Interpreting Hidden Representations

Notation Borrowed from (Chughtai et al. 2024)

The function a standard transformer with L layers and parameters θ implements f_{θ} can be expressed $f_{\theta}(x_{\leq t}) = \operatorname{softmax}(\pi_t(x_{\leq t}))$ where π_t is a vecotr of logits given by

$$egin{aligned} \pi_t &= \operatorname{LayerNorm}(z_t^L) W_U \ z_t^l &= z_t^{l-1} + a_t^l + m_t^l \ a_t^l &= \operatorname{Attn}(z_t^{l-1}) \ m_t^l &= \operatorname{MLP}(z_t^{l-1}), \end{aligned}$$

Logit Lens

$$\tilde{\pi}_t^l = \operatorname{LayerNorm}(z_t^l) W_U$$
 with $l \leq L$.

text: top 1 guess

color: logit of top 1 guess

	(m):	(*). M.	. wain	.હે	d's	3	ø	æ):	, si	. zuč
h_out -		'we'	' show'	' a'	'AN'	' models'	'based'	y.	' a'	. N.
h46_out -	9	' we'	' show'	' a'	'AN'	9	T	77	' a'	' N'
h44_out -	7	' we'	' show'	' a'	'BM'	' models'	'based'	' models'	' a'	' N'
h42_out -	7	' we'	' show'	' a'	'rams'	' models'	'based'	' models'	' a'	' algorithm'
h40_out -	7	' we'	demonstrate	' a'	' machine'	' models'	'based'	' models'	' a'	' algorithm'
h38_out -	' we'	'we'	demonstrate	' 'neural'	'rap'	' models'	'based'	' models'	' a'	' algorithm'
h36_out -	' we'	' we'	demonstrate	' 'neural'	'rap'	' models'	'based'	' models'	' a'	' algorithm'
h34_out -	' we'	'we'	demonstrate	' models'	'rap'	' model'	'based'	' models'	' a'	' algorith'
h32_out -	' we'	' we'	' simulated'	' models'	'rap'	' model'	'based'	' models'	' a'	' adaptive'
h30_out -	' targeted'	'we'	' found'	'a'	'rap'	9	'based'	**	' which'	' hybrid'
h28_out -	' targeted'	' we'	' found'	' a'	'FP'	'Ms'	'based'	'rd'	' which'	' ambitious'
h26_out -	' targeted'	' we'	' found'	' naïve'	'FP'	'Ms'	'based'	'rd'	' which'	' ambitious'
h24_out	' targeted'	' we'	' found'	' algorithms'	'FP'	's'	'based'	'rd'	' which'	' widely'
h22_out -	' targeted'	' we'	' found'	' camp'	'FP'	's'	'based'	'rd'	' which'	' widely'
h20_out -	' targeted'	' although'	' found'	' algorithm'	'FP'	'ouch'	'based'	'rd'	,000,	' single'
h18_out	' targeted'	' although'	' focus'	' camp'	'AP'	'ouch'	'based'	'rd'	'000'	' single'
h16_out -	' targeted'	' unlike'	' focus'	' camp'	'MP'	'IME'	'based'	'rd'	,000,	' single'
h14_out	' targeted'	' note'	' target'	' camp'	'MS'	'IME'	'based'	'rd'	'000'	' single'
h12_out -	' target'	' unlike'	' hope'	' split'	'MP'	'ouch'	'based'	'rd'	,000,	' massive'
h10_out -	' updated'	' however'	"'d"	' session'	'iott'	'IME'	'style'	'rd'	'000'	' massive'
h8_out -	' target'	' however'	' target'	' evaluation'	'rom'	'IME'	'based'	'rd'	'000'	' enormous'
h6_out -	' focused'	' however'	"'d"	'ees'	'rou'	'ools'	'based'	'rd'	' which'	' enormous'
h4_out -	' target'	' however'	' can'	'ees'	'rou'	'ools'	'sided'	'rd'	' and'	' enormous'
h2_out -	' guid'	' and'	' Hardy'	'ees'	'rou'	'ools'	'based'	'rd'	' and'	' enormous'
h0_out -	'chini'	' and'	"'d"	' train'	'rou'	'ools'	'based'	'rd'	' and'	' isolated'
G _R ect	itcally	٠, ٔ	, we	Main	્હે '	d.	\$	·Š	٠, '	. ori

ranks of final top-1 prediction

(not ground truth)

	(*);	(*). Mg	Hairi	, Ġ	d.	.5	ò	(*);	, ari	aut
h_out -	1	1	1	1	1	1	1	1	1	1
h46_out	1	1	1	1	1	2	2	1	1	1
h44_out -	1	1	1	1	2	1	1	2	1	1
h42_out -	1	1	1	1	6	1	1	8	1	7
h40_out -	1	1	2	1	44	1	1	4	1	10
h38_out -	2	1	2	3	97	1	1	13	1	10
h36_out -	2	1	3	4	137	1	1	45	1	16
h34_out -	2	1	7	4	328	2	1	67	1	39
h32_out -	2	1	13	3	580	2	1	48	1	87
h30_out -	6	1	15	1	610	5	1	69	2	147
h28_out -	6	1	16	1	642	4	1	66	3	125
h26_out -	11	1	53	2	596	10	1	101	12	78
h24_out	18	1	36	6	917	14	1	80	13	75
h22_out -	46	1	44	4	926	40	1	114	24	150
h20_out -	132	3	145	5	847	64	1	208	61	368
h18_out -	42	3	97	10	789	67	1	296	52	313
h16_out -	85	3	140	11	1220	146	1	176	89	269
h14_out	115	6	424	20	1243	172	1	170	102	143
h12_out -	187	12	1281	56	1985	322	1	391	89	167
h10_out -	413	11	994	162	1819	493	2	213	139	164
h8_out -	420	10	2338	213	1886	942	1	250	98	77
h6_out -	994	7	4644	683	1660	1381	1	348	130	43
h4_out -	1840	17	6128	1926	2547	2014	2	100	79	29
h2_out -	1587	83	14270	1407	1000	1822	1	95	43	31
h0_out -	20608	321	7807	4768	773	9399	1	486	105	59
Specifically : we rain . G pr .: 3 : an										

