



# Al can learn from data. But can it learn to reason?

Guy Van den Broeck

# Outline

- The paradox of learning to reason from data
   deep learning
- 2. Architectures for learning and reasoning

  \*\*logical reasoning + deep learning\*\*
  - a. Constrained language generation
  - b. Constrained structured prediction

## Outline

1. The paradox of learning to reason from data deep learning

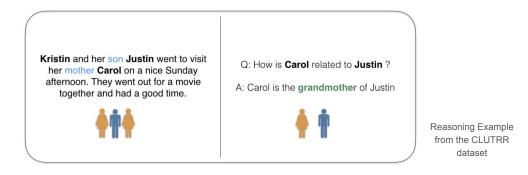
2. Architectures for learning and reasoning

\*\*logical reasoning + deep learning\*\*

- a. Constrained language generation
- b. Constrained structured prediction

### Can Language Models Perform Logical Reasoning?

Language Models achieve high performance on various "reasoning" benchmarks in NLP.



It is unclear whether they solve the tasks following the rules of logical deduction.

#### Language Models:

input  $\rightarrow$  ?  $\rightarrow$  Carol is the grandmother of Justin.

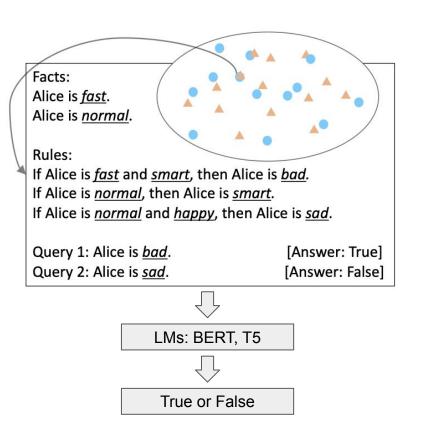
#### Logical Reasoning:

input  $\rightarrow$  Justin in Kristin's son; Carol is Kristin's mother;  $\rightarrow$  Carol is Justin's mother's mother; if X is Y's mother's mother X is Y's grandmother  $\rightarrow$  Carol is the grandmother of Justin.

### Problem Setting: SimpleLogic

The easiest of reasoning problems:

- 1. **Propositional logic** fragment
  - a. bounded vocabulary & number of rules
  - b. bounded reasoning depth (≤ 6)
  - c. finite space ( $\approx 10^{360}$ )
- 2. **No language variance**: templated language
- Self-contained
   No prior knowledge
- Purely symbolic predicates
   No shortcuts from word meaning
- Tractable logic (definite clauses)
   Can always be solved efficiently



#### SimpleLogic

#### Generate textual train and test examples of the form:

Rules: If witty, then diplomatic. If careless and condemned and attractive, then blushing. If dishonest and inquisitive and average, then shy. If average, then stormy. If popular, then blushing. If talented, then hurt. If popular and attractive, then thoughtless. If blushing and shy and stormy, then inquisitive. If adorable, then popular. If cooperative and wrong and stormy, then thoughtless. If popular, then sensible. If cooperative, then wrong. If shy and cooperative, then witty. If polite and shy and thoughtless, then talented. If polite, then condemned. If polite and wrong, then inquisitive. If dishonest and inquisitive, then talented. If blushing and dishonest, then careless. If inquisitive and dishonest, then troubled. If blushing and stormy, then shy. If diplomatic and talented, then careless. If wrong and beautiful, then popular. If ugly and shy and beautiful, then stormy. If shy and inquisitive and attractive, then diplomatic. If witty and beautiful and frightened, then adorable. If diplomatic and cooperative, then sensible. If thoughtless and inquisitive, then diplomatic. If careless and dishonest and troubled, then cooperative. If hurt and witty and troubled, then dishonest. If scared and diplomatic and troubled, then average. If ugly and wrong and careless, then average. If dishonest and scared, then polite. If talented, then dishonest. If condemned, then wrong. If wrong and troubled and blushing, then scared. If attractive and condemned, then frightened. If hurt and condemned and shy, then witty. If cooperative, then attractive. If careless, then polite. If adorable and wrong and careless, then diplomatic. Facts: Alice sensible Alice condemned Alice thoughtless Alice polite Alice scared Alice average

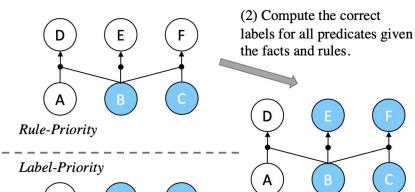
Query: Alice is shy?

### Training a transformer on SimpleLogic

(1) Randomly sample facts & rules.

Facts: B, C

Rules: A, B  $\rightarrow$  D. B  $\rightarrow$  E. B, C  $\rightarrow$  F.



(1) Randomly assign labels to predicates.

True: B, C, E, F. False: A, D.

(2) Set B, C (randomly chosen among B, C, E, F) as facts and sample rules (randomly) consistent with the label assignments.

