Is "Attention = Explanation"? Past, Present & Future

Sarthak Jain & Sarah Wiegreffe Big Picture Workshop, Dec. 2023



Allen Institute for Al

W UNIVERSITY of WASHINGTON

Talk Outline

- 1. Introduction & why we studied this problem
- 2. Attention is not Explanation
- 3. Attention is not not Explanation
- 4. Current & Future Relevance (let's talk about transformers)

Part 1: Introduction & why we studied this problem

Why was this question interesting to Sarthak?

other languages

Help Curators find relevant parts of document

Coch	nran	e Trusted evidence Informed decisio Better health.		Search		Q
Our evidence	About us	Join Cochrane	News and jobs		Cochrane Library	►
		Coronavir	us (COVID-19) resources			
		is the diagnosti	c accuracy of antibody tes	ts for th	e detection of	
Published:	Backgro		VID-13 VIIUS.		Am) score { 1,812 Who is talking about this ar	ticle
25 June 2020 Authors: Deeks JJ, Dinnes J, Takwoingi Y Davenport C, Spijker R, Taylor- Phillips S, Adriano A, Beese S,	easily be with CO no symp	etween people in a simil VID-19 have a mild to me	e caused by the SARS-CoV-2 virus that: ar way to the common cold or 'flu. Mos oderate respiratory illness, and some n fection). Others experience severe sym nd <u>intensive care</u> .	st people nay have	Cochra Crowd	
retzke J, Ferrante di Ruffano L Iarris IM, Price MJ, Dittrich S, mperador D, Hooft L, Leeflang IMG, Van den Bruel A	The imn develop detect a	ing proteins that can att	who have COVID-19 responds to infectic ack the virus (antibodies) in their bloo ood might show whether they currently sly.	d. Tests to	Become a citizen scient	tis
Primary Review Group: nfectious Diseases Group	Why are	accurate tests import	ant?			
	Accurate	testing allows identifie	ation of people who might people treats	agent or	Cochrane evidence in	

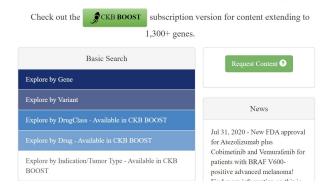
Accurate testing allows identification of people who might need treatment, or

1 6 6 9 - - -

since 2016. CKB CORE contains all the content associated with 85 genes that are commonly found on cancer hotspot panels. New and updated content is pushed out daily and viewable genes are available on a quarterly rotating schedule.

The Clinical Knowledgebase (CKB) Powered by The Jackson Laboratory CKB is a dynamic digital resource for interpreting complex cancer genomic profiles in the context of protein impact, therapies, and clinical trials. CKB CORE is the public access version we have been providing to the community

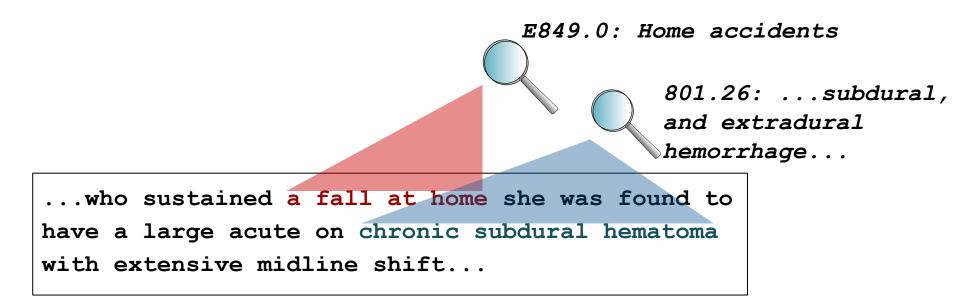
Not finding the content you need? Need more advanced searching?



aka.ms/hanover

http://evidence-inference.ebm-nlp.com/

Why was this question interesting to Sarah?



Mullenbach, Wiegreffe, Duke, Sun, and Eisenstein. <u>NAACL 2018.</u>

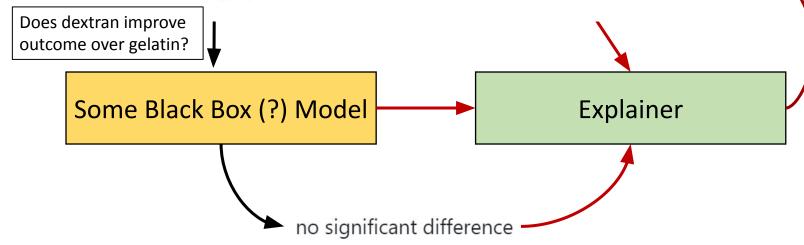
A Generic Classification Setup

In group A, lower peak (median) plasma levels of procalcitonin (0.2 versus 1.4, p < 0.001), IL 8 (5.6 versus 94.8, p < 0.001), IL 10 (47.2 versus 209.7, p = 0.001), endothelial leukocyte adhesion molecule-1 (88.5 versus 130.6, p = 0.033), intercellular adhesion molecule-1 (806.7 versus 1,375.7, P = 0.001) and troponin-I (0.22 versus 0.66, p = 0.018) were found. There was no significant difference in IL 6, IL-6r and C-reactive protein values between groups. Higher figures of the cardiac index (p = 0.010) along with reduced systemic vascular resistance (p = 0.005) were noted in group A.

