Sensitivity as a Complexity Measure for Sequence Classification Tasks

Michael Hahn

Stanford University

with Richard Futrell and Dan Jurafsky

March 31, 2021



The Stanford Natural Language Processing Group



What makes some NLP tasks harder and others easier?

What makes some NLP tasks harder and others easier?

Simple models based on lexical classifiers provide good performance on some tasks.

sentiment analysis POS tagging

. . .

What makes some NLP tasks harder and others easier?

Simple models based on lexical classifiers provide good performance on some tasks.

On other tasks, strong performance attained only recently with massive pretrained models. sentiment analysis POS tagging ...

Winograd sentences Entailment

. . .

What makes some NLP tasks harder and others easier?

Simple models based on lexical classifiers provide good performance on some tasks.

On other tasks, strong performance attained only recently with massive pretrained models. sentiment analysis POS tagging ...

Winograd sentences Entailment

. . .

This talk: Propose a theoretical framework to formalize and capture these differences.

Chomsky Hierarchy (Chomsky, 1956)

Chomsky Hierarchy (Chomsky, 1956)

prominent classification of formal languages by complexity



Chomsky Hierarchy (Chomsky, 1956)

prominent classification of formal languages by complexity

asymptotic worst-case complexity



Chomsky Hierarchy (Chomsky, 1956)

prominent classification of formal languages by complexity

asymptotic worst-case complexity



does not measure how hard it is to achieve high accuracy on realistic task distributions.

Kolmogorov complexity (Li and Vitányi, 1993)

Kolmogorov complexity (Li and Vitányi, 1993)

length of the shortest program producing an output

Kolmogorov complexity (Li and Vitányi, 1993)

length of the shortest program producing an output

uncomputable

Kolmogorov complexity (Li and Vitányi, 1993)

length of the shortest program producing an output

uncomputable

well-defined only in the asymptotic limit

Sensitivity as a Complexity Measure for Sequence Classification Tasks

Sensitivity for Sequence Classification

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks

Idea: Tasks are difficult when they have complex decision boundaries.

Simple Task Difficult Task

<u>Idea:</u> Tasks are difficult when they have complex decision boundaries.



Recent work highlights need to evaluate NLP models at their decision boundary (e.g., Levesque et al., 2011; Jia and Liang, 2017; Ribeiro et al., 2018; Gardner et al., 2019; Kaushik et al., 2019).

When is a decision boundary complex?



When is a decision boundary complex?

When the label often varies between neighbors!

Simple Task





Most neighbors have the same label as the point



Neighbors have the opposite label as the point

When is a decision boundary complex?

When the label often varies between neighbors!

Simple Task

Difficult Task



Can predict label even looking at part of the input.



Changing any part of the input can flip the label.

For a function $f : \{-1,+1\}^n \rightarrow \{-1,+1\}$:



For a function $f : \{-1,+1\}^n \rightarrow \{-1,+1\}$:



For a function $f : \{-1,+1\}^n \rightarrow \{-1,+1\}$:



For a function $f : \{-1,+1\}^n \rightarrow \{-1,+1\}$:



"How many Hamming neighbors of x have the opposite label?"


























When is a decision boundary complex?

When the label often varies between neighbors!

Simple Task

Difficult Task



Most neighbors have the same label as the point



Neighbors have the opposite label as the point

Desiderata:

Desiderata:

1. Alphabets with more than two elements

Desiderata:

1. Alphabets with more than two elements

$$s(f, x) := \sum_{i=1}^{n} \operatorname{Var} \left(f(X) | \forall j \neq i : X_j = x_j \right)$$

Inputs X' that agree with x in all but the i-th input

(O'Donnell, 2014, Def. 8.22)

Desiderata:

- 1. Alphabets with more than two elements
- 2. Nonuniform distribution

Desiderata:

- 1. Alphabets with more than two elements
- 2. Nonuniform distribution

Inputs typically respect grammatical structure of language

Desiderata:

- 1. Alphabets with more than two elements
- 2. Nonuniform distribution

Inputs typically respect grammatical structure of language

Task-specific input distributions

Desiderata:

- 1. Alphabets with more than two elements
- 2. Nonuniform distribution

Inputs typically respect grammatical structure of language

Task-specific input distributions

When measuring task difficulty, we want to focus on inputs that are plausible problem instances

Alphabet Σ (e.g. words, BPE, characters)

Alphabet Σ (e.g. words, BPE, characters) Distribution \prod over the set Σ^* of finite strings

an amazing movie

what a dumb movie

mostly boring

stunning visuals

this was hilarious

i can't believe i wasted my time on this dumb movie

truly incredible, great plot and good acting

```
Alphabet \Sigma (e.g. words, BPE, characters)
Distribution \prod over the set \Sigma^* of finite strings
Classification task = Function f : \Sigma^* \rightarrow [-1,1]
```

an amazing movie +1 what a dumb movie -1 mostly boring -1 stunning visuals +1 this was hilarious +1 i can't believe i wasted my -1 time on this dumb movie truly incredible, great +1

```
Alphabet \Sigma (e.g. words, BPE, characters)
Distribution \prod over the set \Sigma^* of finite strings
Classification task = Function f : \Sigma^* \rightarrow [-1,1]
```

an	amazing	movie	+1
----	---------	-------	----

what a dumb movie -1

mostly boring -1

stunning visuals +1

-1

this was hilarious +1

i can't believe i wasted my time on this dumb movie

truly incredible, great plot and good acting +1

Sensitivity:

In how many places can we change the input to change the output label while respecting ∏?

n $s(f,x) = \sum_{i=1}^{\infty} 1_{f(x) \neq f(x^{\oplus i})}$

 $s(f,x) = \sum_{i=1}^{n} \mathbb{1}_{f(x) \neq f(x^{\oplus i})}$

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}
ight)$$

Input string in Σ^*
KJHJKTGFJKJTGHHKJ

$$s(f, x, P) := \operatorname{Var} \left(f(X) | X \in x^{\oplus P} \right)$$

Input string in Σ^*
KJHJKTGFJKJTGHHKJ
Subset of {1, ..., |x|}
KJHJKTGFJKJTGHHKJ

 $s(f, x, P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$ Inputs that agree with Input string in Σ^* x outside of positions KJHJKTGFJKJTGHHKJ in P. Subset of {1, ..., |x|} **KJHJKTGFJKJTGHHKJ**

$$s(f, x, P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$$

Input string in Σ^*

KJHJKTGFJKJTGHHKJ

Subset of {1, ..., |x|} KJHJKTGFJKJTGHHKJ

- KJIFNTGFJKBASHHKJ -1
- KJQWFTGFJKKHYHHKJ +1
- KJNFATGFJKTBZHHKJ -1
- KJMZXTGFJKUASHHKJ -1

.

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, witty, seductive movie. A cute, witty, seductive movie. A sexy, witty, seductive movie. A shocking, witty, seductive movie. A stylish, witty, seductive movie. A charming, witty, seductive movie. A boring, witty, seductive movie. A bad, witty, seductive movie. A crocodile, witty, seductive movie. A oxymoron, witty, seductive movie.



$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, witty, seductive movie. A cute, witty, seductive movie. A sexy, witty, seductive movie. A shocking, witty, seductive movie. A stylish, witty, seductive movie. A charming, witty, seductive movie. A boring, witty, seductive movie. A bad, witty, seductive movie. A crocodile, witty, seductive movie. A oxymoron, witty, seductive movie.



All high-probability neighbors have positive sentiment

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, witty, seductive movie. A cute, witty, seductive movie. A sexy, witty, seductive movie. A shocking, witty, seductive movie. A stylish, witty, seductive movie. A charming, witty, seductive movie. A boring, witty, seductive movie. A bad, witty, seductive movie. A crocodile, witty, seductive movie. A oxymoron, witty, seductive movie.