Copy rare token

	, Other	(*) till	es (*):	when	(*). Pe	ople (*) sa	4 (*) plast
h_out -	' Plasma'	' times'	, v	' they'	' people'	' say'	' plasma'
h46_out -	' But'	' times'	25	' they'	' people'	' say'	1.00
h44_out -	' Plasma'	' times'	35	' they'	' people'	' say'	' plasma'
h42_out -	' Plasma'	' times'	25	' they'	' people'	' say'	' plasma'
h40_out -	' Plasma'	' times'	25	' they'	' people'	' say'	' plasma'
h38_out -	' Plasma'	' times'	' they'	' they'	' people'	' say'	' plasma'
h36_out -	' But'	' times'	' they'	' they'	' people'	' say'	' plasma'
h34_out -	' But'	' times'	' they'	' they'	' people'	' say'	' electron'
h32_out -	' But'	' times'	' they'	' they'	' people'	' say'	
h30_out -	' But'	' times'	' they'	' they'	' people'	' say'	1.00
h28_out -	' But'	'worldly'	' they'	' referring'	' people'	' say'	
h26_out -	' But'	'worldly'	' they'	' they'	' people'	' say'	1.00
h24_out	' But'	'worldly'	' vague'	' however'	' pressed'	' talk'	
h22_out -	' But'	'worldly'	' confused'	' however'	' pressed'	' want'	
h20_out -	' But'	'worldly'	' confused'	' perhaps'	' they'	' revol'	

Tuned Lens

representational drift:

features may be represented differently at different layers of the network.

Learn some affine transformations that "translate" representations from the basis used at one layer of the network to the basis expected at the final layer.

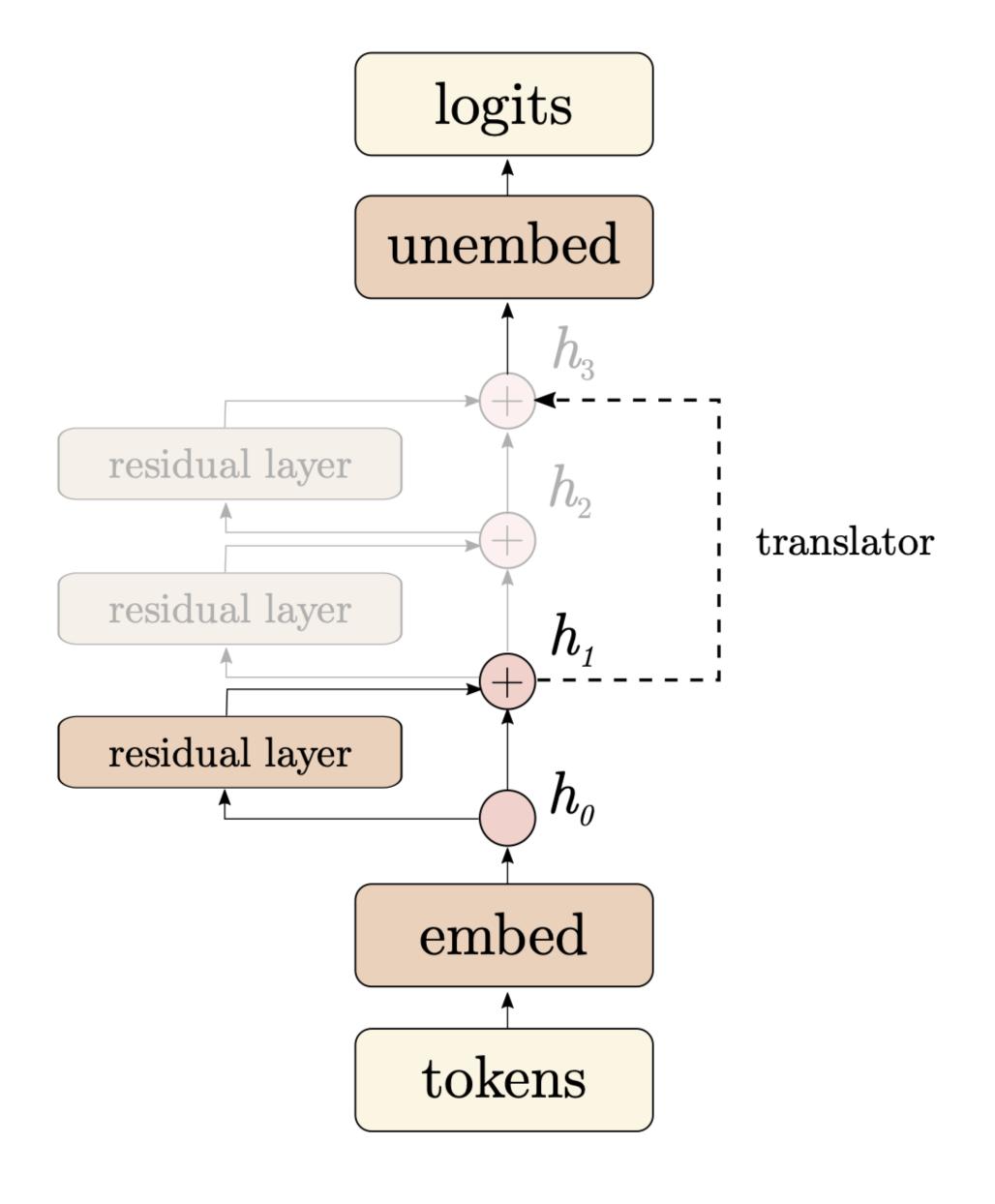


Figure 2 in (Belrose et al, 2023)

TunedLens_{$$\ell$$}(h_{ℓ}) = LogitLens($A_{\ell}h_{\ell} + \mathbf{b}_{\ell}$)

$$\operatorname{argmin} \ \mathbb{E} \left[D_{KL}(f_{>\ell}(\boldsymbol{h}_{\ell}) \,|| \, \operatorname{TunedLens}_k(\boldsymbol{h}_{\ell})) \right]$$

Logit Lens (theirs) model recurrent architecture that called attention former output model yet called attention former 30 that that model model 27 called ** that that model model called called called ** 24 â̦." â̦." model model that that called â̦." â̦." â̦." â̦." â̦." â̦." â̦." â̦." 18 â̦." â̦." â̦." â̦." â̦." â̦." â̦." â̦." 15 â̦." â̦." 12 â̦." 11 п п input architecture simple network the Trans former new Layer Tuned Lens (ours) attention model recurrent architecture that called former output model model architecture that called attention former 30 27 model model that that called ** model model that ** 24 that called 21 model model that that the âĢ 18 model model that the that SO 15 method method that that which SO 12 method that that which SO that which and and for result to and a and to Х same input simple architecture Trans former network new Input token