Does dextran improve outcome over gelatin? Some Black Box (?) Model

A Generic Classification Setup (with Heatmap based Explanation)

In group A, lower peak (median) plasma levels of procalcitonin (0.2 versus 1.4, p < 0.001), IL 8 (5.6 versus 94.8, p < 0.001), IL 10 (47.2 versus 209.7, p = 0.001), endothelial leukocyte adhesion molecule-1 (88.5 versus 130.6, p = 0.033), intercellular adhesion molecule-1 (806.7 versus 1,375.7, P = 0.001) and troponin-I (0.22 versus 0.66, p = 0.018) were found. There was no significant difference in IL 6, IL-6r and C-reactive protein values between groups. Higher figures of the cardiac index (p = 0.010) along with reduced systemic vascular resistance (p = 0.005) were noted in group A.

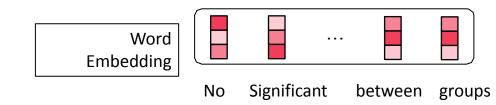


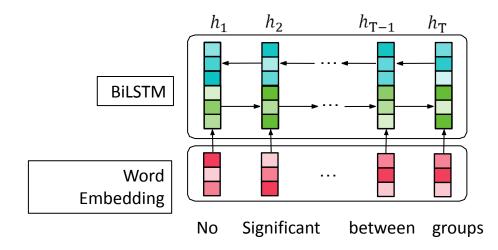
Neural Attention

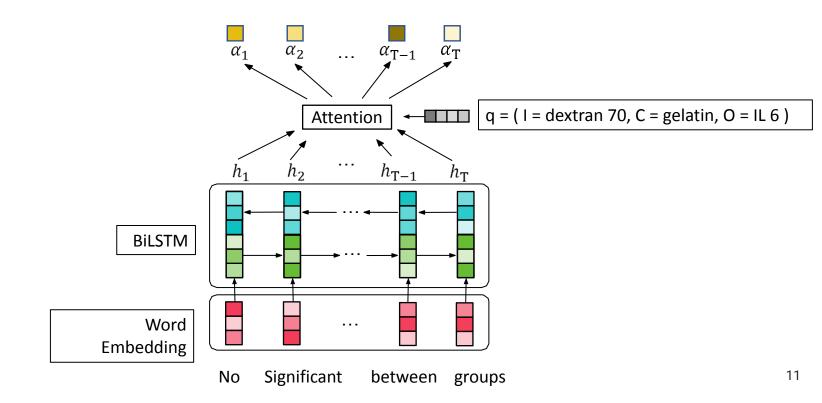


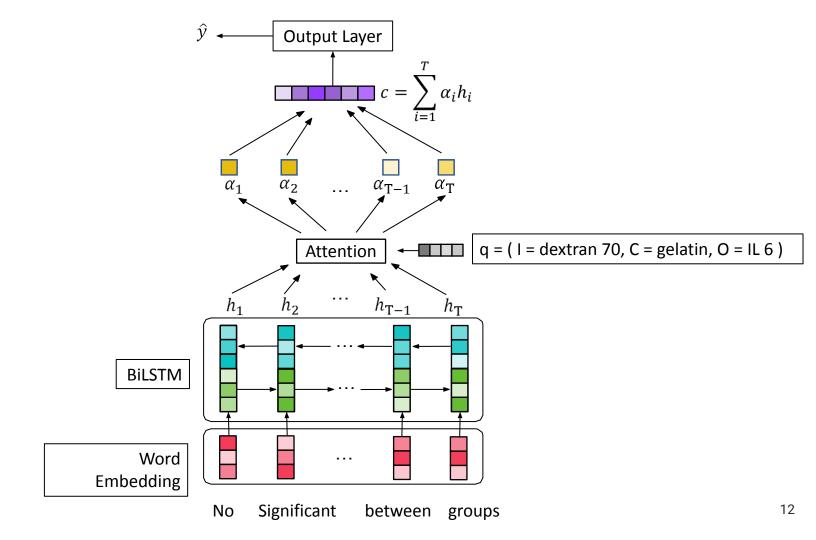
A <u>stop</u> sign is on a road with a mountain in the background.

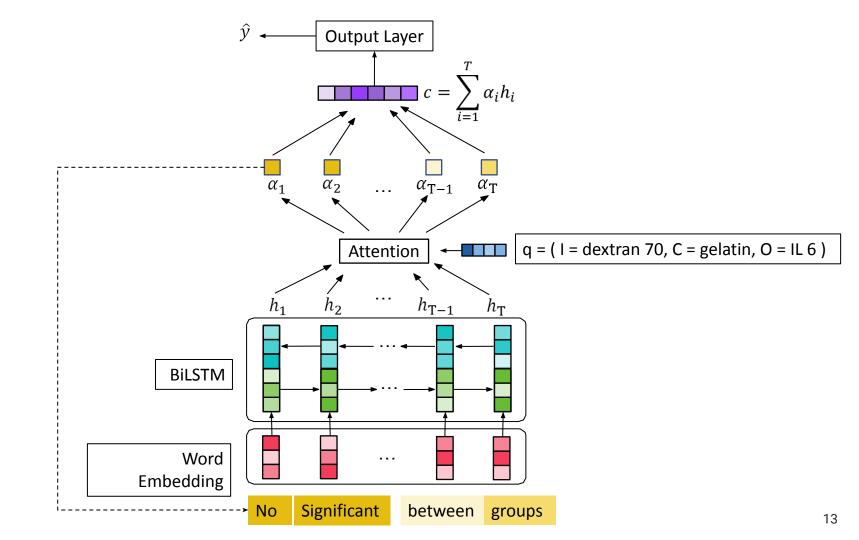
In group A, lower peak (median) plasma levels of procalcitonin (0.2 versus 1.4, p < 0.001), IL 8 (5.6 versus 94.8, *p* < 0.001), IL 10 (47.2 versus 209.7, *p* = 0.001), endothelial leukocyte adhesion molecule-1 (88.5 versus 130.6, p = 0.033), intercellular adhesion molecule-1 (806.7) versus 1,375.7, P = 0.001) and troponin-I (0.22 versus 0.66, p = 0.018) were found. There was no significant difference in IL 6, IL-6r and C-reactive protein values between groups. Higher figures of the cardiac index (p = 0.010) along with reduced systemic vascular resistance (p = 0.005) were noted in group A.











Unclear Questions

What does Attention heatmap tell us – How "important" a word is?

Is there really a 1:1 mapping between Attention and input tokens?

Does Attention tell us how a model reached its prediction?

Part 2: Attention is not Explanation

Jain, S., & Wallace, B.C. (2019). Attention is not Explanation. NAACL-HLT.



Empirical Questions

1. Do Attention weights correlate with existing feature importance measures (gradients and leave-one-out)?

2. **Uniqueness:** Had we attended to different inputs, would the prediction have been different ?

Tasks and Datasets

Binary Classification

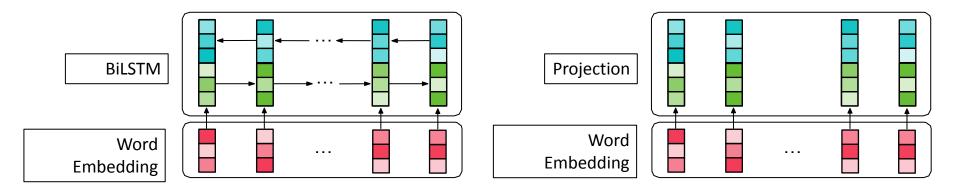
- o Sentiment Classification Stanford Sentiment Treebank, IMDB
- o Topic Classification 20NewsGroup, AGNews
- Diagnosis (MIMIC-III) Diabetes, Anemia
- o Twitter Adverse Drug Reaction
- Multiple Choice Question Answering
 o CNN News, bAbl

Entailment

o SNLI

Encoder Models

• We aim to evaluate whether Attention weights provide transparency, under different encoders consistently



Empirical Questions

1. Do Attention weights correlate with existing feature importance measures (gradients and leave-one-out)?

2. Uniqueness: Had we attended to different inputs, would the prediction have been different ?

Feature Importance – Experiments

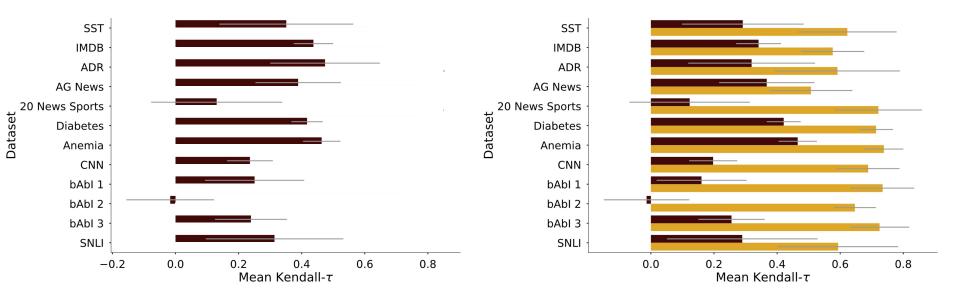
- Rank Correlation (Kendall-Tau) between Attention Scores and Feature Importance Measures (gradients and leave-one-out)
- 0 = no correlation, 1 = perfect correlation
- Total Variation Distance: for comparing class predictions between 2 models

$$ext{tvd}(\hat{y}_1, \hat{y}_2) = rac{1}{2} \sum_{i=1}^{|\mathcal{Y}|} |\hat{y}_{1i} - \hat{y}_{2i}|$$

Feature Importance – Results

GRADIENTS VS ATTENTION

LEAVE-ONE-OUT VS ATTENTION







Empirical Questions

1. Do Attention weights correlate with existing feature importance measures (gradients and leave-one-out)?

2. **Uniqueness:** Had we attended to different inputs, would the prediction have been different ?

Counterfactual Experiments

Empirical questions to measure Uniqueness:

How much on average does an output change if we randomly permute Attention scores?

Can we find maximally different Attention that doesn't change the output by more than some epsilon?

Adversarial Attention – Experiment

For each example -

Find k Attention distributions that are

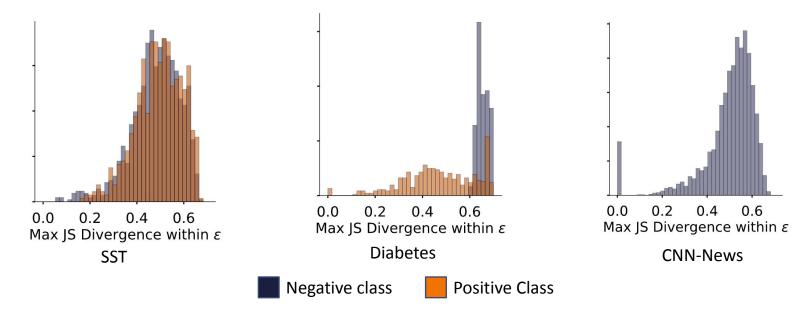
- 1. Maximally different from observed Attention $\hat{\alpha}$, using JS Divergence.
- 2. Maximally different from each other

 \rightarrow argmax over $\{\alpha^{(1)}, ..., \alpha^{(k)}\}$

$$\sum_{i=1}^{k} JSD(\alpha^{(i)}, \hat{\alpha}) + \frac{1}{k(k-1)} \sum_{i>i} JSD(\alpha^{(i)}, \alpha^{(j)})$$

3. Doesn't change output by more than epsilon (= 0.001).

Adversarial Attention – Results (BiLSTM)



Original: reggio falls victim to relying on the very digital technology that he fervently scorns creating a meandering inarticulate and ultimately disappointing film

Adversarial: reggio falls victim to relying on the very digital technology that he fervently scorns creating a meandering inarticulate and ultimately disappointing film $\Delta \hat{y}$: 0.005

Conclusions

Correlation between Attention and Feature Importance scores are often low

Attention distributions do not uniquely characterize *why* a model made a given prediction; alternative heatmaps would have yielded the same output

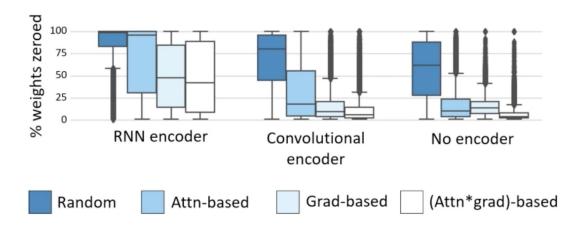


•Attention do not provide clear and consistent interpretation of why a model made a prediction.

•We should question what the author is trying to convey with the heatmap.

Concurrent Relevant Work: Serrano & Smith

- Focused on whether Attention provides relative importance of hidden states themselves
- How quickly does Attention flip when zeroing out attention scores according to their rank?





Part 3: Attention is not *not* Explanation

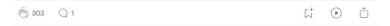
Wiegreffe, S.*, & Pinter, Y.* (2019). Attention is not not Explanation. EMNLP.



Blogpost #1

Attention is not not Explanation





[**Update**, **August 13** — **December 6**, **2019**: Sarah Wiegreffe and I performed experiments to follow up on the points here, as well as constructive setups for detecting and claiming faithful explanation, presented at EMNLP 2019. The paper is available <u>here</u>.

Byron Wallace responded to the paper here.]

[This post is intended for an NLP practitioner audience, and assumes its readers know what attention modules are and how they are being used. All feedback is welcome, either here or to *uvp@gatech.edu* or to *@yuvalpi* on Twitter.]

An upcoming <u>NAACL</u> paper was uploaded to arXiv earlier this month, and has been making the rounds on social media. The title chosen for it was <u>Attention is not Explanation</u>; the authors are Sarthak Jain and Byron C. Wallace (from here on I will refer to them, and the paper, as J&W). Such a title sets high expectations for a rigorous, convincing proof of the claim. In this post I argue that it does not deliver on them.

Main Arguments

- 1. Explanation can be **many things**
- 2. Rank Correlation is not always appropriate + missing baselines
- 3. Counterfactual Distributions are **not Counterfactual Weights**
 - a. Attention distribution is **not a primitive**

Explanation can be many things

- Explainability = both post-hoc rationalizations and faithful "interpretability".
- Human explanation is post-hoc
 - invent a story that plausibly justifies our actions, even if it not an entirely accurate reconstruction



Counterfactual Distributions are *not* Counterfactual Weights

- Detaching attention scores from the attention mechanism degrades the model itself.
 - Attention scores are not assigned arbitrarily by the model.
 - Jain & Wallace removed the linkage that motivates the original claim of attention distribution explainability.
- Adversarial search was *per-instance*
- Too high degree of freedom

Blogpost #2: Response to Sarah/Yuval

"Attention is not Explanation" - Assumption or Conclusion?

Strengthening the Feature Importance Correlation Experiments

If Attention distribution is not a primitive, what do heatmaps tell us?





"Attention is not Explanation" - Assumption or Conclusion?

• Why expect attention to have any identification with input tokens, given contextualization layer?

• We assumed faithfulness as necessary component of any explanation method, but didn't clarify it enough.





Strengthening the Feature Importance Correlation Experiments

• Does gradient and Leave-one-out correlate with each other?

• Rank Correlation metrics do not take account magnitudes and long tail can artificially depress the correlation scores.





If Attention distribution is not a primitive, what do heatmaps tell us?

• Attention model rather than Attention heatmap is the valid primitive - **we agree**. But then why show heat-maps over a handful of examples?

• Multiple valid causes can exist - **we agree**. But does attention tell us which one model used?



Attention is not not Explanation

- 1. Explanation can be **many things**
- 2. Rank Correlation is not always appropriate + **missing baselines**
- 3. Counterfactual Distributions are **not Counterfactual Weights**

Attention is not not Explanation

- 1. Explanation can be **many things**
- 2. Rank Correlation is not always appropriate + missing baselines
- 3. Counterfactual Distributions are **not Counterfactual Weights**
- 4. Random seed variance as a baseline for adversaries

What is explanation?

Plausible Explainability

- **Goal:** increasing user trust, satisfaction, or understanding
- Rationale generation (Ehsan et al. 2019, Riedl 2019)
- Evaluation: users



What is explanation?

Plausible Explainability

- **Goal:** increasing user trust, satisfaction, or understanding
- Rationale generation (<u>Ehsan et al. 2019</u>, <u>Riedl 2019</u>)
- Evaluation: users



Faithful Explainability

- **Goal:** understanding how models make predictions (Lipton 2016, Rudin 2018)
- Models' explanations are exclusive
- Evaluation: not exclusively users



What is explanation?

Plausible Explainability

- **Goal:** increasing user trust, satisfaction, or understanding
- Rationale generation (<u>Ehsan et al. 2019</u>, <u>Riedl 2019</u>)
- Evaluation: users



Faithful Explainability

- **Goal:** understanding how models make predictions (<u>Lipton 2016</u>, <u>Rudin 2018</u>)
- Models' explanations are exclusive
- Evaluation: not exclusively users



If Attention is (Faithful) Explanation:

Attention should be a **necessary component** for good performance

If Attention is (Faithful) Explanation:

- Attention should be a **necessary component** for good performance
- 2. If **trained models** can vary in attention distributions while giving similar predictions, they might be bad for explanation

Necessary	
-----------	--

Hard to manipulate

If Attention is (Faithful) Explanation:

- Attention should be a **necessary component** for good performance
- 2. If **trained models** can vary in attention distributions while giving similar predictions, they might be bad for explanation
- 3. Attention weights should work well in **uncontextualized settings**

Necessary	
-----------	--

Hard to manipulate

Work out of context

Selecting Meaningful Tasks

Necessary

1. Attention should be a **necessary component** for good performance

Searching for Adversarial Models

Hard to manipulate

- 1. Attention should be a **necessary component** for good performance
- 2. If **trained models** can vary in attention distributions while giving similar predictions, they might be bad for explanation

Adversarial Training

- 1. Train a base model (M_b)
- 2. Train an adversary (M_a) that **minimizes change in prediction scores** from the base model, while *maximizing changes in the learned attention distributions.*

$$\mathcal{L}(\mathcal{M}_a,\mathcal{M}_b)^{(i)}= ext{tvd}(\hat{y}_a^{(i)},\hat{y}_b^{(i)})-\lambda\,\, ext{kl}(oldsymbollpha_a^{(i)}\paralleloldsymbollpha_b^{(i)})$$

Adversarial Training

- 1. Train a base model (M_b)
- 2. Train an adversary (M_a) that **minimizes change in prediction scores** from the base model, while *maximizing changes in the learned attention distributions.*

$$\mathcal{L}(\mathcal{M}_a,\mathcal{M}_b)^{(i)} = ext{tvd}(\hat{y}_a^{(i)},\hat{y}_b^{(i)}) - \lambda ext{KL}(oldsymbol{lpha}_a^{(i)} \parallel oldsymbol{lpha}_b^{(i)})$$

Comparisons

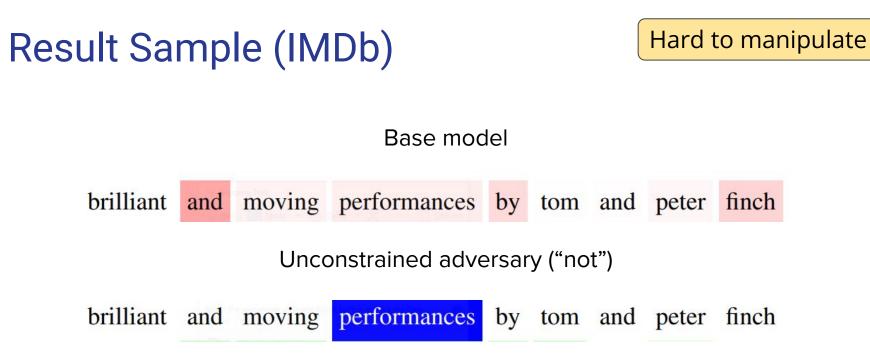
- 1. Random seed variance
- - Re-running the **base setup** with multiple random seeds to calibrate what a. we expect for variance in attention weights
- 2. Jain & Wallace (2019) 🕂
 - Instance-specific adversarial attention weights а.
 - No consistency requirement b.
 - No model trained C.

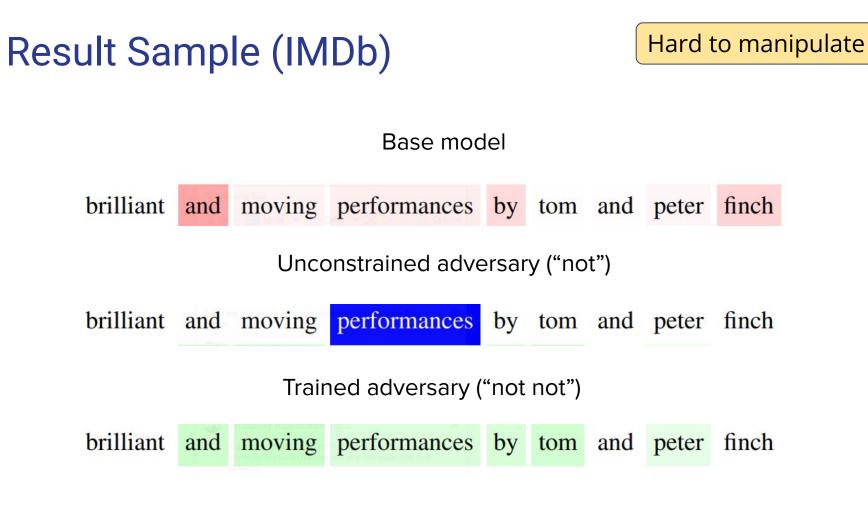
Result Sample (IMDb)

