Mechanistic Interpretability: Self-conditioning

Zhaokun Wang(HS) Master students of Computational Linguistics

Contents: 2 papers

1.Self-conditioning Pre-Trained Language Models

2.On the Multilingual Ability of Decoder-based Pretrained Language Models: Finding and Controlling Language-Specific Neurons

1.Figures and tables keep the same number in each paper ²

Contents of Paper 1

Introduction

•**Transformers** introduced in 2017 revolutionized NLP. •**BERT** and **GPT-2** became popular around **2019**. •Earlier work explored **Finding Experts in Transformer Models**.

Inspiration from Previous Work

Inspiration from Images:

Neurons capture visual concepts like **"trees"** or **"dogs"** (Bau et al., 2017).

In Text:

Sentiment neurons in LSTMs detect emotions like **happiness** or **sadness** (Radford et al., 2017).

TLMs' Pros and Cons

Pros

• Mastery of diverse tasks (text generation, summarization).

Cons

- Mechanism unknown
- Lack control over output.
- Biases inherited from training data.

FIND MECHANISM CONDITIONED TEXT GENERATION

Concepts as binary sentence datasets

Structure: **Concept c: Described by sentences labeled as:**

Contains c: Positive examples. Does not contain c: Negative examples.

Primary Dataset: OneSec (from Wikipedia, annotated with WordNet senses).

WordNet Label Format: lemma%ss:pp:pos:src

lemma: Base form (e.g., "bird"). **ss**: Sense number (e.g., "1"). **pp**: Semantic category ID (e.g., "05" for animal). **pos**: Part of speech (e.g., "n" for noun). **src**: Annotation source (manual/automatic).

Flexible Representation:

Broad (*sport*), precise (*football*), or abstract (sentiment). Distinguish homographs (*note*: "reminder" vs "tone").

Method overview

Goal: Control concept presence in text generation.

Key Idea:

Use **internal expert units** in TLMs for self-conditioning. No need for external models, fine-tuning, or additional parameters.

Steps:

Identify expert units. Intervene to simulate concept presence. Adjust intervention strength k to control concept intensity.

Generative Mechanism

•**Language Model**: Autoregressive generation:

$$
p(x) = \prod_{t=1}^{T} p(x_t | x_{< t})
$$

•**Conditioned Generation**:

 $p(x | y = c) \propto p(y = c | x) p(x)$ $\cdot p(y = c | x)$: Conditional probability (concept presence).

 $\cdot p(x)$: Ensures text remains natural.

•Hypothesis: TLMs internally model $p(y = c | x)$ naturally.

Selfconditioning method

Expert Units: Neurons contributing to $p(y = c | x)$. **Expertise Measurement**: Rank units using **Average Precision (AP)**.

Steps:

Identify expert units for a concept. Apply do(c, k): Set top-k units to simulate concept presence.

Adjust k to control concept intensity.

Other methods

FUDGE (Future Discriminator Guidance)

Core Idea: Uses a lightweight **external discriminator** to guide generation dynamically.

Process:

Trains a discriminator to predict if text will meet target conditions. Adjusts token probabilities based on discriminator scores.

PPLM-BoW (Plug and Play Language Model)

Core Idea: Modifies TLM's hidden states to push generation toward a target concept. **Process:**

Defines target concepts via a **Bag of Words (BoW).**

Optimizes hidden states using gradient updates during inference.

AP Definition

Precision-Recall Curve:

Precision: Correct positive predictions. Recall: Identified actual positives.

AP Definition:

Area under the Precision-Recall Curve. $AP \in [0,1]$: Higher AP = better predictor.

Use in Method:

Rank expert units by AP to identify top contributors to a concept.

Assist Figure 1: Precision and recall formular

Assist Figure 2: An example of PR Curve ¹⁵

Experiments analysis

Experimental Analysis Overview

Analysis 1: Concept Control

•**Goal**: Control text generation using **expert units**.

•**Method**:

•Apply do(c,k) to intervene on k-top expert units.

•Use WordNet concepts (e.g., bird%1:05:00).

1.Increasing k for bird%1:05:00.

Table 1: Generated sentences using GPT2-L with context Once upon a time

•Concept presence increases with k.

•At k=200, repetition occurs saturation.