0.4

8.0

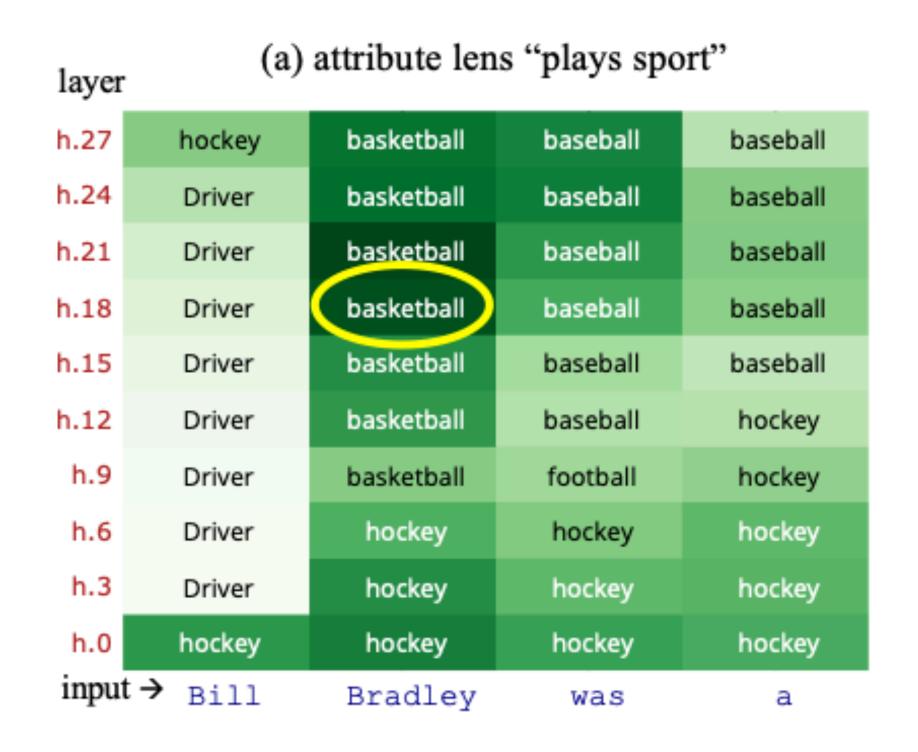
0.6

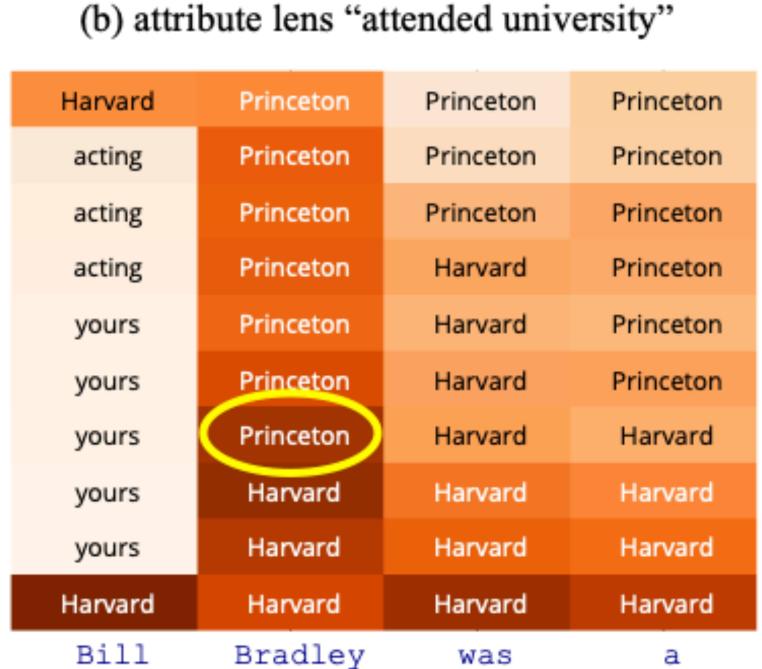
Probability

0.2

Figure 1 in (Belrose et al, 2023)

Attribute Lens





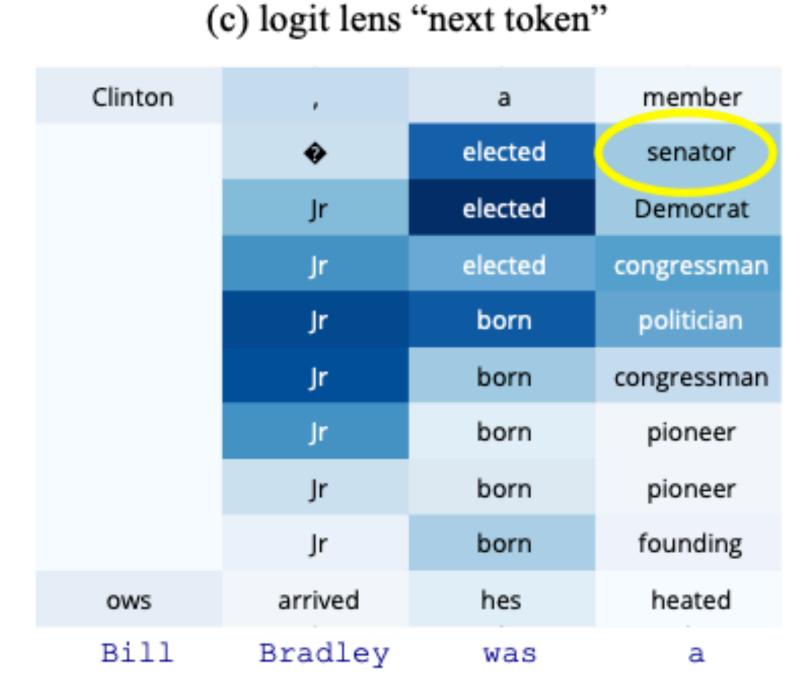


Figure 8 Hernandez et al, 2024

Notation Borrowed from (Chughtai et al. 2024)

The function a standard transformer with L layers and parameters θ implements f_{θ} can be expressed $f_{\theta}(x_{\leq t}) = \operatorname{softmax}(\pi_t(x_{\leq t}))$ where π_t is a vecotr of logits given by

$$egin{aligned} \pi_t &= \operatorname{LayerNorm}(z_t^L) W_U \ z_t^l &= z_t^{l-1} + a_t^l + m_t^l \ a_t^l &= \operatorname{Attn}(z_t^{l-1}) \ m_t^l &= \operatorname{MLP}(z_t^{l-1}), \end{aligned}$$

Logit Lens

$$\tilde{\pi}_t^l = \text{LayerNorm}(z_t^l) W_U$$
 with $l \leq L$.

Direct Logit Attribution (DLA)