#### Test accuracy for different reasoning depths

Test	0	1	2	3	4	5	6
RP	99.9	99.8	99.7	99.3	98.3	97.5	95.5

Test	0	1	2	3	4	5	6
LP	100.0	100.0	99.9	99.9	99.7	99.7	99.0

#### Has the transformer learned to reason from data?

- 1. Easiest of reasoning problems (no variance, self-contained, purely symbolic, tractable)
- 2. RP/LP data covers the whole problem space
- 3. The learned model has almost 100% test accuracy
- 4. There exist transformer parameters that compute the ground-truth reasoning function:

<u>Theorem 1:</u> For a BERT model with n layers and 12 attention heads, by construction, there exists a set of parameters such that the model can correctly solve any reasoning problem in SimpleLogic that requires at most n – 2 steps of reasoning.

Surely, under these conditions, the transformer has learned the ground-truth reasoning function!



#### The Paradox of Learning to Reason from Data

Train	Test	0	1	2	3	4	5	6
RP	RP	99.9	99.8	99.7	99.3	98.3	97.5	95.5
	LP	99.8	99.8	99.3	96.0	90.4	75.0	57.3
LP	RP	97.3	66.9	53.0	54.2	59.5	65.6	69.2
	LP	100.0	100.0	99.9	99.9	99.7	99.7	99.0

The BERT model trained on one distribution fails to generalize to the other distribution within the same problem space.



- If the transformer has learned to reason, it should not exhibit such generalization failure.
- 2. If the transformer **has not learned** to reason, it is baffling how it achieves near-perfect in-distribution test accuracy.

### Why? Statistical Features

Monotonicity of entailment:

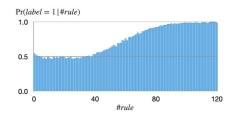
Any rules can be freely added to the axioms of any proven fact.

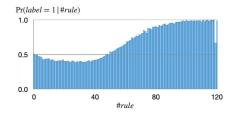


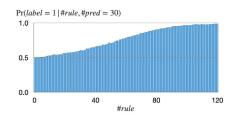
The more rules given, the more likely a predicate will be proven.



 $Pr(label = True \mid Rule \# = x)$  should increase (roughly) monotonically with x







(a) Statistics for examples generated by Rule-Priority (RP).

(b) Statistics for examples generated by Label-Priority (LP).

(c) Statistics for examples generated by uniform sampling;

### Model leverages statistical features to make predictions

RP\_b downsamples from RP such that  $Pr(label = True \mid rule\# = x) = 0.5$  for all x

Train	Test	0	1	2	3	4	5	6
	RP	99.9	99.8	99.7	99.3	98.3	97.5	95.5
RP	RP RP_b	99.0	99.3	98.5	97.5	96.7	93.5	88.3

- Accuracy drop from RP to RP\_b indicates that the model is using rule# as a statistical feature to make predictions.
- 2. Potentially countless statistical features
- Such features are inherent to the reasoning problem, cannot make data "clean"

#### First Conclusion

Experiments unveil the fundamental difference between

- 1. learning to reason, and
- 2. learning to achieve high performance on benchmarks using statistical features.

Be careful deploying AI in applications where this difference matters.

FAQ: Do bigger transformers solve this problem? No, already 99% accurate...

FAQ: Will reasoning emerge? Perhaps on 99% of human behavior...

# Outline

 The paradox of learning to reason from data <del>deep learning</del>

### 2. Architectures for learning and reasoning

logical reasoning + deep learning

- a. Constrained language generation
- b. Constrained structured prediction

# Outline

The paradox of learning to reason from data
 deep learning

2. Architectures for learning and reasoning

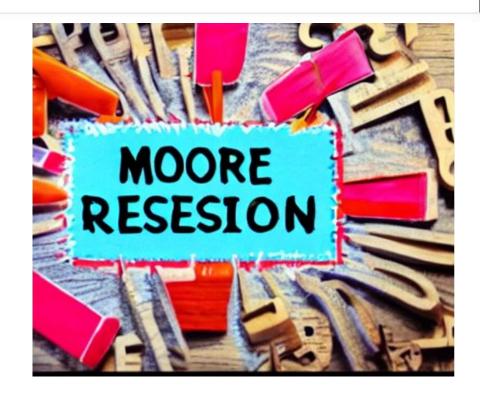
logical reasoning + deep learning

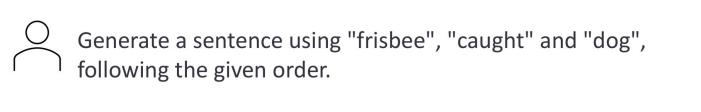
- a. Constrained language generation
- b. Constrained structured prediction

# Generative models are still hard to control

more reasoning!

Generate image







Generate a sentence using "frisbee", "caught" and "dog", following the given order.



After a perfect throw, the <u>frisbee</u> glided through the air, and the <u>dog</u>, with incredible agility, <u>caught</u> it mid-flight.

ChatGPT



Generate a sentence using "frisbee", "caught" and "dog", following the given order.



After a perfect throw, the <u>frisbee</u> glided through the air, and the <u>dog</u>, with incredible agility, <u>caught</u> it mid-flight.

ChatGPT



That's not correct. Generate a sentence using "frisbee", "caught" and "dog". The keywords should appear in the order as specified.



Here's the correct sentence: The <u>dog caught</u> the <u>frisbee</u> in mid-air, showing off its amazing catching skills.

ChatGPT



Generate a sentence using "frisbee", "caught" and "dog", following the given order.



After a perfect throw, the <u>frisbee</u> glided through the air, and the <u>dog</u>, with incredible agility, <u>caught</u> it mid-flight.



That's not correct. Generate a sentence using "frisbee", "caught" and "dog". The keywords should appear in the order as specified.



Here's the correct sentence: The <u>dog caught</u> the <u>frisbee</u> in mid-air, showing off its amazing catching skills.

ChatGPT



A <u>frisbee</u> is <u>caught</u> by a <u>dog</u>.

A pair of <u>frisbee</u> players are <u>caught</u> in a <u>dog</u> fight.

GeLaTo

### What do we have?

Prefix: "The weather is"

Constraint a: text contains "winter"

Model only does  $p(\text{next-token}|\text{prefix}) = \frac{\text{cold}}{\text{warm}} \frac{\text{0.05}}{\text{0.10}}$ 

Train some  $q(.|\alpha)$  for a specific task distribution  $\alpha \sim p_{\rm task}$  (amortized inference, encoder, masked model, seq2seq, prompt tuning,...)

Train  $q(\text{next-token}|\text{prefix}, \alpha)$ 

### What do we need?

Prefix: "The weather is"

Constraint a: text contains "winter"

Generate from 
$$p(\text{next-token}|\text{prefix}, \alpha) = \frac{\text{cold}}{\text{warm}} \frac{\text{0.50}}{\text{0.01}}$$

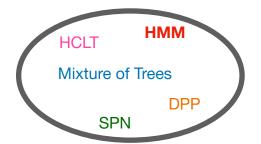
$$\propto \sum_{\text{text}} p(\text{next-token, text, prefix}, \alpha)$$

# Marginalization!

#### Tractable Probabilistic Models

Tractable Probabilistic Models (TPMs) model joint probability distributions (just like auto-regressive LMs) and allow efficient computation of various probabilistic queries.

Probabilistic (Generating) Circuits

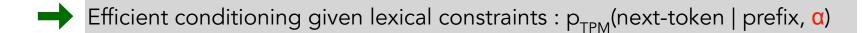


e.g., efficient marginalization:

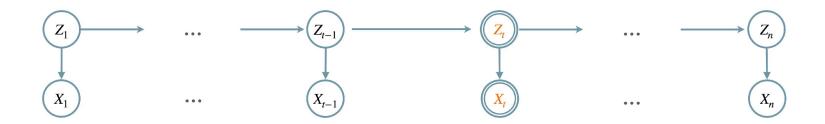
$$p_{TPM}$$
(3rd token = frisbee, 5th token = dog)

in particular ...

$$\sum_{\text{sentence}} p_{\text{TPM}}$$
(sentence, next-token = "warm", prefix = "The weather is",  $\alpha$ )



# Step 1: Distill an HMM $p_{hmm}$ that approximates $p_{gpt}$



- 1. An HMM with 4096 hidden states and 50k emission tokens
- 2. Train the HMM on data sampled from GPT2-large (domain-adapted, either via prompting or fine-tuning), effectively minimizing KL( $p_{qpt}//p_{HMM}$ )
- 3. Leverages the <u>latent variable distillation</u> technique for training probabilistic circuits at scale [ICLR 23]. (Cluster embeddings of examples to estimate latent Z<sub>i</sub>)

# Computing $p_{hmm}(\alpha \mid x_{1:t+1})$

For  $\alpha$  in conjunctive normal form (CNF):

$$(w_{1,1} \lor ... \lor w_{1,d1}) \land ... \land (w_{m,1} \lor ... \lor w_{m,dm})$$

where each  $w_{ij}$  is a keyword (i.e. a string of tokens), representing the constraint that  $w_{ij}$  appears in the generated text.

e.g., 
$$\alpha$$
 = ("swims"  $\vee$  "like swimming")  $\wedge$  ("lake"  $\vee$  "pool")

#### Efficient algorithm:

For m clauses and sequence length n, time-complexity for generation is  $O(2^{|m|}n)$ .

<u>Trick</u>: dynamic programming with clever preprocessing and local belief updates

## CommonGen: a Challenging Benchmark

Given 3-5 concepts (keywords), our goal is to generate a sentence using all keywords, which can appear in any order and any form of inflections. e.g.,

Input: snow drive car

Reference 1: A car drives down a snow covered road.

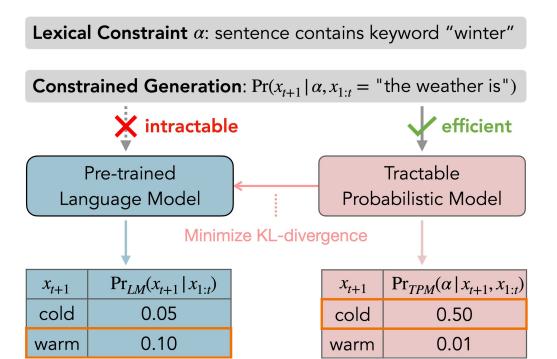
Reference 2: Two cars drove through the snow.

$$(w_{1,1} \lor ... \lor w_{1,d1}) \land ... \land (w_{m,1} \lor ... \lor w_{m,dm})$$

Each clause represents the inflections for one keyword.

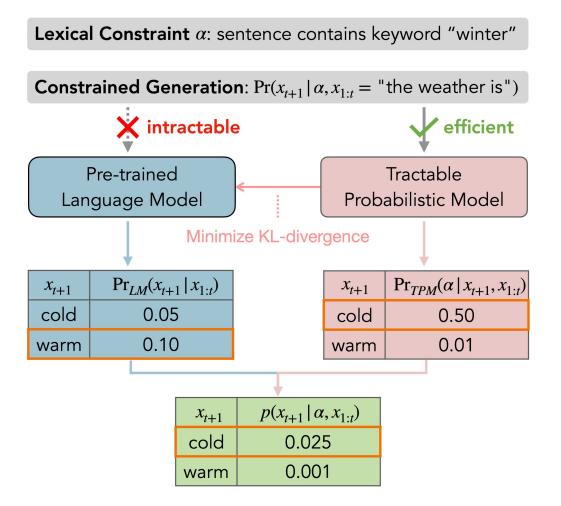
### GeLaTo Overview





### GeLaTo Overview





# Step 2: Control $p_{gpt}$ via $p_{hmm}$

#### <u>Unsupervised</u>

Language model is not fine-tuned/prompted to satisfy constraints

By Bayes rule:

$$p_{gpt}(x_{t+1} | x_{1:t}, \alpha) \propto p_{gpt}(\alpha | x_{1:t+1}) \cdot p_{gpt}(x_{t+1} | x_{1:t})$$

Assume  $p_{hmm}(\alpha \,|\, x_{1:t+1}) \approx p_{gpt}(\alpha \,|\, x_{1:t+1})$ , we generate from:

$$p(x_{t+1} | x_{1:t}, \alpha) \propto p_{hmm}(\alpha | x_{1:t+1}) \cdot p_{gpt}(x_{t+1} | x_{1:t})$$

Method	Generation Quality							Constraint Satisfaction				
Wellou	ROUGE-L		BLEU-4		CIDEr		SPICE		Coverage		Success Rate	
Unsupervised	dev	test	dev	test	dev	test	dev	test	dev	test	dev	test
InsNet (Lu et al., 2022a)	-	-	18.7	-	-	-	-	-	100.0	-	100.0	-
NeuroLogic (Lu et al., 2021)	-	41.9	-	24.7	-	14.4	-	27.5	-	96.7	-	-
A*esque (Lu et al., 2022b)	-	44.3	-	28.6	-	15.6	-	29.6	-	97.1	-	-
NADO (Meng et al., 2022)	-	-	26.2	-	-	-	=	-	96.1		_	-
GeLaTo	44.6	44.1	29.9	29.4	16.0	15.8	31.3	31.0	100.0	100.0	100.0	100.0

# Step 2: Control $p_{gpt}$ via $p_{hmm}$

#### **Supervised**

Language model is fine-tuned to perform constrained generation (e.g. seq2seq)

Empirically  $p_{HMM}(\alpha \mid x_{1:t+1}) \approx p_{gpt}(\alpha \mid x_{1:t+1})$  does not hold well enough;

we view  $p_{HMM}(x_{t+1} | x_{1:t}, \alpha)$  and  $p_{gpt}(x_{t+1} | x_{1:t})$  as classifiers trained for the same task with different biases; thus we generate from their <u>weighted</u> <u>geometric mean</u>:

$$p(x_{t+1} | x_{1:t}, \alpha) \propto p_{hmm}(x_{t+1} | x_{1:t}, \alpha)^w \cdot p_{gpt}(x_{t+1} | x_{1:t})^{1-w}$$

