
$$

Then $\mathcal{E}^{*}$ is a global optimum of Problem (1). Conversely, any global optimum of Problem (1) degenerates to $\mathcal{E}^{*}$ almost surely over $\mathbb{P}_{x}$. Intractability of the objective.

$$
\begin{aligned}
I\left(X_{S} ; Y\right) & =\mathbb{E}\left[\log \frac{\mathbb{P}_{m}\left(X_{S}, Y\right)}{\mathbb{P}\left(X_{S}\right) \mathbb{P}_{m}(Y)}\right]=\mathbb{E}\left[\log \frac{\mathbb{P}_{m}\left(Y \mid X_{S}\right)}{\mathbb{P}_{m}(Y)}\right] \\
& =\mathbb{E}\left[\log \mathbb{P}_{m}\left(Y \mid X_{S}\right)\right]+\text { Const. } \\
& =\mathbb{E}_{X} \underbrace{}_{\text {Intractable to compute directly. }} \mathbb{E}_{Y \mid X_{S}}\left[\log \mathbb{P}_{m}\left(Y \mid X_{S}\right)\right]
\end{aligned}+\text { Const. }
$$

## Approximations

A variational formulation: Introduce a variational family for approximation:

$$
\mathcal{Q}:=\left\{\mathbb{Q} \mid \mathbb{Q}=\left\{x_{S} \rightarrow \mathbb{Q}_{s}\left(Y \mid x_{S}\right), S \in \wp_{k}\right\}\right\} .
$$

An application of Jensen's inequality yields the lower bound

$$
\begin{aligned}
\mathbb{E}_{Y \mid X_{s}}\left[\log \mathbb{P}_{m}\left(Y \mid X_{S}\right)\right] & \geq \int_{\mathbb{P}_{m}\left(Y \mid X_{S}\right) \log \mathbb{Q}_{s}\left(Y \mid X_{S}\right)} \\
& =\mathbb{E}_{Y \mid X_{S}}\left[\log \mathbb{Q}_{s}\left(Y \mid X_{S}\right)\right]
\end{aligned}
$$

where equality holds iff $\mathbb{P}_{m}\left(Y \mid X_{S}\right) \stackrel{d}{=} \mathbb{Q}_{s}\left(Y \mid X_{S}\right)$.
A single neural network $g_{\alpha}$ for parametrizing $\mathbb{Q}$ :
Define $\mathbb{Q}_{s}\left(Y \mid x_{S}\right):=g_{\alpha}\left(\widetilde{x}_{S}, Y\right)$, where $\widetilde{x}_{S} \in \mathbb{R}^{d}$ is defined by

$$
\left(\widetilde{x}_{S}\right)_{i}=\mathbf{1}\{i \in S\} \cdot x_{i} .
$$

Continuous relaxation of subset sampling:
Gumbel $(0,1): G_{i}=-\log \left(-\log u_{i}\right), u_{i} \sim \operatorname{Uniform}(0,1)$
Concrete $\left(\log p_{1}, \ldots, \log p_{d}\right):$ A random vector $C \in \mathbb{R}^{d}$, with

$$
C_{i}=\frac{\exp \left\{\left(\log p_{i}+G_{i}\right) / \tau\right\}}{\sum_{j=1}^{d} \exp \left\{\left(\log p_{j}+G_{j}\right) / \tau\right\}} .
$$

Approximate $k$ out of $d$ subset sampling:

$$
C^{j} \sim \operatorname{Concrete}\left(w_{\theta}(X)\right) \text { i.i.d. for } j=1,2, \ldots, k,
$$

$$
V(\theta, \zeta)=\left(V_{1}, V_{2}, \ldots, V_{d}\right), \quad V_{i}=\max C_{i}^{i}
$$

$$
\widetilde{X}_{S} \approx V(\theta, \zeta) \odot X
$$

( $\tau$ : temperature, $\theta$ : parameters of explainer, $\zeta:$ auxiliary random variables, $\odot$ : elementwise product)

## Final Objective

Objective: Containing parameters of both explainer and variational dist. $\theta, \alpha$ $\max _{\theta, \alpha} \mathbb{E}_{X, Y, \zeta}\left[\log g_{\alpha}(V(\theta, \zeta) \odot X, Y)\right]$
Optimization: Stochastic gradient methods such as Adam and RMSProp.

## Synthetic Experiments

Four data sets: Orange skin, XOR, Nonlinear additive model, Switch. Comparing methods: Saliency Map, DeepLIFT, KerneISHAP, LIME Evaluation: Median rank of the influential features, time complexity.


## Real-world Experiments

Data sets and models: IMDB movie review with word-based CNN and Hierarchical LSTM respectively, MNIST with CNN Evaluation: Post-hoc accuracy, human accuracy

$$
\begin{aligned}
& \text { Post-hoc accuracy (PA) IMDB-Word IMDB-Sent MNIST } \\
& \begin{array}{llll}
\text { Human accuracy (HA) } & 0.90 .84 & 0.849 & 0.774 \\
0.958 \\
\hline
\end{array} \\
& \text { HA on words: } 84.4 \%>\text { HA on original: } 83.7 \%
\end{aligned}
$$

## Visualization:



