Deep Machines that know when they do not know

Kristian Kersting

Getting deep systems that reason and know when they don’t know

Responsible AI systems that explain their decisions and co-evolve with the humans

Open AI systems that are easy to realize and understandable for the domain experts
AI and ML have a strong impact

Data are now ubiquitous; there is great value from understanding this data, building models and making predictions.

However, there are not enough data scientists, statisticians, machine learning and AI experts.

Provide the foundations, algorithms, and tools to develop systems that ease or even automate AI model discovery from data as much as possible.
Deep Neural Networks

Potentially much more powerful than shallow architectures, represent computations


Differentiable Programming
Deep Neural Networks

Potentially much more powerful than shallow architectures, represent computations


They “develop intuition” about complicated biological processes and generate scientific data

[Schramowski, Brugger, Mahlein, Kersting 2019]
Deep Neural Networks

Potentially much more powerful than shallow architectures, represent computations


They “invent” constrained optimizers

[Schramowski, Bauckhage, Kersting arXiv:1803.04300, 2018]
Deep Neural Networks

Potentially much more powerful than shallow architectures, represent computations


Semantics derived automatically from language corpora contain human-like biases

They “capture” stereotypes from human language
Deep Neural Networks

Potentially much more powerful than shallow architectures, represent computations


The Moral Choice Machine

<table>
<thead>
<tr>
<th>Dos</th>
<th>WEAT</th>
<th>Bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>smile</td>
<td>0.116</td>
<td>0.348</td>
</tr>
<tr>
<td>sightsee</td>
<td>0.090</td>
<td>0.281</td>
</tr>
<tr>
<td>cheer</td>
<td>0.094</td>
<td>0.277</td>
</tr>
<tr>
<td>celebrate</td>
<td>0.114</td>
<td>0.264</td>
</tr>
<tr>
<td>picnic</td>
<td>0.093</td>
<td>0.260</td>
</tr>
<tr>
<td>snuggle</td>
<td>0.108</td>
<td>0.238</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Don’ts</th>
<th>WEAT</th>
<th>Bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>rot</td>
<td>-0.099</td>
<td>-1.118</td>
</tr>
<tr>
<td>negative</td>
<td>-0.101</td>
<td>-0.763</td>
</tr>
<tr>
<td>harm</td>
<td>-0.110</td>
<td>-0.730</td>
</tr>
<tr>
<td>damage</td>
<td>-0.105</td>
<td>-0.664</td>
</tr>
<tr>
<td>slander</td>
<td>-0.108</td>
<td>-0.600</td>
</tr>
<tr>
<td>slur</td>
<td>-0.109</td>
<td>-0.569</td>
</tr>
</tbody>
</table>

But lucky they also “capture” our moral choices

[Jentzsch, Schramowski, Rothkopf, Kersting AIES 2019]
The Moral Choice Machine

<table>
<thead>
<tr>
<th>Dos</th>
<th>WEAT</th>
<th>Bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>smile</td>
<td>0.116</td>
<td>0.348</td>
</tr>
<tr>
<td>sightsee</td>
<td>0.090</td>
<td>0.281</td>
</tr>
<tr>
<td>cheer</td>
<td>0.094</td>
<td>0.277</td>
</tr>
<tr>
<td>celebrate</td>
<td>0.114</td>
<td>0.264</td>
</tr>
<tr>
<td>picnic</td>
<td>0.093</td>
<td>0.260</td>
</tr>
<tr>
<td>snuggle</td>
<td>0.108</td>
<td>0.238</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Don’t</th>
<th>WEAT</th>
<th>Bias</th>
</tr>
</thead>
<tbody>
<tr>
<td>rot</td>
<td>-0.099</td>
<td>-1.118</td>
</tr>
<tr>
<td>negative</td>
<td>-0.101</td>
<td>-0.763</td>
</tr>
<tr>
<td>harm</td>
<td>-0.110</td>
<td>-0.730</td>
</tr>
<tr>
<td>damage</td>
<td>-0.105</td>
<td>-0.664</td>
</tr>
<tr>
<td>slander</td>
<td>-0.108</td>
<td>-0.600</td>
</tr>
<tr>
<td>slur</td>
<td>-0.109</td>
<td>-0.569</td>
</tr>
</tbody>
</table>

But lucky they also “capture” our moral choices

[Jentzsch, Schramowski, Rothkopf, Kersting AIES 2019]
Can we trust deep neural networks?