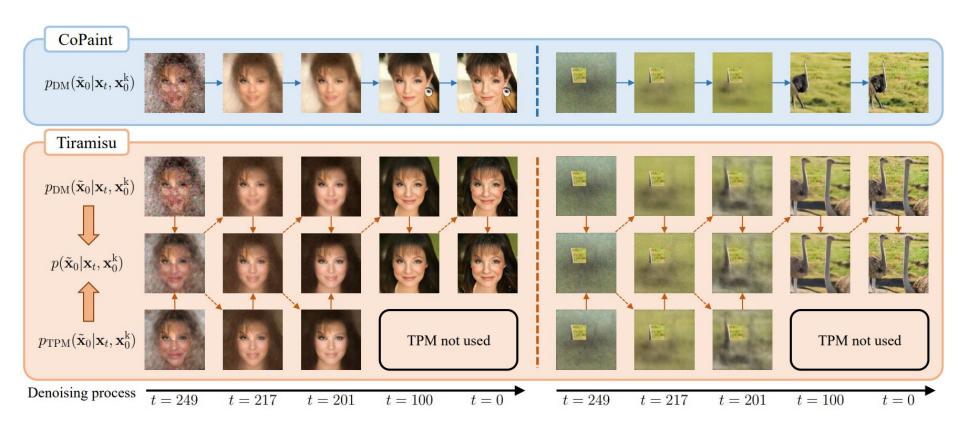
Method	Generation Quality								Constraint Satisfaction			
Method	<b>ROUGE-L</b>		BLEU-4		<b>CIDEr</b>		SPICE		Coverage		Success Rate	
Supervised	dev	test	dev	test	dev	test	dev	test	dev	test	dev	test
NeuroLogic (Lu et al., 2021)	-	42.8	_	26.7	T-	14.7	_	30.5	_	97.7	_	$93.9^{\dagger}$
A*esque (Lu et al., 2022b)	-	43.6	-	28.2	1	15.2	-	30.8	_	97.8	-	$97.9^{\dagger}$
NADO (Meng et al., 2022)	44.4 <sup>†</sup>	-	30.8	-	16.1 <sup>†</sup>	-	32.0 <sup>†</sup>	-	97.1	-	$88.8^{\dagger}$	-
GeLaTo	46.0	45.6	34.1	32.9	16.7	16.8	31.3	31.9	100.0	100.0	100.0	100.0

### Advantages of our framework:

- 1. Constraint  $\alpha$  is <u>guaranteed to be satisfied</u>: for any next-token  $x_{t+1}$  that would make  $\alpha$  unsatisfiable,  $p(x_{t+1} \mid x_{1:t}, \alpha) = 0$  for both settings.
- 2. Training  $p_{hmm}$  does not depend on  $\alpha$ , which is only imposed at inference (generation) time. Once  $p_{hmm}$  is trained, we can impose whatever  $\alpha$ .
- 3. We can impose <u>additional tractable constraints</u>:
  - The keywords are generated following a particular order.
  - (Some) keywords must appear at a particular position.
  - (Some) keywords must not appear in the generated sentence.

Conclusion: you can control an intractable generative model using a tractable generative model for (symbolic) reasoning.

# Controlling the denoiser with a probabilistic circuit



## High-resolution image benchmarks

Tasks			Algorithms									
Dataset	Mask	Tiramisu (ours)	CoPaint	RePaint	DDNM	DDRM	DPS	Resampling				
	Left	0.189	0.185	0.195	0.254	0.275	0.201	0.257				
	Top	0.187	0.182	0.187	0.248	0.267	0.187	0.251				
CelebA-HQ	Expand1	0.454	0.468	0.504	0.597	0.682	0.466	0.613				
CCICUA-IIQ	Expand2	0.442	0.455	0.480	0.585	0.686	0.434	0.601				
	V-strip	0.487	0.502	0.517	0.625	0.724	0.535	0.647				
	H-strip	0.484	0.488	0.517	0.626	0.731	0.492	0.639				
	Left	0.286	0.289	0.296	0.410	0.369	0.327	0.369				
	Top	0.308	0.312	0.336	0.427	0.373	0.343	0.368				
ImageNet	Expand1	0.616	0.623	0.691	0.786	0.726	0.621	0.711				
imagervei	Expand2	0.597	0.607	0.692	0.799	0.724	0.618	0.721				
	V-strip	0.646	0.654	0.741	0.851	0.761	0.637	0.759				
	H-strip	0.657	0.660	0.744	0.851	0.753	0.647	0.774				
	Left	0.285	0.287	0.314	0.345	0.366	0.314	0.367				
	Top	0.310	0.323	0.347	0.376	0.368	0.355	0.372				
I CUN Dadaaaa	Expand1	0.615	0.637	0.676	0.716	0.695	0.641	0.699				
LSUN-Bedroom	Expand2	0.635	0.641	0.666	0.720	0.691	0.638	0.690				
	V-strip	0.672	0.676	0.711	0.760	0.721	0.674	0.725				
	H-strip	0.679	0.686	0.722	0.766	0.726	0.674	0.724				
Average		0.474	0.481	0.518	0.596	0.591	0.489	0.571				

## Outline

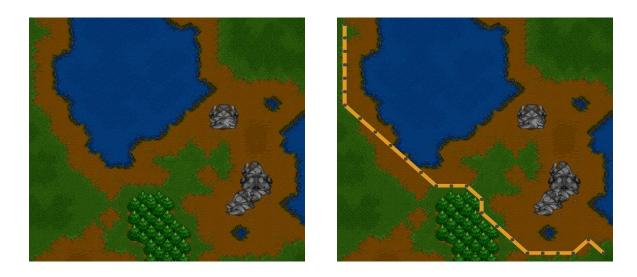
The paradox of learning to reason from data
 deep learning

2. Architectures for learning and reasoning

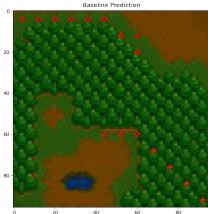
logical reasoning + deep learning

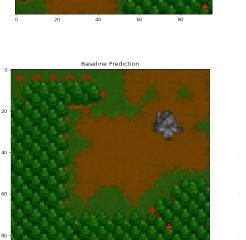
- a. Constrained language generation
- b. Constrained structured prediction

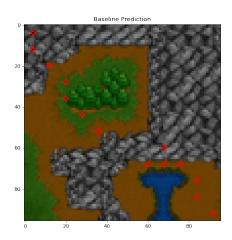
# Warcraft Shortest Path

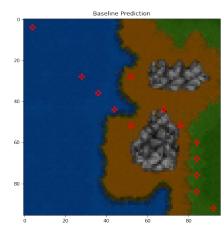


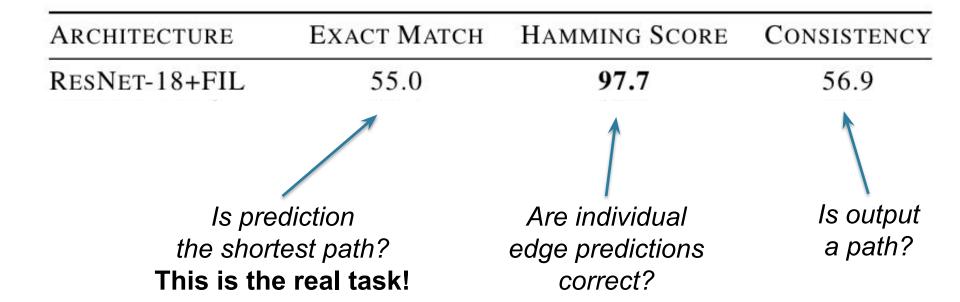
// for a  $12 \times 12$  grid,  $2^{144}$  states but only  $10^{10}$  valid ones!



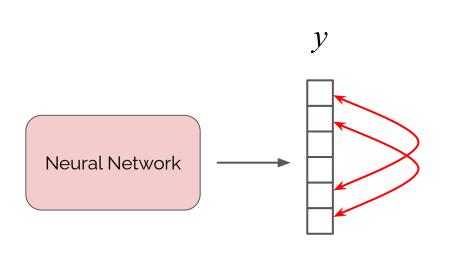




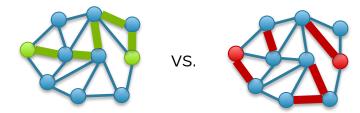




#### Declarative Knowledge of the Output



How is the output structured? Are all possible outputs valid?



How are the outputs related to each other?

Learning this from data is inefficient Much easier to express this declaratively

#### pylon

```
PyTorch Code

for i in range(train_iters):
    ...
    py = model(x)
    ...
    loss = CrossEntropy(py,...)
```

1) Specify knowledge as a predicate

```
def check(y):
    ...
    return isValid
```

## pylon

```
PyTorch Code

for i in range(train_iters):
    ...
    py = model(x)
    ...
    loss = CrossEntropy(py,...)
    loss += constraint_loss(check)(py)
```

1) Specify knowledge as a predicate

```
def check(y):
    ...
    return isValid
```

2 Add as loss to training

```
loss += constraint_loss(check)
```

### pylon

```
PyTorch Code

for i in range(train_iters):
    ...
    py = model(x)
    ...
    loss = CrossEntropy(py,...)

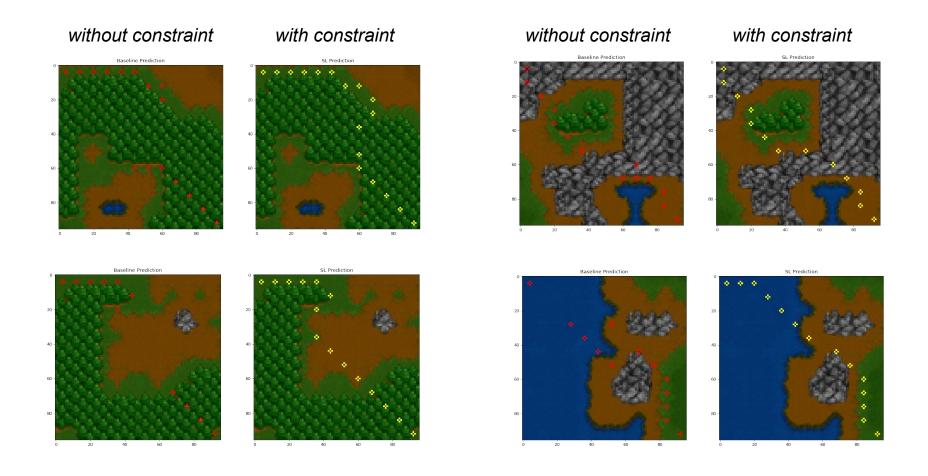
    loss += constraint_loss(check)(py)
```

