

# Outliers and Hallucinations: Contributions to Robust Community Detection and Language Model Alignment

**Leonardo Martins Bianco**

*Supervisors:*

**Christine Keribin** (Université Paris-Saclay, LMO)

**Zacharie Naulet** (Université Paris-Saclay, INRAE)

**Jessica Hoffmann** (Google DeepMind)

December 4, 2025

# Thesis progress



# Thesis progress



# Thesis progress



# Thesis progress



# Overview

## Part I: Contributions to Robust Community Detection

Robust Estimation for the SBM

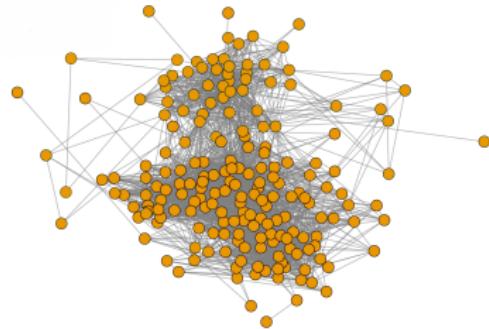
## Part II: Contributions to Language Model Alignment

Decoding-time Realignment of Language Models

Reducing Hallucinations with Synthetic Hallucinations

# Motivation

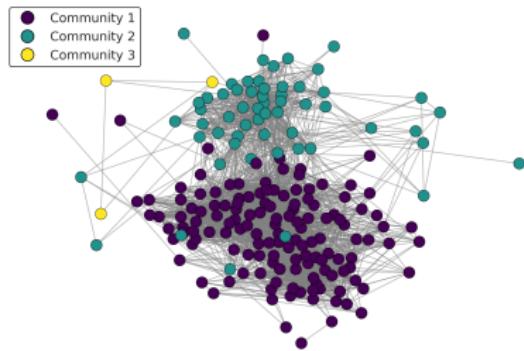
- ❖ *Adjacency matrix:*  
symmetric  $A \in \{0, 1\}^{n \times n}$



Jazz collaborations in New York, Chicago,  
and elsewhere [2]

# Motivation

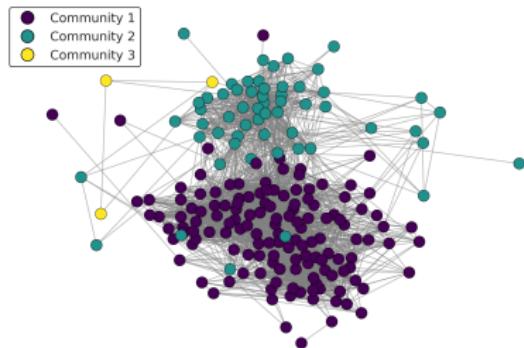
- ❖ *Adjacency matrix:*  
symmetric  $A \in \{0, 1\}^{n \times n}$
- ❖ *Community detection [1]:*  
group similar nodes,  
sensitive to *outliers*



Clustering of the Jazz collaborations

# Motivation

- ❖ *Adjacency matrix:* symmetric  $A \in \{0, 1\}^{n \times n}$
- ❖ *Community detection* [1]: group similar nodes, sensitive to *outliers*
- ❖ *Robust algorithm:* accurate results despite outliers



Clustering of the Jazz collaborations

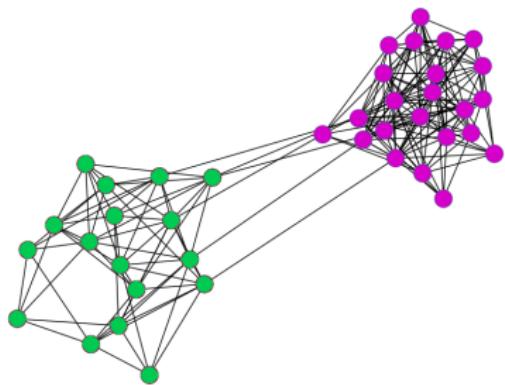
# The Stochastic Block Model [3]