Unmasking Clever Hans predictors and assessing what machines really learn

Sebastian Lapuschkin, Stephan Wäldchen, Alexander Binder, Grégoire Montavon, Wojciech Samek & Klaus-Robert Müller

*Nature Communications* 10, Article number: 1096 (2019)
DNNs do not quantify all of the uncertainty. They are not calibrated joint distributions. \( P(Y|X) \neq P(Y,X) \)

Train & Evaluate

MNIST

SVHN

SEMEION

Transfer Testing


[Peharz, Vergari, Molina, Stelzner, Trapp, Kersting, Ghahramani UDL@UAI 2018]
Getting deep systems that know when they don’t know.
Can we borrow ideas from deep learning for probabilistic graphical models?

Judea Pearl, UCLA
Turing Award 2012
This results in Sum-Product Networks, a deep probabilistic learning framework.

Computational graph (kind of TensorFlow graphs) that encodes how to compute probabilities.

Inference is linear in size of network.
This results in Sum-Product Networks, a deep probabilistic learning framework.

Computational graph (kind of TensorFlow graphs) that encodes how to compute probabilities.

Inference is linear in size of network.
And there is a way to select models

Testing independence of random variables using e.g. (nonparametric) tests

Conditioning, e.g., via clustering

Examples

Random Variables

keep growing alternatingly * and + layers
SPFlow: An Easy and Extensible Library for Sum-Product Networks

Domain Specific Language, Inference, EM, and Model Selection as well as Compilation of SPNs into TF and PyTorch and also into flat, library-free code even suitable for running on devices: C/C++, GPU, FPGA

SPFlow, an open-source Python library providing a simple interface to inference, learning and manipulation routines for deep and tractable probabilistic models called Sum-Product Networks (SPNs). The library allows one to quickly create SPNs both from data and through a domain specific language (DSL). It efficiently implements several probabilistic inference routines like computing marginals, conditional and (approximate) most probable explanations (MPEs) along with sampling.

https://github.com/SPFlow/SPFlow
Random sum-product networks

[Peharz, Vergari, Molina, Stelzner, Trapp, Kersting, Ghahramani UDL@UAI 2018]
How do we do data science offshore?
There are generic protocols to validate computations on authenticated data without knowledge of the secret key.

#### DNA MSPN ####
- Gates: 298208
- Yao Bytes: 9542656
- Depth: 615

#### DNA PSPN ####
- Gates: 228272
- Yao Bytes: 7304704
- Depth: 589

#### NIPS MSPN ####
- Gates: 1001477
- Yao Bytes: 32047264
- Depth: 970

---

Homomorphic sum-product network

[Molina, Weinert, Treiber, Schneider, Kersting 2019]
Learning the Structure of Autoregressive Deep Models such as PixelCNNs [van den Oord et al. NIPS 2016]

Learn Conditional SPN by testing conditional independence and using conditional clustering, using e.g. [Zhang et al. UAI 2011; Lee, Honovar UAI 2017; He et al. ICDM 2017; Zhang et al. AAAI 2018; Runge AISTATS 2018]

**Conditional SPNs**
[Shao, Molina, Vergari, Peharz, Kersting 2019]
Learn Conditional SPN by testing conditional independence and using conditional clustering, using e.g. [Zhang et al. UAI 2011; Lee, Honovar UAI 2017; He et al. ICDM 2017; Zhang et al. AAAI 2018; Runge AISTATS 2018]

**Conditional SPNs**
[Shao, Molina, Vergari, Peharz, Kersting 2019]
Learn Conditional SPN by testing conditional independence and using conditional clustering, using e.g. [Zhang et al. UAI 2011; Lee, Honovar UAI 2017; He et al. ICDM 2017; Zhang et al. AAAI 2018; Runge AISTATS 2018]

**Conditional SPNs**
[Shao, Molina, Vergari, Peharz, Kersting 2019]
Mind the data science loop

- Question
- Data collection and preparation
- Deployment
- Answer found?
- How to report results? What is interesting?
- Discuss results
- ML

Continuous? Discrete? Categorical? ...
Multinomial? Gaussian? Poisson? ...