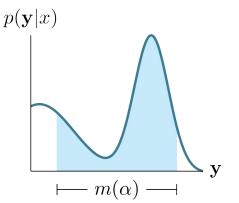
1) Specify knowledge as a predicate

2 Add as loss to training

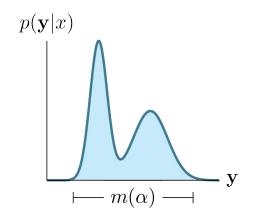
```
loss += constraint_loss(check)
```

3 pylon derives the gradients (solves a combinatorial problem)





a) A network uncertain over both valid& invalid predictions



c) A network allocating most of its mass to models of constraint

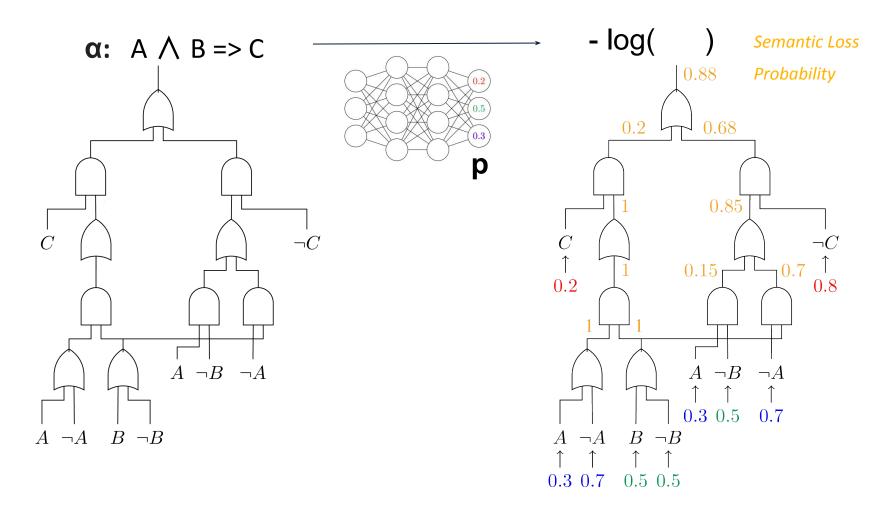


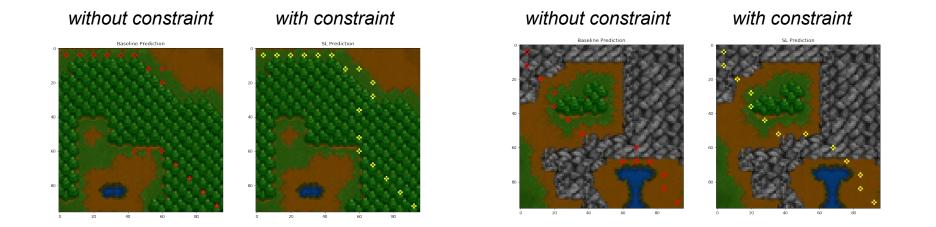
Semantic Loss

Probability of satisfying constraint α after sampling from neural net output layer **p** 

In general: #P-hard 😕

Do this probabilistic-logical reasoning during learning in a computation graph

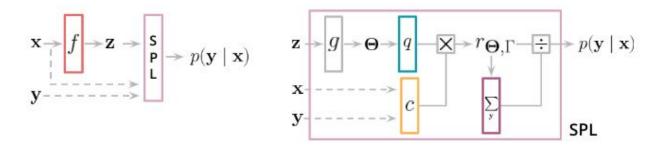




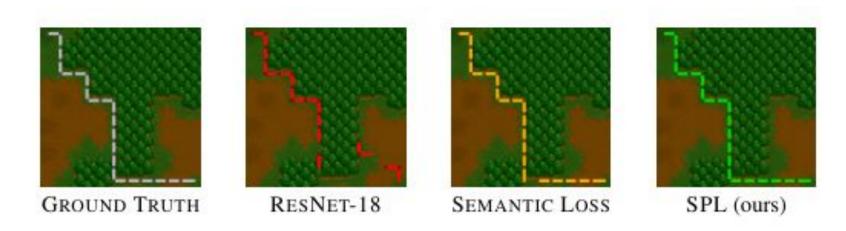
ARCHITECTURE	Ехаст Матсн	HAMMING SCORE	Consistency
RESNET-18+FIL	55.0	97.7	56.9
RESNET-18+ $\mathcal{L}_{SL}$	59.4	97.7	61.2