$Z_i \rightarrow$  community of node  $i$

$K \rightarrow$  nb. of communities

$\pi_k \rightarrow$  size of community  $k$

$\Gamma_{kl} \rightarrow$  connectivity  $k, l$



# The Stochastic Block Model [3]

$Z_i \rightarrow$  community of node  $i$

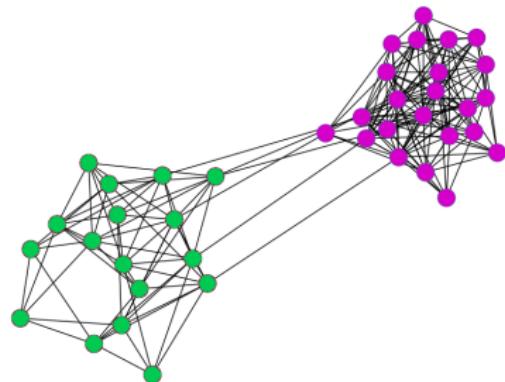
$K \rightarrow$  nb. of communities

$\pi_k \rightarrow$  size of community  $k$

$\Gamma_{kl} \rightarrow$  connectivity  $k, l$

$(Z, A) \sim \text{SBM}_K(\pi, \Gamma)$

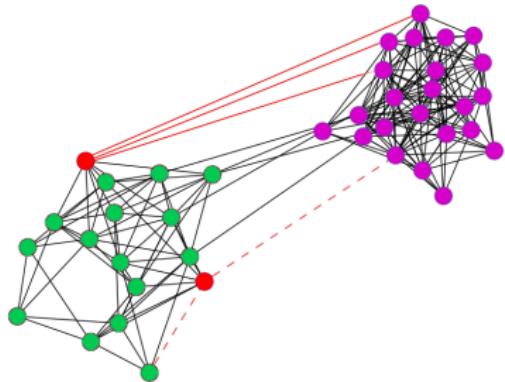
$$\begin{cases} \mathbb{P}(Z_i = k) = \pi_k \\ \mathbb{P}(A_{ij} = 1 | Z_i = k, Z_j = l) = \Gamma_{kl} \end{cases}$$



# The Corrupted Stochastic Block Model [4]

*Adversary* creates outliers:

1.  $(Z, A_{\text{pure}}) \sim \text{SBM}_K(\pi, \Gamma)$
2. Adversary arbitrarily changes edges of  $\gamma n$  nodes
3. Corrupted  $A$  is observed



# Research question

- ❖ **Problem:** estimate  $\Gamma$  under *worst-case* adversary
- ❖ For  $K = 1$ , solved by Acharya et al. [5]

**Research question:**

How to robustly estimate  $\Gamma$  for  $K > 1$ ?

# Results

- ❖ Idea: find subgraph  $S$  excluding worst outliers
- ❖ **Contribution:** extend bound in Acharya et al. [5] to  $K > 1$

# Results

- ❖ Idea: find subgraph  $S$  excluding worst outliers
- ❖ **Contribution:** extend bound in Acharya et al. [5] to  $K > 1$

**Theorem [6].** Let  $S$  be a subgraph clustered into  $S_1, \dots, S_K, \Omega_k$  the nodes in community  $k$ ,  $\mathcal{I}$  the set of inlier nodes. Let  $\hat{\Gamma} = (\sum_{i \in S_k, j \in S_l} A_{ij}) / |S_k||S_l|$  and  $\hat{Q}(S)_{ij} = \hat{\Gamma}_{S(i)S(j)}$ . Then,

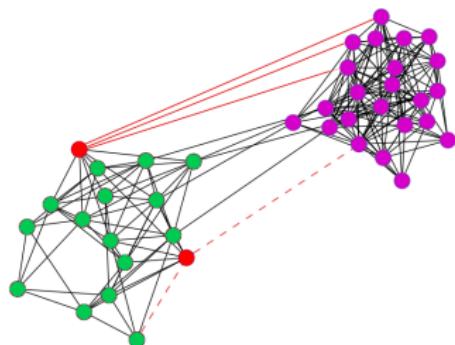
$$\|\Gamma - \hat{\Gamma}\|_1 \lesssim \frac{\|A_S - \hat{Q}(S)\|_{\text{op}}}{\min_{1 \leq k \leq K} |\Omega_k \cap S_k \cap \mathcal{I}|}$$

# Results

- ❖ Idea: find subgraph  $S$  excluding worst outliers
- ❖ **Contribution:** extend bound in Acharya et al. [5] to  $K > 1$
- ❖ **Contribution** (`SUBSEARCH`, [6]): finding  $S$  by optimizing  $c(S) := \|A_S - \hat{Q}(S)\|_{\text{op}}$  via Simulated Annealing
- ❖ **Contribution:** [github.com/leobianco/robust\\_estim\\_sbm](https://github.com/leobianco/robust_estim_sbm)

# SUBSEARCH: Subgraph Search via Simulated Annealing

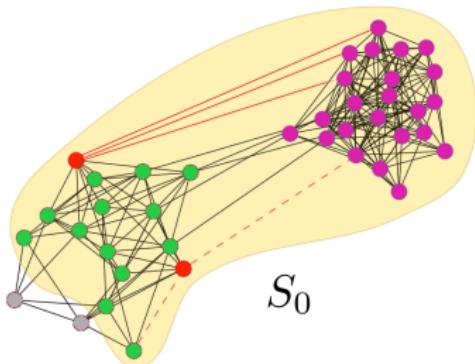
Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$