Kristian Kersting - Sum-Product Probabilistic Programming: The Democratization of Machine Learning and Data Science
Distribution-agnostic Deep Probabilistic Learning

Use nonparametric independency tests and piece-wise linear approximations
However, we have to provide the statistical types and do not gain insights into the parametric forms of the variables. Are they Gaussians? Gammas? …
We can even automatically discovers the statistical types and parametric forms of the variables.
That is, the machine understands the data with few expert input ...

Exploring the Titanic dataset

This report describes the dataset Titanic and contains general statistical information and an analysis on the influence different features and subgroups of the data have on each other. The first part of the report contains general statistical information about the dataset and an analysis of the variables and probability distributions. The second part focuses on a subgroup analysis of the data. Different clusters identified by the network are analyzed and compared to give an insight into the structure of the data. Finally, the influence different variables have on the predictive capabilities of the model are analyzes. The whole report is generated by fitting a sum product network to the data and extracting all information from this model.


...and can compile data reports automatically
The machine understands the data with no expert input …

…and can compile data reports automatically

*[Baehrens, Schroeter, Harmeling, Kawanabe, Hansen, Müller JMLR 11:1803-1831, 2010]

Explanation vector*
(computable in linear time in the size of the SPN) showing the impact of "gender" on the chances of survival for the Titanic dataset
P(heart attack | )?
P(heart attack | )? 

The New York Times

Opinion

A.I. Is Harder Than You Think

By Gary Marcus and Ernest Davis
Mr. Marcus is a professor of psychology and neural science. Mr. Davis is a professor of computer science.

May 18, 2018
Crossover of ML and DS with data & programming abstractions


Building general-purpose data science and ML machines

Make the ML/DS expert more effective

Increases the number of people who can successfully build ML/DS applications
Understanding Electronic Health Records

Atherosclerosis is the cause of the majority of Acute Myocardial Infarctions (heart attacks)

Logical Variables (Abstraction)

Rule/Database view

Probability

<table>
<thead>
<tr>
<th>Algorithm for Mining Markov Logic Networks</th>
<th>Likelihood</th>
<th>AUC-ROC</th>
<th>AUC-PR</th>
<th>Time</th>
<th>state-of-the-art</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boosting</td>
<td>0.81</td>
<td>0.96</td>
<td>0.93</td>
<td>9s</td>
<td>37200x faster</td>
</tr>
<tr>
<td>LSM</td>
<td>0.73</td>
<td>0.54</td>
<td>0.62</td>
<td>93 hrs</td>
<td></td>
</tr>
</tbody>
</table>

[Kersting, Driessens ICML’08; Karwath, Kersting, Landwehr ICDM’08; Natarajan, Joshi, Tadepelli, Kersting, Shavlik. IJCAI’11; Natarajan, Kersting, Ip, Jacobs, Carr IAAI ’13; Yang, Kersting, Terry, Carr, Natarajan AIME ’15; Khot, Natarajan, Kersting, Shavlik ICDM’13, MLJ’12, MLJ’15, Yang, Kersting, Natarajan BIBM’17]
Human-in-the-loop learning
New field: Probabilistic Programming

Formulae parse trees + Algebraic Decision Diagrams + Matrix Free Optimization

Applies to QPs but here illustrated on MDPs for a factory agent which must paint two objects and connect them. The objects must be smoothed, shaped and polished and possibly drilled before painting, each of which actions require a number of tools which are possibly available. Various painting and connection methods are represented, each having an effect on the quality of the job, and each requiring tools. Rewards (required quality) range from 0 to 10 and a discounting factor of 0.9 was used.
In general, computing the exact posterior is intractable, i.e., inverting the generative process to determine the state of latent variables corresponding to an input is time-consuming and error-prone.

Deep Probabilistic Programming

(2) Ease the implementation by some high-level, probabilistic programming language

(1) Instead of optimizing variational parameters for every new data point, use a deep network to predict the posterior given $X$  [Kingma, Welling 2013, Rezende et al. 2014]
(1) Instead of optimizing variational parameters for every new data point, use a deep network to predict the posterior given $X$. [Kingma, Welling 2013, Rezende et al. 2014]