Hard to manipulate

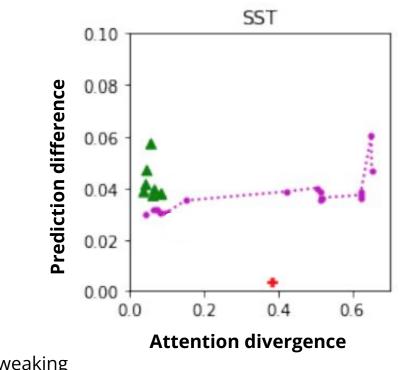
Base model

brilliant and moving performances by tom and peter finch





Hard to manipulate



Random seed J&W untrained tweaking Trained divergence (lambdas)

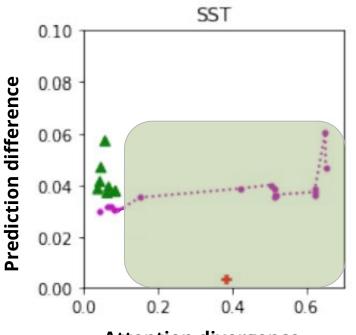
- Slow increase in prediction difference
 - Does not support use of attention weights for faithful explanation

Random seed

J&W untrained tweaking

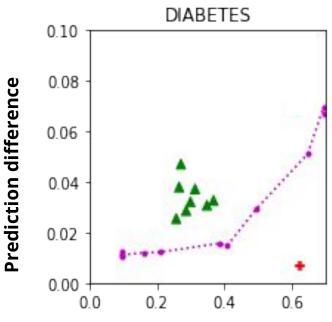
Trained divergence (lambdas)

Hard to manipulate

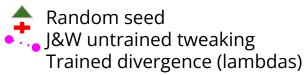




Hard to manipulate

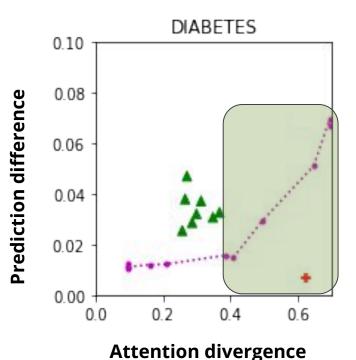


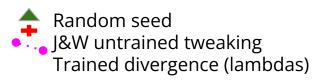
Attention divergence



- Fast increase in prediction difference = attention scores not easily manipulable
 - Supports use of attention weights for faithful explanation

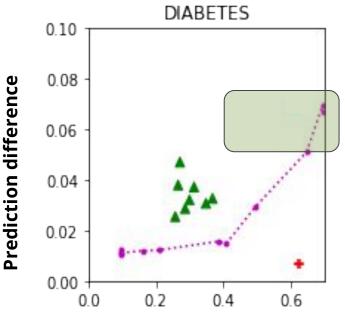






- Fast increase in prediction difference = attention scores not easily manipulable
 - Supports use of attention weights for faithful explanation
- Another interpretation: y-axis differences are small & random seed variance is high
 - Does not support use of attention weights for faithful explanation

Hard to manipulate

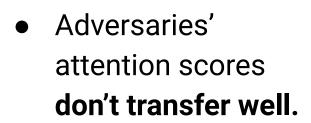


Attention divergence

Probing Attention

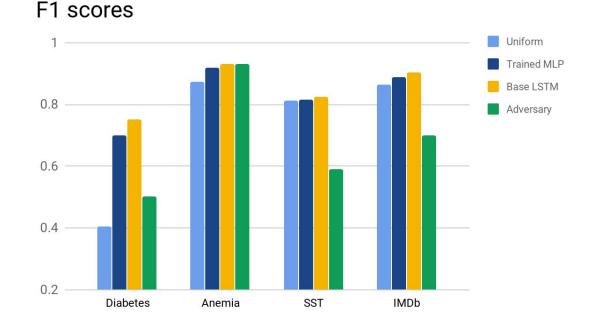
- 1. Attention should be a **necessary component** for good performance
- 2. If **trained models** can vary in attention distributions while giving similar predictions, they might be bad for explanation
- 3. Attention weights should work well in **uncontextualized settings**

Work out of context



Results

 Situation is not nearly as bleak as previously portrayed.



Conclusion

• 3 desiderata of attention for "faithful" explanation

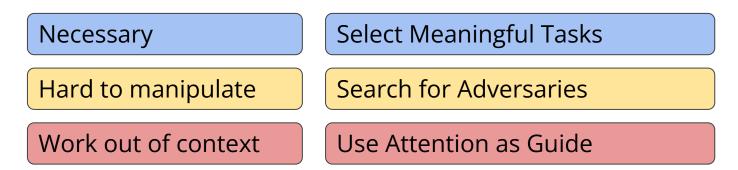
Necessary

Hard to manipulate

Work out of context

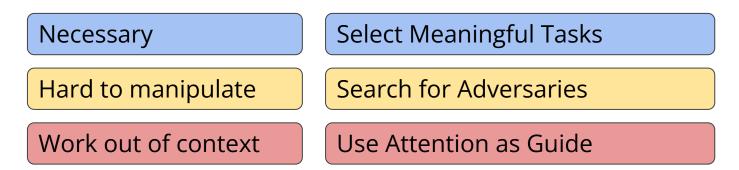
Conclusion

- 3 desiderata of attention for "faithful" explanation
- 3 methods to measure the utility of attention distributions for faithful explanation



Conclusion

- 3 desiderata of attention for "faithful" explanation
- 3 methods to measure the utility of attention distributions for faithful explanation
- Results showing performance is **highly task-dependent**



2019 Takeaways

- 1. Use guides to judge token-output correlation
- 2. Use adversarial models to investigate exclusivity
- 3. Calibrate your notion of variance
- 4. Investigate models & tasks where attention is necessary

We agreed on many things

We both valued & wanted to investigate *faithful* instance-level explanations.