•Few expert units (0.048%) can control text generation.

2.Condition text on elevator%1:06:00 and frustration%1:12:00

Table 2: Generated sentences using GPT2-L with the context used by OpenAI for 2 different concepts.

•Text remains coherent.

•Concepts are integrated.

3.Test homograph concepts lead

•Correct meaning controlled by context.

Analysis 2: Bias Mitigation

- **Goal**: Achieve gender parity in text generation.
- **Methods**:
	- **Ours**: Top-k expert units.
	- **FUDGE**: External classifier (λ).
	- **PPLM-BoW**: Gradient steps.
- **Metrics**:
	- **Δp(c,*)**: Probability difference.
	- **Perplexity**: Text naturalness.

Example Text at Parity Points

Context "The nurse said that" + $do(man, 30)$

The nurse said that he was not in the mood. The nurse said that he had not been given any instructions... *The nurse said that* he felt that she was too old... *The nurse said that* he could not understand what was happening... *The nurse said that* he had to leave the room...

Context "The warrior desired that" + $do(woman, 30)$

The warrior desired that she could be with her lover... The warrior desired that she be seen, so she was sent on the hunt... The warrior desired that she had the courage and strength... The warrior desired that she may be able to bear children... The warrior desired that she should be able to walk around...

Table 4: Sentences generated at the generative parity points that continue "The nurse said that" with he and "The warrior desired that" with she.

Experiment: Generate sentences at parity for biased contexts.

"The nurse said that" → **man**.

"The warrior desired that" → **woman**.

1. Compare perplexity when achieving gender parity in text generation.

Figure 1: Perplexity (the lower the better) at parity points with our method (top) and FUDGE (bottom). $\sqrt{24}$

- Our method achieves parity at lower perplexity (∼69.5) than FUDGE ∼85.4∼85.4) and PPLM-BoW (>250).
- Our method preserves text naturalness while achieving parity.

2. Parity Point vs. Model Bias

•**Objective**: Investigate the relationship between **model bias** and effort (parity point) needed to achieve balance.

- Strong correlation for our method (r=−0.806r for woman).
- FUDGE and PPLM-BoW show weaker or inconsistent correlation.
- Model bias predicts required intervention strength for our method.

3. The Effect of Strong Conditioning

- Our method maintains diversity at strong parity points.
- FUDGE: Repetition increases (p>0.5).
- PPLM-BoW: High repetition (p>0.9).

Figure 3: Probability of generating woman or man when conditioning on the same concept.

Analysis 3:Differences with FUDGE and PPLM-BoW

Our method: Efficient, diverse, and fine-grained without extra parameters. **FUDGE**: Flexible but requires external components. **PPLM-BoW**: Simple but slow and repetitive.

Analysis 4: Efficiency Comparison

- Objective: Test **Top-30 expert units** for conditioning.
- An exhaustive search for all possible combinations is not feasible.
- Procedure: Intervene on Top-30 experts ranked by **AP,** Moving groups (e.g., 31-60, 61-90), Baseline (no intervention, **k = 0**).
- Contexts:
	- "The nurse said that" \rightarrow **man**
	- "The doctor said that" → **woman**

Experiment 4 Results

Figure 4: Probabilities p(he|do(man, 30)) and p(she|do(woman, 30)) for contexts "The nurse said that" and "The doctor said that" respectively.

> **Top-30 experts** \rightarrow Highest probabilities. **Random subsets** → perform poorly. **Trends**: Probability drops as subsets move away. **Conclusion**: **Top-K strategy works**.

Conclusion

Takeaways

Efficient Control: Uses expert units for precise concept conditioning.

Natural Text: Maintains naturalness with minimal intervention.

Self-contained: No fine-tuning or external models required.

Proven Effective: Works for diverse concepts and biases.

Application of Self-conditioning

TLM Mechanism:

Explains internal generative process. Useful for identifying and mitigating biases in LMs.

Comparison with Alternatives:

Vs. Zero-shot/Few-shot Prompt Engineering. Vs. HFRL (Human Feedback Reinforcement Learning).

Practical Challenges:

Requires identifying expert units for: **Different LM Versions**. **Diverse Concepts**.

A little bit like ...? Intervention and "One Flew Over the Cuckoo's Nest"

Intervention => Adjusting expert units; **Brain surgery** => Altering brain function.

- Over-intervention degrades text quality.
- Risk of unintended model behavior.
- Insight: Precision and minimal disruption are crucial.

Assist Figure 3: A scene from the movie One Flew Over the Cuckoo's Nest

Expert units are more common in **shallow layers** (general concepts) and decrease in **deeper layers** (task-specific representations).

Expert units identified in **GPT-2** (e.g., "gender") map to similar positions in **RoBERTa**, maintaining high AP values and showing cross-model generalization.

1. If the model maximizes $p(x | y=c)$ without ensuring linguistic correctness, could it result in nonsensical or incoherent sentences?

2. With larger models like GPT-3 or GPT-4, would the number of expert units required for intervention remain proportionally small, or would it scale non-linearly with model complexity?

3. Could this approach be extended to detect and mitigate other biases (e.g., racial or agerelated) automatically across diverse contexts, rather than pre-defining specific concepts like "nurse" or "warrior"?

4. Is the smaller number of expert units needed to induce the "man" concept due to an inherent bias favoring men in occupations?

5. How do the authors propose to automate finding the optimal k to achieve parity, as mentioned in section 5.2? **6.** Should the paper have included a structured human evaluation, rather than relying on selected examples?

 \bigcup

More questions?

Paper 2

On the Multilingual Ability of Decoder-based Pretrained Language Models:

Finding and Controlling Language-Specific Neurons

Introduction

1.Multilingual Abilities of PLMs

Explicit: Trained on multilingual data (e.g., XGLM, BLOOM)

Incidental: Emerges from English-dominant data (e.g., Llama2)

Improves cross-lingual tasks (e.g., translation) Reveals **how PLMs handle multiple languages**

Why It Matters Focus: Decoderbased PLMs

> Complex **language-specific recovery**

Behavior of **language-specific neurons** is unknown

1.Method Overview

Objective: Identify and control **language-specific neurons**.

Focus:Transition from **word-level** to **sentence-level** neuron analysis.

Key Models: XGLM, BLOOM, Llama2.

Languages: English, German, French, Spanish, Chinese, Japanese.

2.Procedure

Finding Neurons:

Label texts as target (Positive) or non-target (Negative).

Measure activations using **mean** across tokens.

Identify **Top-k** (positive) and **Bottom-k** (negative) neurons.

Controlling Neurons:

Replace activations with **median values** for the target language.

Apply in **unconditional** and **conditional** text generation.

Figure 1: Overview of our proposal.

3.Key Differences from Prior Methods

Experiments analysis

1.Experiment Setup

BLEU Score:

Measures text quality using **n-gram overlap** with reference text.

•**Tasks**:

1.Finding Language-specific Neurons 2.Unconditional Generation: No input, random sampling.

3.Conditional Generation: Machine translation with ambiguous prompts.

Evaluation:

•**Target Language Probability**.

•**Text Quality** (BLEU Score).

1. Finding Languagespecific Neurons

Goal: Identify neurons activated uniquely for each language.

Method:

Rank neurons by **Average Precision (AP)**. Analyze **Top-k**, **Middle-k**, and **Bottom-k** neurons.

1.1 Distribution Across Model Layers

Figure 2: Neuron Activation Patterns (Top, Middle, Bottom Layers)

Top/Bottom-k Neurons: Concentrated in the **first** and **last layers**. **Middle-k Neurons**: Located in the **middle layers**.

Top and **Bottom layers** contain **language-specific neurons**.

Middle layers focus on **language-agnostic** semantic processing.

1.2 Overlap Across Languages

Overlap between languages: < 5%. Example: German-Spanish (74), French-Japanese (21).

Neurons are highly distinct for each language. Supports language-specific processing in decoder models.

Table 3: Pairwise neuron overlap for six languages (de, en, es, fr, ja, zh).

2.Unconditional Text Generation Setup

Objective:

Assess if neuron intervention controls the output language.

Setup:

Input: [BOS] token (no prompt).

100 generations (random sampling: temperature=0.8, top-p=0.9).

Metrics:

Target Language Probability: Classified using FastText.

Text Quality: Measured using BLEU-4 score.