Different types of DLA

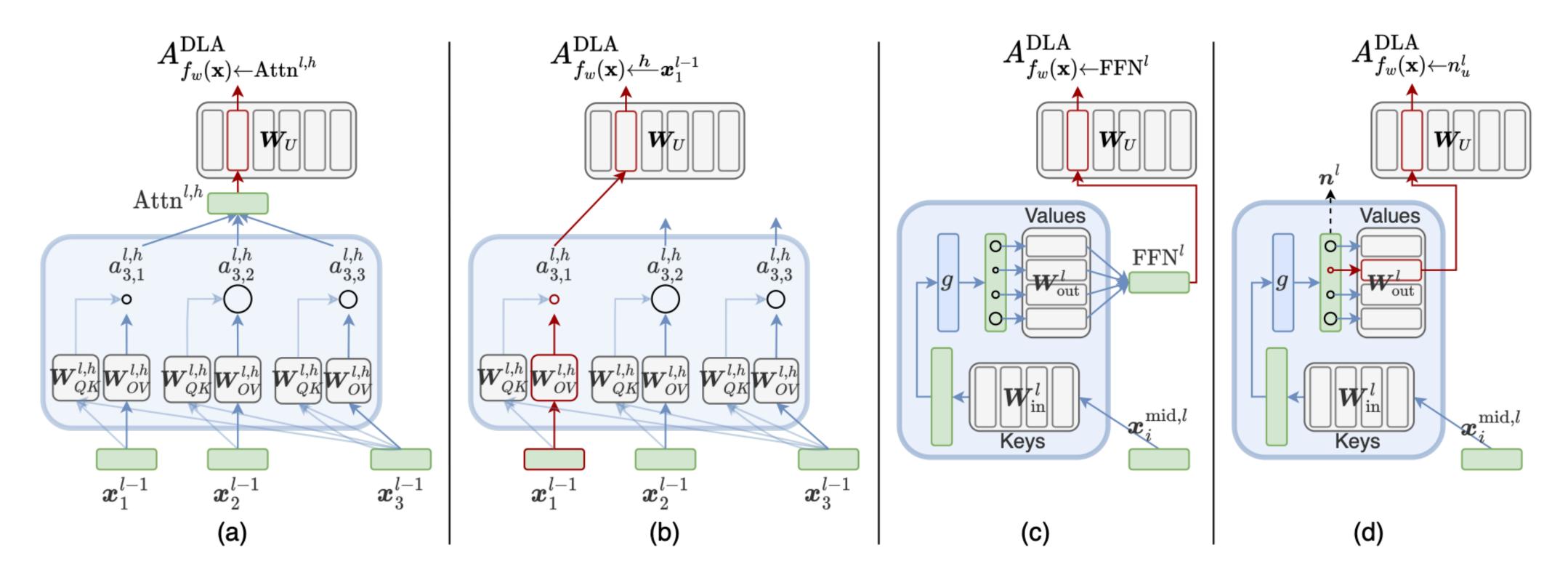


Figure 5: Direct Logit Attributions (DLA) on output token w. (a) DLA of an attention head Attn^{l,h}, (b) DLA of an intermediate representation x_1^{l-1} via an attention head, (c) DLA of an FFN block, and (d) DLA of a single neuron.

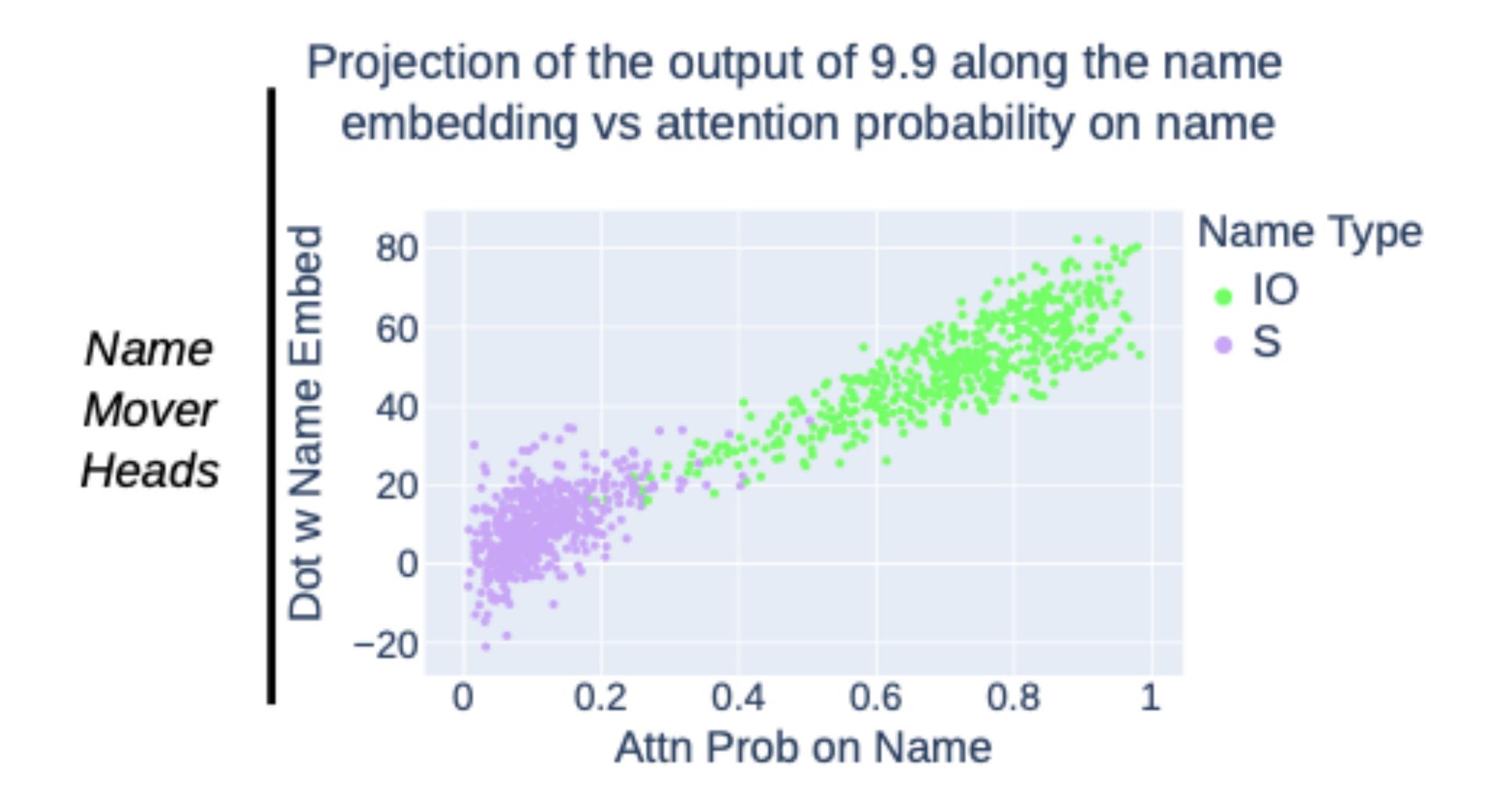


Figure 3(c) from Wang et al, 2022

Patchscopes

Step 1: Feeding Source Prompt to Source Model

Step 2: Transforming Hidden State

Step 3: Feeding Target Prompt to Target Model

Step 4: Running Execution on Patched Target

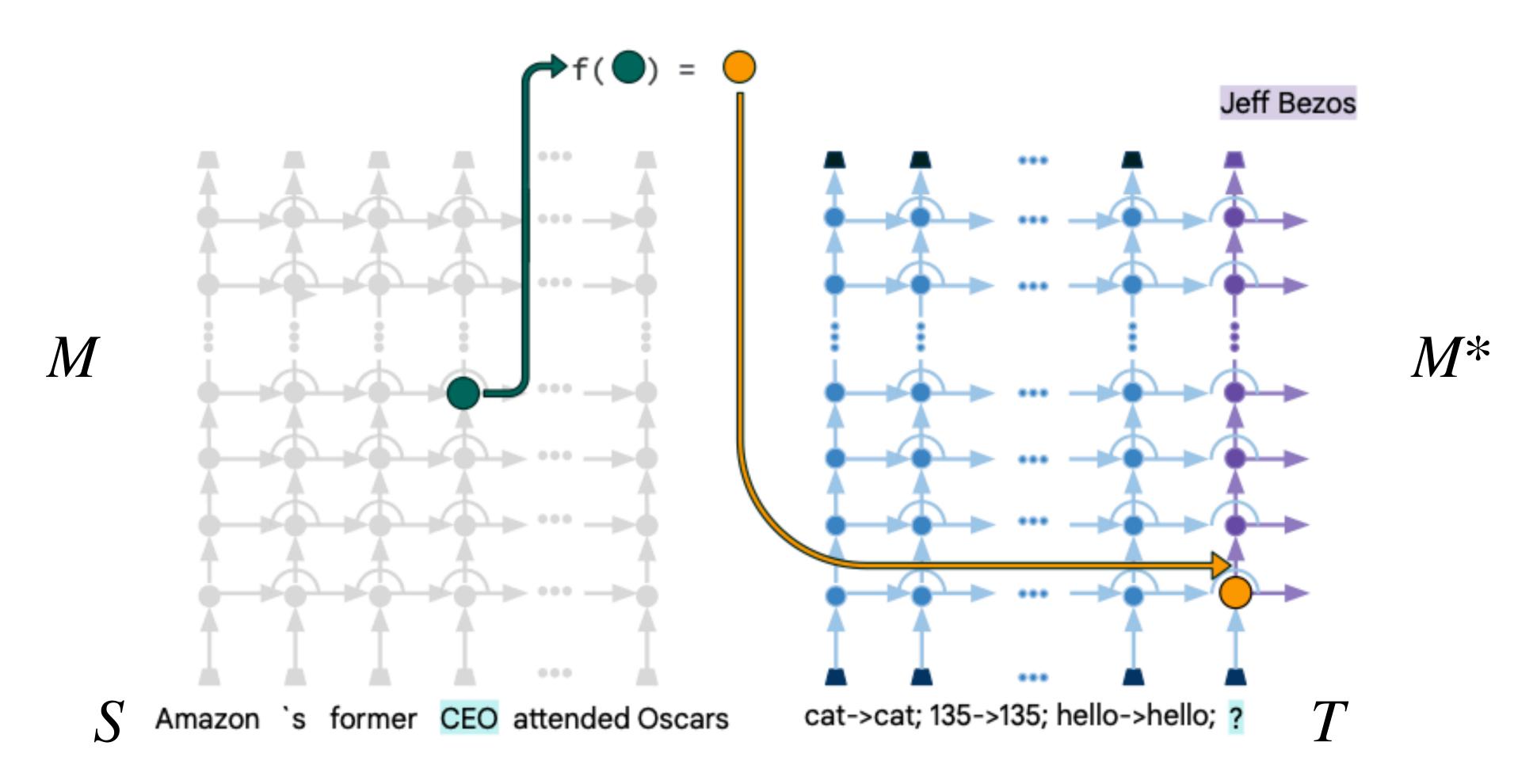


Figure 1 from Gandeharioun et al, 2024

 $(S, i, M, l), (T, i^*, f, M^*, l^*)$

Entity resolution

to and how that relates to the tokens processed. $\mathcal{M}^* = \mathcal{M} \leftarrow \text{Vicuna (13B)}, \ \ell^* = \ell, S \leftarrow \text{"Diana, Princess of Wales"}.$

l	Generation	Explanation
1-2	: Country in the United Kingdom	Wales
3	: Country in Europe	Wales
4	: Title held by female sovereigns in their own right or by queens consort	Princess of Wales (unspecific)
5	: Title given to the wife of the Prince of Wales (and later King)	Princess of Wales (unspecific)
6	: Diana, Princess of Wales (1961-1997), the first wife of Prince Charles, Prince of Wales, who was famous for her beauty and humanitarian work	Diana, Princess of Wales

I am wondering why KL divergence isn't a good metric to calculate distance between intermediate and final probability distribution?

Could we use simply mean squared error? What about the dot product?