- Both of our search procedures ultimately found adversarial distributions (though with varying levels of success).
- Attention as explanation depends on dataset & model.
- Different (valid) experiments can reach different views on the utility of model internals.

Our Takeaways (now)

- 1. Faithfulness and plausibility are **different criteria** with distinct merits that **must be evaluated separately.**
- 2. Attention mechanisms in LSTM networks can serve as faithful explanation **under certain conditions; there is no one-size-fits-all answer**.

Our Takeaways (now)

3. Faithfulness evaluation is difficult due to **lack of** ground-truth.

a. Researchers must convince the audience of the meaningfulness of their desiderata.

4. It's important to be careful when drawing analogies between machines and human behavior.

a. Attention is easy to compute and its qualitative results are cognitively satisfying.

We collaborated on another paper!

Association for Computational Linguistics 2020 Annual Conference

Learning to Faithfully Rationalize by Construction

Sarthak Jain, Sarah Wiegreffe, Yuval Pinter, Byron C. Wallace

- About building faithfulness directly into neural architectures (with BERT)
- Threshold attention to obtain an *explanation* first, then classify.

Related & Subsequent Work

Checkout survey Is Attention Explanation? An Introduction to the Debate (2022)

Why is Attention not faithful explanation?

(Grimsley et al. 2020, Sun & Lu 2020)

Do our results generalize to other NLP tasks?

(Vashishth et al. 2019, Pruthi et al. 2020)

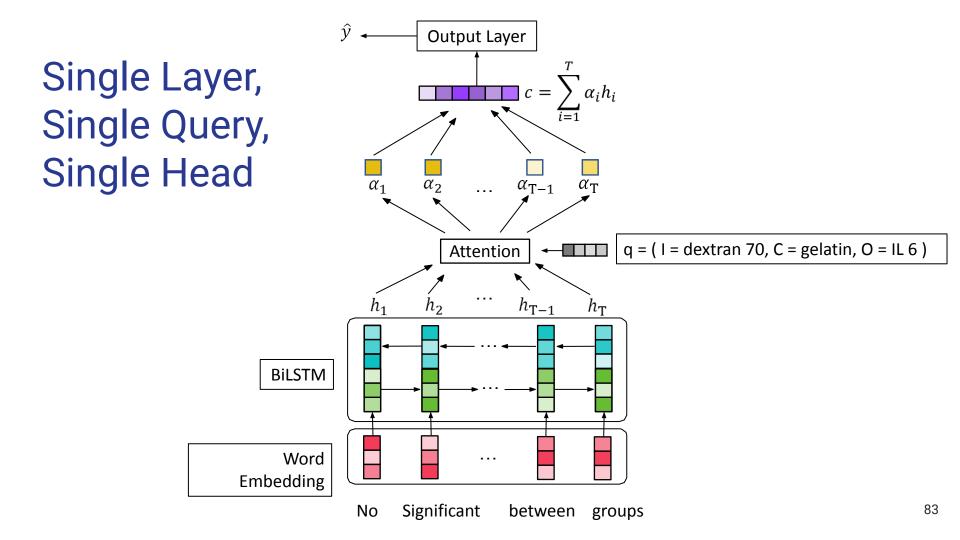
How to evaluate faithfulness?

(Jacovi & Goldberg 2020)

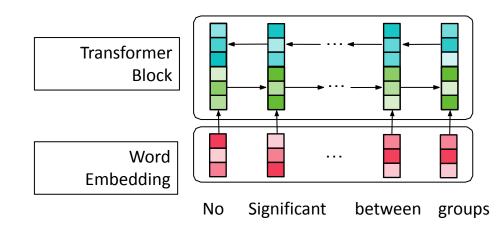
How to improve faithfulness?

(Mohankumar et al. 2020, Tutek & Snajder 2020)

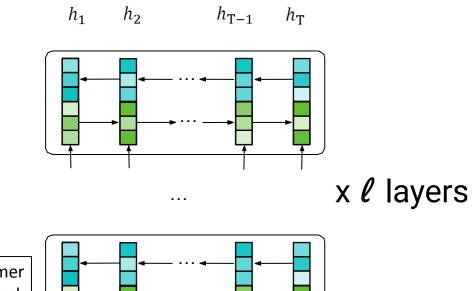
Part 4: Current & Future Relevance (let's talk about transformers)

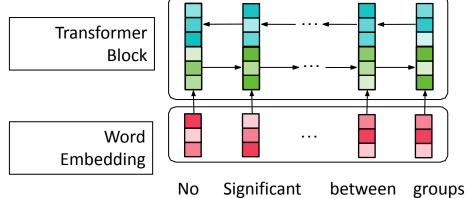


Attention in Transformers



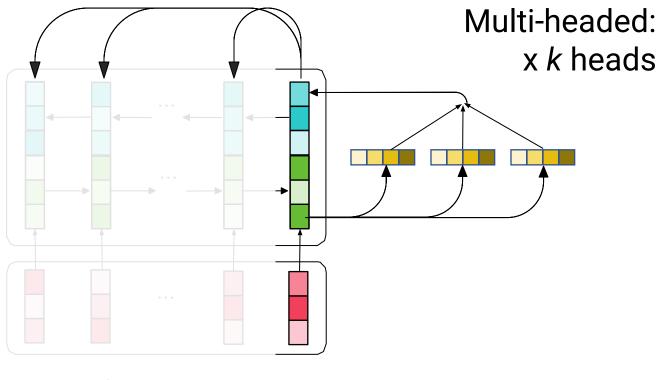
Attention in Transformers





Attention in Transformers Self-attention: x n input tokens groups

Attention in Transformers



No Significant between groups

Attention in Transformers: Challenges

- Sheer *amount* of attention
 - e.g., 13B LLaMA model: 40 layers x 100 input tokens x 40 heads
 - ~= 160,000 individual attention patterns which could be studied.