## Semantic Probabilistic Layers

- How to give a 100% guarantee that Boolean constraints will be satisfied?
- Bake the constraint into the neural network as a special layer

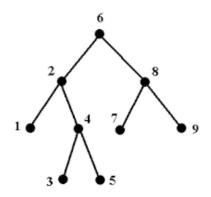


Secret sauce is again tractable circuits – computation graphs for reasoning



ARCHITECTURE	Ехаст Матсн	HAMMING SCORE	Consistency
RESNET-18+FIL	55.0	97.7	56.9
RESNET-18+ $\mathcal{L}_{SL}$	59.4	97.7	61.2
RESNET-18+SPL	75.1	97.6	100.0
OVERPARAM. SDD	78.2	96.3	100.0

#### Hierarchical Multi-Label Classification

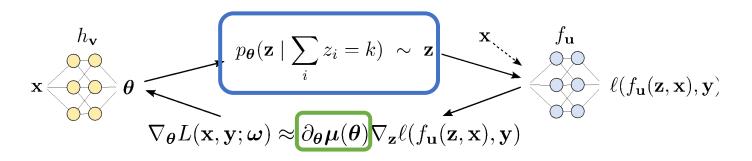


"if the image is classified as a dog, it must also be classified as an animal"

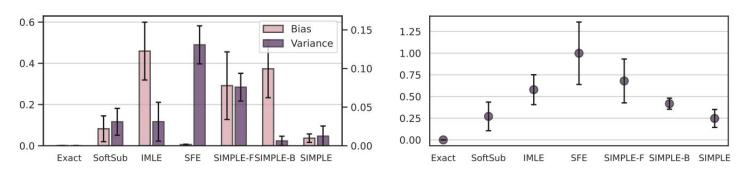
"if the image is classified as an animal, it must be classified as either cat or dog"

DATASET	EXACT MATCH			
	HMCNN	MLP+SPL		
CELLCYCLE	$3.05 \pm 0.11$	$\textbf{3.79} \pm \textbf{0.18}$		
DERISI	$1.39 \pm 0.47$	$\textbf{2.28} \pm \textbf{0.23}$		
EISEN	$5.40 \pm 0.15$	$\textbf{6.18} \pm \textbf{0.33}$		
EXPR	$4.20 \pm 0.21$	$\textbf{5.54} \pm \textbf{0.36}$		
GASCH1	$3.48 \pm 0.96$	$\textbf{4.65} \pm \textbf{0.30}$		
GASCH2	$3.11 \pm 0.08$	$\boldsymbol{3.95 \pm 0.28}$		
SEQ	$5.24 \pm 0.27$	$\textbf{7.98} \pm \textbf{0.28}$		
SPO	$\boldsymbol{1.97 \pm 0.06}$	$\boldsymbol{1.92 \pm 0.11}$		
DIATOMS	$48.21 \pm 0.57$	$58.71 \pm 0.68$		
ENRON	$5.97 \pm 0.56$	$\boldsymbol{8.18 \pm 0.68}$		
IMCLEF07A	$79.75 \pm 0.38$	$86.08 \pm 0.45$		
IMCLEF07D	$76.47 \pm 0.35$	$81.06 \pm 0.68$		

# **SIMPLE**: Gradient Estimator for *k*-Subset Sampling



We achieve *lower bias and variance* by exact, discrete samples and exact derivative of conditional marginals.



and SotA Learning to Explain (L2X) and sparse discrete VAE results.

## Secret Sauce: Probabilistic Circuits



#### **Tutorial (3h)**



https://youtu.be/2RAG5-L9R70

#### **Overview Paper (80p)**

Probabilistic Circuits: A Unifying Framework for Tractable Probabilistic Models*	
YooJung Choi	
Antonio Vergari	
Guy Van den Broeck  Computer Science Department  University of California  Los Angeles, CA, USA	
Contents	
1 Introduction	3
2 Probabilistic Inference: Models, Queries, and Tractability	4
2.2 Probabilistic Queries	5 6 8 9

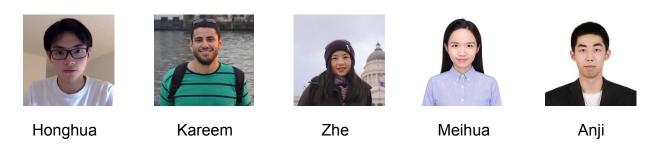
http://starai.cs.ucla.edu/papers/ProbCirc20.pdf

# Outline

- The paradox of learning to reason from data
   deep learning
- 2. Architectures for learning and reasoning logical (and probabilistic) reasoning + deep learning
  - a. Constrained language generation
  - b. Constrained structured prediction

# **Thanks**

# This was the work of many wonderful students/postdocs/collaborators!



References: <a href="http://starai.cs.ucla.edu/publications/">http://starai.cs.ucla.edu/publications/</a>