I find it very interesting that the way layers in a transformer work is that they essentially take one embedding and transform it into another and those two vectors would come from the same "language" (that is, if you use the W matrix, you would get the first token at the bottom and the next token at the top).

Have there been studies or attempts to make those two vectors belong to completely different categories, so that there would be "current token" and "next token" embeddings.

I was also wondering if this is directly related to the issue of GPT-2 often repeating the same sequence of tokens over and over. Is the problem that is sometimes simply not enough layers?

Do you think it makes sense to project the activations using the same unembedding weights?

What happens if we retrained the unembedding matrix to generate the next word from the activations wouldn't that give a better idea of the info in a certain layer?

The authors claim the logit lens technique provides intuitive insights into intermediate layer activations. However, could the observed phenomena be explained by simpler statistical artifacts rather than genuine model behavior? What additional experiments could validate the robustness of the logit lens findings?

The study indicates that the model discards input tokens quickly. Could this be a sign of a potential issue with how transformers manage long-range dependencies? How might this affect the model's performance on tasks requiring detailed contextual understanding, such as coreference resolution or summarization?

Questions about Patchscope

So in experiment 4.1 and 4.2, Patchscopes has an unfair headstart compared to the baselines, and reporting that "its performance is higher" I see as deception. Do I miss something here?

Questions about Patchscope

The most interesting finding to me was when the model being used to interpret patching has more parameters, cross-model patching works really well.

Am I overestimating how important this specific result about cross-modal patching is, or do you think it's just a cool result but has fairly little practical implications?

Questions

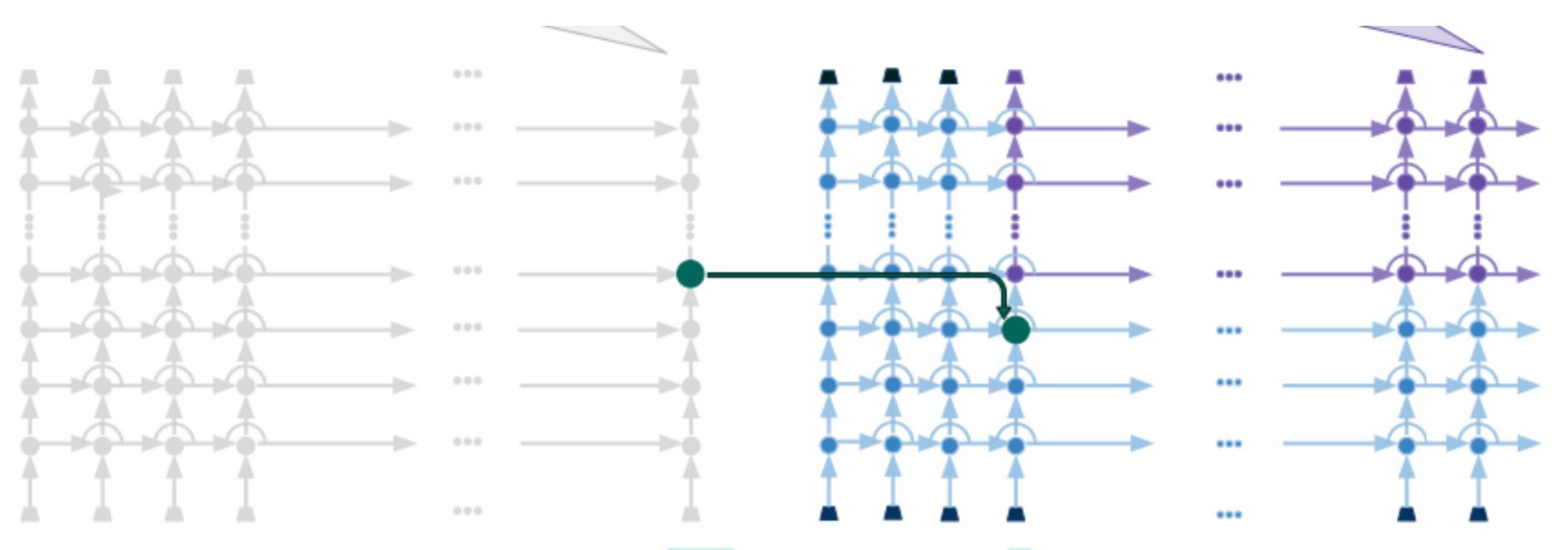
It seems that patching into the later layers seems to perform better than patching into earlier layers. Could this indicate that a significant amount of transformations are necessary to extract the information from the embedding?

If many transformations are required, it is probably hard to manipulate the embedding to change model predictions. Could a probe work nonetheless, similar to how it was done in the Othello paper? I believe the kind of adversarial training the Othello paper did is hard to do on a full GPT model.

Questions

- I have a hard time believing that just because intermediate representations make some sense in vocabulary space when decoded using (last embed-> vocab) codebook, it's a right thing or a sensible thing to do.
 - 1. Also, I think the "logit lens" is just a codebook for the final representation, and so any conclusion by using it on an intermediate representation doesn't guarantee anything. Just a correlation. Am I right in saying that?
 - 1. It's as if saying that, with time a language changed, eg. A->B->C->D-> English, and you're comparing a sentence in A/D and English, saying that it makes sense for D but not A.
 - 2. It's not true, because you're using the wrong codebook. The information is there though, you just need to extract it right.