2.1 Modify specific language neurons with a [BOS] token as input.

Figure 3: Outputs when activating language-specific neurons

2.2 Measured accuracy before and after intervention

Before Intervention: Low probability of target languages.

After Intervention: Top-k: Positive activation \rightarrow Higher probability. Bottom-k: Negative activation \rightarrow Complementary role. Combined: Best results (e.g., German \rightarrow 95%).

Table 4: Target Language Probability

2.3 Neuron Activation Distribution

Figure 5: Neuron Activation Distribution ("on" vs "off")

Ecperiments:

Compared activation values of **language-specific neurons** when target language (French) is active ("on") vs inactive ("off").

Top-k Neurons: Strong positive activation for target languages. **Bottom-k Neurons**: Strong negative activation helps

distinction.

Both **Top** and **Bottom neurons** are critical.

2.4 Ablation Study of Neuron Intervention

1000–10,000 neurons → Optimal balance of accuracy and quality (BLEU). Too many neurons → Text collapses, quality drops.

Optimal control requires a balanced intervention range.

Figure 6: Vary the number of neurons intervened ($log_{10}(k)$).

3.Conditional Text Generation Setup

Objective:

Control target language output in **machine translation tasks.**

Setup:

Input: Ambiguous prompt ("Translate into a target language"). Evaluation: Accuracy (language occurrence) and BLEU (translation quality).

3.1 Model Generated Examples

Setup: Ambiguous prompt + neuron intervention.

No Intervention: Default language output (English). **With Intervention**: Model successfully generates target language text (German, French, etc.).

Neuron intervention effectively controls output language.

Figure 4: Translation Results with Neuron Intervention.

3.2 Conditional Generation Results

Llama2 achieves significant improvements in both **Accuracy** and **BLEU**.

BLOOM and XGLM show **limited improvements**, especially on BLEU scores.

Conclusion:

Llama2 produces correct translations; others struggle with coherence.

Table 5: Translation Accuracy and BLEU scores across tasks.

3.3 Effect of Prompts (Ambiguous & Explicit)

Ambiguous prompts benefit most from **neuron intervention**.

Explicit prompts: Already activate target language neurons \rightarrow minimal improvement.

Table 6: Translation tasks with different prompt settings

Conclusion

Conclusion

Language-Specific Neurons exist in first and last layers of decoder-based PLMs.

Neuron Intervention controls target language generation.

Future Work: Model compression and fine-tuning for unseen languages.

Limitations: Focus on open models and six languages

Reference

- **Paper 1:** Suau X, Zappella L, Apostoloff N. Self-conditioning pre-trained language models[J]. arXiv preprint arXiv:2110.02802, 2021.
- **Paper 2:** Kojima T, Okimura I, Iwasawa Y, et al. On the Multilingual Ability of Decoder-based Pre-trained Language Models: Finding and Controlling Language-Specific Neurons[J]. arXiv preprint arXiv:2404.02431, 2024.
- **Paper 3:** Suau X, Zappella L, Apostoloff N. Finding experts in transformer models[J]. arXiv preprint arXiv:2005.07647, 2020.
- **PR Formular:** (Aqeel Anwar), "What is Average Precision in Object Detection / Localization Algorithms and How to Calculate it?," *Towards Data Science*, (May 13, 2022). [Online]. Available: https://towardsdatascience.com/what-isaverage-precision-in-object-detection-localization-algorithms-and-how-to-calculate-it-3f330efe697b
- **PR Curve Figure:** (Nisha Arya Ahmed), "Mean Average Precision (mAP): A complete guide," *Kili Technology*, (Time unknown). [Online]. Available: [https://kili-technology.com/data-labeling/machine-learning/mean-average-precision-map](https://kili-technology.com/data-labeling/machine-learning/mean-average-precision-map-a-complete-guide)[a-complete-guide](https://kili-technology.com/data-labeling/machine-learning/mean-average-precision-map-a-complete-guide)
- **Movie Picture:** Film Festival Cologne, "FFCGN On-Demand in September" (Original: FFCGN On-Demand im September), (Time unknown). [Online]. Available: <https://filmfestival.cologne/artikel/ffcgn-on-demand-im-september>
- Unicorn picture are generated by Gemini.

Q&A