All high-probability neighbors have positive sentiment

s(f,x,P) is low

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, witty, seductive movie. A cute, witty, seductive movie. A sexy, witty, seductive movie. A shocking, witty, seductive movie. A stylish, witty, seductive movie. A charming, witty, seductive movie. A boring, witty, seductive movie. A bad, witty, seductive movie. A crocodile, witty, seductive movie. A oxymoron, witty, seductive movie.



All high-probability neighbors have positive sentiment

s(f,x,P) is low

"We still know the label even if we don't know the blue word."

$$s(f, x, P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$$

$$s(f, x, P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$$

A brilliant, amazing, convincing movie. A boring, annoying, disappointing movie.

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, amazing, convincing movie. A boring, annoying, disappointing movie. Both sentiments represented among high-probability neighbors

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, amazing, convincing movie. A boring, annoying, disappointing movie. Both sentiments represented among high-probability neighbors

s(f,x,P) is high

$$s(f,x,P) := \operatorname{Var}\left(f(X)|X \in x^{\oplus P}\right)$$

A brilliant, amazing, convincing movie. A boring, annoying, disappointing movie. Both sentiments represented among high-probability neighbors

s(f,x,P) is high

"We don't know the label if we don't know the blue words."

$$bs(f, x) := \max_{\substack{k, P_1 \cup \dots \cup P_k \\ i=1}} \sum_{i=1}^k s(f, x, P_i)$$
Partitions of {1, ..., |x|}
into disjoint subsets

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

"In how many different places can we change the input to flip the label?"

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

"In how many different places can we change the input to flip the label?"

...while respecting input distribution \square .

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

"In how many different places can we change the input to flip the label?"

...while respecting input distribution \prod .

New probabilistic adaptation of previously-defined block sensitivity of Boolean functions (Nisan, 1991; Bernasconi, 1996; Hatami et al., 2010).

a gorgeous, witty, seductive movie.

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . s(f,x,P) = 0.93

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie .

s(f,x,P) = 0.93

block sensitivity: 0.93

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . High Sensitivity:

s(f,x,P) = 0.93

block sensitivity: 0.93

a painfully funny ode to bad behavior .
Low Sensitivity:

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . High Sensitivity:

s(f,x,P) = 0.93

block sensitivity: 0.93

a painfully funny ode to bad behavior .

1. Not a funny story, just bad behavior . s(f,x,P) = 0.96

Low Sensitivity:

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . High Sensitivity: s(f,x,P) = 0.93

block sensitivity: 0.93

a painfully funny ode to bad behavior .

1. Not a funny story, just bad behavior . s(f,x,P) = 0.96

2. a painfully bleak ode to bad behavior . s(f,x,P) = 0.74

Low Sensitivity:

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . High Sensitivity: s(f,x,P) = 0.93

block sensitivity: 0.93

a painfully funny ode to bad behavior .

1. Not a funny story, just bad behavior . s(f,x,P)

bad movies.

2. a painfully bleak ode to bad behavior.

3. a painfully funny ode to

s(f,x,P) = 0.96

s(f,x,P) = 0.74

s(f,x,P) = 0.18

block sensitivity: 1.88

Sensitivity for Sequence Classification

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks

Sensitivity for Sequence Classification

formalizes complexity of decision boundary



Difficult Task

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks

Sensitivity for Sequence Classification

formalizes complexity of decision boundary

generalizes theory from Boolean functions to general sequence classification

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks



$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^{k} s(f,x,P_i)$$

1

Sensitivity for Sequence Classification

formalizes complexity of decision boundary

generalizes theory from Boolean functions to general sequence classification

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks



$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^{k} s(f,x,P_i)$$

1

	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,		
LSTM		
Transformer		







































Averaging word embeddings to derive sentence embeddings (Wieting et al., 2015; Arora et al., 2017; Ethayarajh, 2018)



Averaging word embeddings to derive sentence embeddings (Wieting et al., 2015; Arora et al., 2017; Ethayarajh, 2018)

Convolutional Networks (Kim 2016) with Average Pooling



Averaging word embeddings to derive sentence embeddings (Wieting et al., 2015; Arora et al., 2017; Ethayarajh, 2018)

Convolutional Networks (Kim 2016) with Average Pooling

Log-linear models and SVMs using n-gram features



this is an amazing movie, really stunning visuals and acting

 $bs(f,x) \le 2L^2 C^2 k^2$



this is an amazing movie, really stunning visuals and acting

 $bs(f,x) \le 2L^2 C^2 k^2$ Lipschitz constant of output function



this is an amazing movie, really stunning visuals and acting

 $bs(f,x) \le 2L^2 C^2 k^2$ Norm of vectors



this is an amazing movie, really stunning visuals and acting

 $bs(f,x) \le 2L^2 C^2 k^2$ Window width



this is an amazing movie, really stunning visuals and acting

 $bs(f,x) \le 2L^2 C^2 k^2$

independent of the input length!

	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,		
LSTM		
Transformer		

	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,	No	
LSTM		
Transformer		

	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,	No	Strict Bound
LSTM		
Transformer		

LSTMs and Transformers

RNNs and LSTMs can express PARITY because they express all regular languages (Horne and Hush, 1994)



LSTMs and Transformers

RNNs and LSTMs can express PARITY because they express all regular languages (Horne and Hush, 1994)



Transformers cannot express PARITY generalizably across input lengths

Transformers and PARITY

Proof Idea:

Assume we have a candidate transformer given.

For proof, see: Hahn (2020, TACL)

Transformers and PARITY

Proof Idea:

Assume we have a candidate transformer given.

We construct a pair of inputs that are classified the same, even though their parity differs

For proof, see: Hahn (2020, TACL)
Transformers and PARITY

Proof Idea:

Assume we have a candidate transformer given.

We construct a pair of inputs that are classified the same, even though their parity differs

Method: We fix a few input bits to 'distract' the transformer, so that it ignores most input bits.







Idea: Some input bits will be ignored, since their attention weights are always smaller than those of the fixed bits.



	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,	No	Strict Bound
LSTM	Yes	
Transformer	No	

Uniformly random Boolean functions



Randomly initialized LSTMs, binarized scalar output with a threshold chosen to balance +1 and -1 outputs.

Uniformly random Boolean functions





- LSTM with 128 units, Adam (lr 0.003, batch size 32)
- No train/test split this tests fitting ability, not generalization.

With a transformer (4 layers, 4 heads, 32 units)



With a transformer (4 layers, 4 heads, 32 units)

8 layers



With a transformer (4 layers, 4 heads, 32 units)

8 layers

512 units



	Can represent f _{PARITY} ?	Can practically learn high-sensitivity functions?
Lexical Classifier, CNN,	No	Strict Bound
LSTM	Yes	Hard
Transformer	No	Hard

Sensitivity for Sequence Classification

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

Sensitivity Bounds for ML Methods

Sensitivity for Sequence Classification

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

Sensitivity Bounds for ML Methods

Sensitivity can be used for rigorous analysis of the power of ML models

$$bs(f,x) \le 2L^2 C^2 k^2$$



Sensitivity for Sequence Classification

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

Sensitivity Bounds for ML Methods

Sensitivity can be used for rigorous analysis of the power of ML models

Sensitivity predicts learnability



Sensitivity for Sequence Classification

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

Sensitivity Bounds for ML Methods

$$bs(f,x) := \max_{k,P_1 \cup ..., \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$
$$s(f,x,P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$$



the task.

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$
$$s(f,x,P) := \operatorname{Var}\left(f(X) | X \in x^{\oplus P}\right)$$

Inputs that agree with x outside of positions in P.

Sampled using XLNet (Yang et al 2019) and u-PMLM

(Liao et al 2020).

$$bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

Exponential number of subsets!

Restrict to polynomial number of subsets

Results in lower bound

Text Classification



- CR, MR: review sentiment (Hu and Liu, 2004; Pang and Lee, 2005)
- MPQA: question type (Wiebe et al., 2005)
- Subj: subjectivity (Pang and Lee, 2005)
- f estimated using finetuned RoBERTa (Liu et al., 2019)



Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later.

Hypothesis:

Steve Jobs worked for Apple.

Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 1. Chris Cook was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later.