And for patchscopes, I have a similar doubt as above. Assuming that it makes sense, can you please elaborate on how chain-of-thought patchscopes work exactly?



The current CEO of the company that created Visual Basic Script

The current CEO of the company that created Visual Basic Script

Figure 4. An illustration of CoT Patchscope on a single example. In this example, $\pi_1 \leftarrow$ "the company that created Visual Basic Script", $\pi_2 \leftarrow$ "The current CEO of", $S = T \leftarrow [\pi_2][\pi_1] =$ "The current CEO of the company that created Visual Basic Script". Note that $\mathcal{M} = \mathcal{M}^*$ and $f \leftarrow \mathbb{I}$.

Questions about Tuned Lens

About iterative inference:

they make a point that transformers iteratively refine their representations in the direction of the output, slowly changing the representations at each layer in the anti-gradient direction. I am wondering how this is related to the fact that there are circuits in the models, and there are attention heads that can do very interpretable updates (not necessarily moving representations in the direction of the output), or store something in the residual stream (also not necessarily moving the representations in the right direction). Is it just two complementary mechanisms?

Alignment of residuals with gradients (Pythia 6.7B)

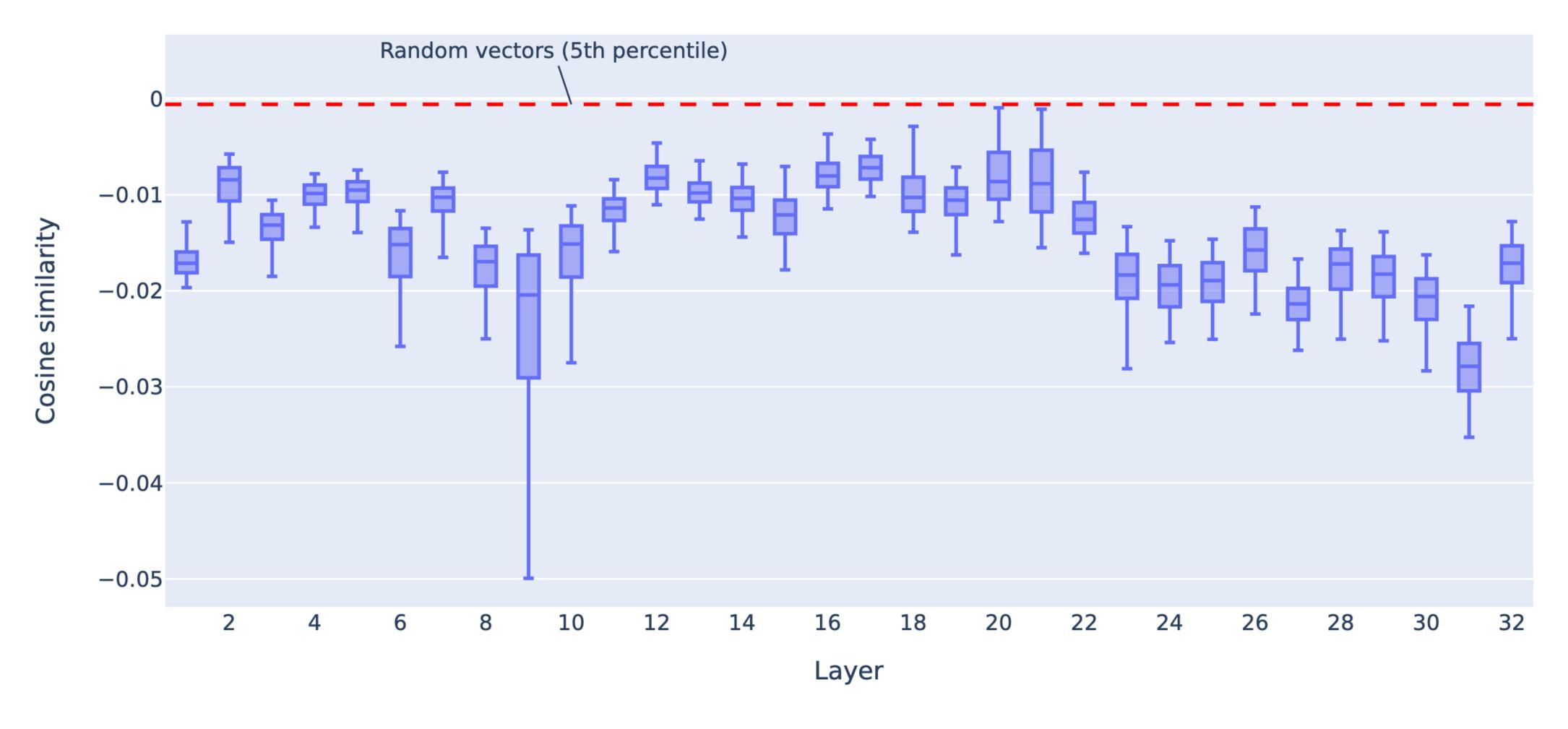


Figure 19 from (Belrose et al, 2023)

Questions about Tuned Lens

About representational drift:

The authors say that the covariance between the representations in close layers in quite high and for further layers it is quite low, and they use this motivation to introduce a change of basis matrix into the Tuned Lens formula. I did not understand, how the fact that the covariance between matrices is low implies that the matrices are represented in different bases, and not that they just have different information stored in them.