Attention in Transformers: Challenges

- Sheer *amount* of attention
 - e.g., 13B LLaMA model: 40 layers x 100 input tokens x 40 heads
 - ~= 160,000 individual attention patterns which could be studied.
- Simplifying approach for BERT:
 - Final-layer attention paid by the [CLS] token to all other tokens (aggregated over heads)

- Can attention be used in Transformers to provide heatmap based explanation?
 - Token Identifiability, Adversarial Attention Distributions, Effective Attention, Attention Flows
- Do all attention distributions in transformers really matter?
 - Ablation & Pruning
- What can attention tell us about the global mechanisms used by Transformer models?
 - Linguistic Subtasks, Copying Behavior, Factual Knowledge, Token Identifiability

1. Token Identifiability

• On Identifiability in Transformers (Brunner et al. 2020)

2. Adversarial attention distributions exist for BERT

• Learning to Deceive with Attention-Based Explanations (Pruthi et al. 2020)

3. Modifications to attention scores to improve their interpretability:

Effective Attention

- On Identifiability in Transformers (Brunner et al. 2020)
- Effective Attention Sheds Light On Interpretability (Sun & Marasović 2021)

Attention Flows

- *Quantifying Attention Flow in Transformers* (Abnar & Zuidema 2020)
- Attention Flows are Shapley Value Explanations (Ethayarajh & Jurafsky 2021)

4. Ablation + Pruning of heads: possible

- Analyzing Multi-Head Self-Attention: Specialized Heads Do the Heavy Lifting, the Rest Can Be Pruned (Voita et al. 2019)
- Are Sixteen Heads Really Better than One? (Michel et al. 2019)
- Revealing the Dark Secrets of BERT (Kovaleva et al. 2019)
- Self-Attention Attribution: Interpreting Information Interactions Inside Transformer (Hao et al. 2021)

5. Specialization of attention heads to linguistic subtasks (e.g., syntax/PoS/coreference).

- Analyzing the Structure of Attention in a Transformer Language Model (Vig & Belinkov 2019)
- What Does BERT Look At? An Analysis of BERT's Attention (Clark et al. 2019)
- Analyzing Multi-Head Self-Attention: Specialized Heads Do the Heavy Lifting, the Rest Can Be Pruned (Voita et al. 2019)
- Attention is Not Only a Weight: Analyzing Transformers with Vector Norms (Kobayashi et al. 2020)

6. Attention promotes copying behavior

- A Mathematical Framework for Transformer Circuits (Elhage et al. 2021)
- In-context Learning and Induction Heads (Olsson et al. 2022)
- Locating and editing factual associations in GPT (Meng et al. 2022)

- 7. Attention on key entities can predict model correctness
 - Attention Satisfies: A Constraint-Satisfaction Lens on Factual Errors of Language Models (Yuksekgonul et al. 2023)

Current & Future Relevance: Community-Level Shifts

1. Types of tasks we care about

2. Generality of behavior we want to explain

Current & Future Relevance: Community-Level Shifts

1. Types of tasks we care about

In group A, lower peak (median) plasma levels of procalcitonin (0.2 versus 1.4, p < 0.001), IL 8 (5.6 versus 94.8, p < 0.001), IL 10 (47.2 versus 209.7, p = 0.001), endothelial leukocyte adhesion molecule-1 (88.5 versus 130.6, p = 0.033), intercellular adhesion molecule-1 (806.7 versus 1,375.7, P = 0.001) and troponin-I (0.22 versus 0.66, p = 0.018) were found. There was no significant difference in IL 6, IL-6r and C-reactive protein values between groups. Higher figures of the cardiac index (p = 0.010) along with reduced systemic vascular resistance (p = 0.005) were noted in group A.

 Attention is no longer very useful for instance-level explanations

Did Aristotle use a laptop?

StrategyQA

```
The following are multiple choice questions
about high school mathematics.
How many numbers are in the list 25, 26, ..., 100?
(A) 75 (B) 76 (C) 22 (D) 23
Answer: B
Compute i + i^2 + i^3 + \dots + i^{258} + i^{259}.
(A) -1 (B) 1 (C) i (D) -i
Answer: A
MMI U
```



Current & Future Relevance: Community-Level Shifts

- 2. Generality of behavior we want to explain
- Our focus: providing **instance-level explanations** of model behavior
- Current focus: understanding the **mechanisms** underlying general-purpose Transformers
 - Beyond specific models, datasets and even architectures, tasks
 - \circ <u>Understanding attention is still important</u> \bigstar

Attention is still important

Is Attention All You Need?



Current Status: Yes Time Remaining: 1122d 2h 59m 27s

Proposition:

On January 1, 2027, a Transformer-like model will continue to hold the state-of-the-art position in most benchmarked tasks in natural language processing.

For the Motion

Jonathan Frankle @jefrankle Harvard Professor Chief Scientist Mosaic ML



Against the Motion

Sasha Rush @srush_nlp Cornell Professor Research Scientist Hugging Face 😫



isattentionallyouneed.com

Thank you!



@successar_nlp, sarahwiegreffe
{successar, wiegreffesarah}@gmail.com