Hypothesis:

Steve Jobs worked for Apple.

Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 1. Chris Cook was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 2. Steve Jobs was attacked by Sculley and the other executives [...] and resigned from the company a few weeks later. Hypothesis:

Steve Jobs worked for Apple.

Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 1. Chris Cook was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 2. Steve Jobs was attacked by Sculley and the other executives [...] and resigned from the company a few weeks later. Hypothesis:

Steve Jobs worked for Apple.

3. Jobs later worked for Apple

Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 1. Chris Cook was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 2. Steve Jobs was attacked by Sculley and the other executives [...] and resigned from the company a few weeks later. Hypothesis:

Steve Jobs worked for Apple.

- 3. Jobs later worked for Apple
- 4. Steve Jobs returned to Apple

Steve Jobs was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 1. Chris Cook was attacked by Sculley and other Apple executives [...] and resigned from the company a few weeks later. 2. Steve Jobs was attacked by Sculley and the other executives [...] and resigned from the company a few weeks later. Hypothesis:

Steve Jobs worked for Apple.

- 3. Jobs later worked for Apple
- 4. Steve Jobs returned to Apple
- 5. Steve Jobs worked for Google

Syntax



• Anaphor licensing (Marvin and Linzen, 2018; Hu et al., 2020)

"The author next to the senators hurt {himself, themselves}." "The author that liked the senators hurt {himself, themselves}."

• Estimated using medium-size GPT-2



• f estimated using off-the-shelf parser (Qi et al., 2018, 2020) on English Web Treebank



Input length doesn't explain away sensitivity differences












Using u-PMLM (Liao et al., 2020) instead of XLNet:







Low Sensitivity:

- a gorgeous, witty, seductive movie.
- 1. a farce of ideas squanders this movie .

High Sensitivity:

- a painfully funny ode to bad behavior.
- 1. Not a funny story, just bad behavior.
- 2. a painfully bleak ode to bad behavior .
- 3. a painfully funny ode to b
 - bad movies .



https://nlp.stanford.edu/sentiment/treebank.html?w=ode%2Cbad





Low Sensitivity:

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie .

Only positive constituents Dispersion 0 Block Sensitivity 0.93

Low Sensitivity:

a gorgeous, witty, seductive movie.

1. a farce of ideas squanders this movie . High Sensitivity:

a painfully funny ode to bad behavior.
1. Not a funny story, just bad behavior.
2. a painfully bleak ode to bad behavior.
3. a painfully funny ode to bad movies.

Only positive constituents Dispersion 0 Block Sensitivity 0.93

3 positive constituents 5 negative constituents Dispersion 0.97 Block Sensitivity 1.88



Sentence length not significant beyond sensitivity (p > 0.05)

Sensitivity as a Complexity Measure for Sequence Classification Tasks

Sensitivity for Sequence Classification

 $bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^{\infty} s(f,x,P_i)$

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks

Sensitivity predicts task difficulty



Sensitivity as a Complexity Measure for Sequence Classification Tasks

Sensitivity for Sequence Classification

 $bs(f,x) := \max_{k,P_1 \cup \dots \cup P_k} \sum_{i=1}^{k} s(f,x,P_i)$

Sensitivity Bounds for ML Methods

Sensitivity and Difficulty of NLP Tasks

Sensitivity predicts task difficulty

Sensitivity identifies difficult inputs







Pretrained models extract features from which label can be decoded with simple classifiers





Models often rely on spurious statistical patterns

Models often rely on spurious statistical patterns

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Models often rely on spurious statistical patterns

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018)

Models often rely on spurious statistical patterns

Make the decision boundary `simpler' (e.g., Gardner et al. 2019).

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018)

Models often rely on spurious statistical patterns

Make the decision boundary `simpler' (e.g., Gardner et al. 2019).

<u>Conjecture:</u> They reduce sensitivity.

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018)

Models often rely on spurious statistical patterns

Make the decision boundary `simpler' (e.g., Gardner et al. 2019).

<u>Conjecture:</u> They reduce sensitivity.

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018) Labels are correlated with output of simple lexical classifiers

Models often rely on spurious statistical patterns

Make the decision boundary `simpler' (e.g., Gardner et al. 2019).

<u>Conjecture:</u> They reduce sensitivity.

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018) Labels are correlated with output of simple lexical classifiers

Changing the premise while staying within the task distribution less likely to flip the label

Models often rely on spurious statistical patterns

Make the decision boundary `simpler' (e.g., Gardner et al. 2019).

<u>Conjecture:</u> They reduce sensitivity.

Simple lexical correlates of the label in Reading Comprehension (e.g. Kaushik and Lipton, 2018; Gururangan et al., 2018)

Hypothesis alone predictive of the label in entailment tasks (Poliak et al., 2018) Labels are correlated with output of simple lexical classifiers

Changing the premise while staying within the task distribution less likely to flip the label

<u>Future work:</u> Can sensitivity help automatically mitigate spurious patterns?

Introduced sensitivity as a complexity measure for sequence classification

Introduced sensitivity as a complexity measure for sequence classification

Measures complexity of decision boundary



Simple Task



Difficult Task

Introduced sensitivity as a complexity measure for sequence classification

Measures complexity of decision boundary

Generalizes well-studied theory from Boolean functions to general sequence classification

 $bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$



Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Simple lexical classifiers cannot express high-sensitivity functions

 $bs(f,x) \leq 2L^2C^2k^2$

Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Simple lexical classifiers cannot express high-sensitivity functions

$$bs(f,x) \le 2L^2 C^2 k^2$$

Even LSTMs & Transformers are biased towards low sensitivity





Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Sensitivity predicts difficulty of NLP tasks

Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Sensitivity predicts difficulty of NLP tasks

Characterizes which tasks require pretrained models



Introduced sensitivity as a complexity measure for sequence classification

Sensitivity predicts what functions are difficult for ML models

Sensitivity predicts difficulty of NLP tasks

Characterizes which tasks require pretrained models







Predicts difficulty of individual inputs
Thanks!

Why Subsets?

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

(1) Words are composed into phrases. Changing a phrase can change meaning when changing any word cannot.

a gorgeous, witty, seductive movie. a farce of ideas squanders this movie.

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

- (1) Words are composed into phrases. Changing a phrase can change meaning when changing any word cannot.
- (2) There are distributions \prod where we would always get 0 with singletons.

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

- (1) Words are composed into phrases. Changing a phrase can change meaning when changing any word cannot.
- (2) There are distributions \prod where we would always get 0 with singletons.
- (3) Block sensitivity can only increase with finer tokenization.

$$bs(f,x) := \max_{k,P_1 \cup ... \cup P_k} \sum_{i=1}^k s(f,x,P_i)$$

- (1) Words are composed into phrases. Changing a phrase can change meaning when changing any word cannot.
- (2) There are distributions \prod where we would always get 0 with singletons.
- (3) Block sensitivity can only increase with finer tokenization.
- (4) Model fit predicting accuracy on SST-2 is stronger with block sensitivity



Relation to Adversarial Examples

Relation to Adversarial Examples

Adversarial Brittleness

(Szegedy et al., 2013; Jia and Liang, 2017)

Neighboring inputs on which the model output changes erroneously.

sh the model

Neighboring inputs within the data distribution on which the true label changes.

a painfully funny ode to bad behavior



+1

a painfully funny ode to bad behavior +

a painfully funny ode to terrible behavior +1 -1

+1

High Sensitivity

Measuring Sensitivity without Models

overall very good for what it's trying to do.

The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility



The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility



The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility

overall very good for what it's trying to do.

The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility



The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility



The review sounds POSITIVE. Can you change the text so it sounds NEGATIVE?

Save and try another possibility



Poisson regression: $\beta = 0.061$, p = 0.0023

controlling for task, sentence length, and random variation between sentences and annotators.



Empirical Learnability of PARITY

Empirical Learnability Results:



Bhattamishra, Ahuja, Goyal (2020, EMNLP)

Empirical Learnability Results:



Bhattamishra, Ahuja, Goyal (2020, EMNLP)

Empirical Learnability Results:



LSTM

Bhattamishra, Ahuja, Goyal (2020, EMNLP)

Sensitivity using Human Oracle Labels

Sensitivity using Human Oracle Labels



Role of Task Model

Role of Task Model



Task — QQP — RTE — SST2

Even powerful neural models are biased towards low sensitivity



Even powerful neural models are biased towards low sensitivity



Empirical and theoretical evidence that neural networks generalize because they are biased towards "simple" functions (De Palma et al., 2018).

Even powerful neural models are biased towards low sensitivity



Empirical and theoretical evidence that neural networks generalize because they are biased towards "simple" functions (De Palma et al., 2018).

Some studies propose notions close to sensitivity (Franco, 2006; De Palma et al., 2018, Novak et al., 2018).

Even powerful neural models are biased towards low sensitivity



Empirical and theoretical evidence that neural networks generalize because they are biased towards "simple" functions (De Palma et al., 2018).

Some studies propose notions close to sensitivity (Franco, 2006; De Palma et al., 2018, Novak et al., 2018).

Empirically, neural networks learn low Fourier frequencies first

(Rahaman et al., 2019; Xu et al., 2019; Cao et al., 2019).

• For Boolean functions: low average sensitivity <=> Fourier spectrum concentrated on low frequencies!

Other Complexity Metrics

Chomsky Hierarchy and Kolmogorov Complexity are orthogonal to sensitivity



Kolmogorov Complexity










Other Complexity Measures

Chomsky Hierarchy and Kolmogorov Complexity are orthogonal to sensitivity



Conjecture about Degree and Block Sensitivity

Conjecture 2. Define bs(f, x, P) as in (1).

For $d \in [n]$, let $\Pi_d f$ be the orthogonal projection of f onto the subspace of degree-d polynomials in $L^2(\{-1,1\}^n, \mathbb{P})$. Define the "average degree" to be

$$adeg(f) := \sum_{d=1}^{n} d \cdot \|\Pi_d f - \Pi_{d-1} f\|_2^2$$
(3)

Then the conjecture is:

$$adeg(f) \le \mathop{\mathbb{E}}_{x \sim \mathbb{P}} bs(f, x)$$
 (4)



Proof for Transformers and PARITY





Idea: Some input bits will be ignored, since their attention weights are always smaller than those of the fixed bits.









For each input bit, imagine the highest possible attention value.



By fixing one input, we can make the head ignore all remaining input bits.



By fixing one input, we can make the head ignore all remaining input bits.



Now let's repeat this for every Layer 1 head.



Now let's repeat this for every Layer 1 head.



Now let's repeat this for every Layer 1 head.





Solution: Fix bits in such a way that each head ignores all but *k* input bits (for some constant *k*)



Solution: Fix bits in such a way that each head ignores all but *k* input bits (for some constant *k*)



Solution: Fix bits in such a way that each head ignores all but *k* input bits (for some constant *k*)



Solution: Fix bits in such a way that each head ignores all but *k* input bits (for some constant *k*).

Can guarantee that this fixes only < 10% of bits.



Set each input i.i.d. to

- * with p=95%
- 0 with p=2.5%
- 1 with p=2.5%



Set each input i.i.d. to

- * with p=95%
- 0 with p=2.5%
- 1 with p=2.5%



What is Probability that

- 1) each head depends on only k inputs, and
- 2) only < 10% of bits are fixed?

Enough to show that this is > 0!



*

Show this k each head

*

0

*

What is Probability that

- 1) each head depends on only k inputs, and
- 2) only < 10% of bits are fixed?

Enough to show that this is > 0!

Show this by calculating for each head and combining via Lovasz Local Lemma.

Input

Layer 1



We can now fold Layer 1 into Layer 2....



We can now fold Layer 1 into Layer 2....

...and repeat the construction...



We can now fold Layer 1 into Layer 2....

...and repeat the construction...

...until only the final layer remains!



The prediction ignores bit X₅!

Thus, the transformer could never have modeled Parity (or Dyck₂).