(2) Ease the implementation by some high-level, probabilistic programming language

```python
import pyro.distributions as dist
def model(data):
    # define the hyperparameters that control the beta prior
    alpha0 = torch.tensor(18.0)
    beta0 = torch.tensor(18.0)
    # sample f from the beta prior
    f = pyro.sample("latent_fairness", dist.Beta(alpha0, beta0))
    # loop over the observed data
    for i in range(len(data)):
        # observe datapoint $i$ using the bernoulli
        # likelihood Bernoulli$(f)$
        pyro.sample("obs_$(i)".format(i), dist.Bernoulli(f), obs=data[i])

def guide(data):
    # register the two variational parameters with Pyro.
    alpha_q = pyro.param("alpha_q", torch.tensor(18.0),
                         constraint=constraints.positive)
    beta_q = pyro.param("beta_q", torch.tensor(18.0),
                         constraint=constraints.positive)
    # sample latent_fairness from the distribution Beta(alpha_q, beta_q)
    pyro.sample("latent_fairness", dist.Beta(alpha_q, beta_q))
```

Sum-Product Network

Deep Neural Network
Unsupervised scene understanding

Consider e.g. unsupervised scene understanding using a generative model

[Attend-Infer-Repeat (AIR) model, Hinton et al. NIPS 2016]

Sum-Product Probabilistic Programming: Making machine learning and data science easier [Stelzner, Molina, Peharz, Vergari, Trapp, Valera, Ghahramani, Kersting ProgProb 2018]

Probabilistic Programming:
Easier modelling by programming generative models in a high-level, prob. language

Deep Probabilistic Prog.:
Modelling and inference might be hard, so use a deep neural network for it

Use deep probabilistic models that feature tractable, deterministic inference

```
from spn.structure.leaves.parametric.Parametric import Categorical
from spn.structure.Base import Sum, Product

assign_ids = spn.assign_ids, rebuild_scopes_bottom_up

p0 = Product(children=[Categorical(p=[0.3, 0.7], scope=0), Categorical(p=[0.4, 0.6], scope=1)])
p1 = Product(children=[Categorical(p=[0.5, 0.5], scope=0), Categorical(p=[0.6, 0.4], scope=1)])
p2 = Product(children=[Categorical(p=[0.2, 0.8], scope=0), Categorical(p=[0.3, 0.7], scope=1)])
p3 = Product(children=[Categorical(p=[0.4, 0.6], scope=0), Categorical(p=[0.3, 0.7], scope=1)])
sp = Sum([assign_ids(p0, p1, p2, p3)])
```
Actually, the main idea is to replace the VAEs within AIR by SPNs.

- VAE:
  - infinite mixture model
  - intractable density
  - intractable posterior

- SPN:
  - “large” but finite mixture model
  - tractable density
  - tractable marginals [Peharz et al., 2015]
  - tractable posterior [Vergari et al., 2017]
Sum-Product Attent-Infer Repeat (SuPAIR)

[Stelzner, Peharz, Kersting ICML 2019]
Sum-Product Attent-Infer Repeat (SuPAIR)

Multi-MNIST

[Stelzner, Peharz, Kersting ICML 2019]
Sum-Product Attent-Infer Repeat (SuPAIR)

[Stelzner, Peharz, Kersting ICML 2019]
There are strong investments into (deep) probabilistic programming.

RelationalAI, Apple, Microsoft and Uber are investing hundreds of millions of US dollars.
Since we need languages for Systems AI, the computational and mathematical modeling of complex AI systems.


Getting deep systems that reason and know when they don’t know

Responsible AI systems that explain their decisions and co-evolve with the humans

Open AI systems that are easy to realize and understandable for the domain experts

„Tell the AI when it is right for the wrong reasons and it adapts its behavior“
Explanation should be understandable by humans

The twin science: cognitive science
"How do we humans get so much from so little?" and by that I mean how do we acquire our understanding of the world given what is clearly by today's engineering standards so little data, so little time, and so little energy.

Josh Tenenbaum, MIT

Lake, Salakhutdinov, Tenenbaum, Science 350 (6266), 1332-1338, 2015
Tenenbaum, Kemp, Griffiths, Goodman, Science 331 (6022), 1279-1285, 2011
Overall, AI/ML/DS indeed refine “formal” science, but …

- **AI is more than deep neural networks.** Probabilistic and causal models are whiteboxes that provide insights into applications

- **AI is more than a single table.** Loops, graphs, different data types, relational DBs, … are central to data science and high-level programming languages for DS help to capture this complexity

- **AI is more than just Machine Learners and Statisticians**

Learning-based programming offers a framework for building systems that help to go beyond, democratize, and even automize traditional AI/ML/DS
Kristian Kersting - Sum Product Probabilistic Programming: The Democratization of Machine Learning and Data Science