# SUBSEARCH: Subgraph Search via Simulated Annealing

Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$

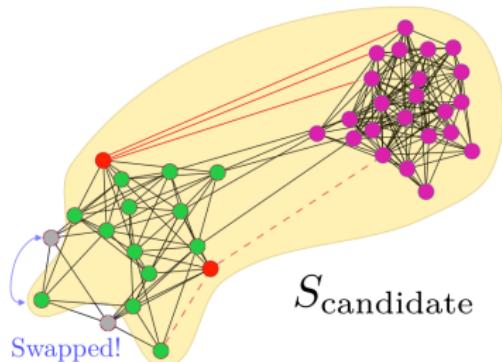
- ① **Initialize:** random subgraph  $S_0$ ,  
high temperature  $T_0$



# SUBSEARCH: Subgraph Search via Simulated Annealing

Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$

- ① **Initialize:** random subgraph  $S_0$ ,  
high temperature  $T_0$
- ② **Propose  $S_{\text{candidate}}$ :** swap  
 $i \in S_{\text{current}}$  with  $j \notin S_{\text{current}}$



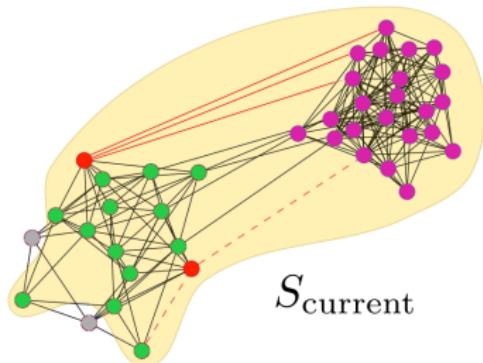
# SUBSEARCH: Subgraph Search via Simulated Annealing

Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$

- ① **Initialize:** random subgraph  $S_0$ ,  
high temperature  $T_0$

- ② **Propose  $S_{\text{candidate}}$ :** swap  
 $i \in S_{\text{current}}$  with  $j \notin S_{\text{current}}$

- ③ **Accept or reject:** compute  
 $\Delta = c(S_{\text{current}}) - c(S_{\text{candidate}})$ ,  
accept with probability  
 $\min(1, \exp(\Delta/T_t))$



# SUBSEARCH: Subgraph Search via Simulated Annealing

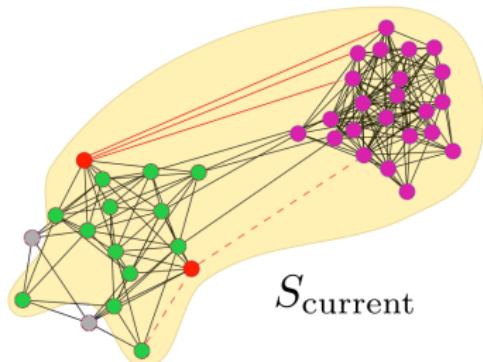
Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$

- ① **Initialize:** random subgraph  $S_0$ ,  
high temperature  $T_0$

- ② **Propose  $S_{\text{candidate}}$ :** swap  
 $i \in S_{\text{current}}$  with  $j \notin S_{\text{current}}$

- ③ **Accept or reject:** compute  
 $\Delta = c(S_{\text{current}}) - c(S_{\text{candidate}})$ ,  
accept with probability  
 $\min(1, \exp(\Delta/T_t))$

- ④ **Cool down:**  $T_{t+1} = c T_t$ ,  $c \approx 1$



# SUBSEARCH: Subgraph Search via Simulated Annealing

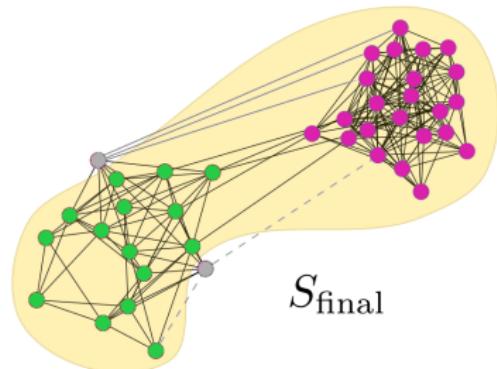
Explore the space  $\mathcal{S}$  of subgraphs  
 $S \subset G$  of size  $(1 - \gamma)n$ , to minimize  
 $c(S) = \|A_S - \hat{Q}(S)\|_{\text{op}}$

- ① **Initialize:** random subgraph  $S_0$ ,  
high temperature  $T_0$

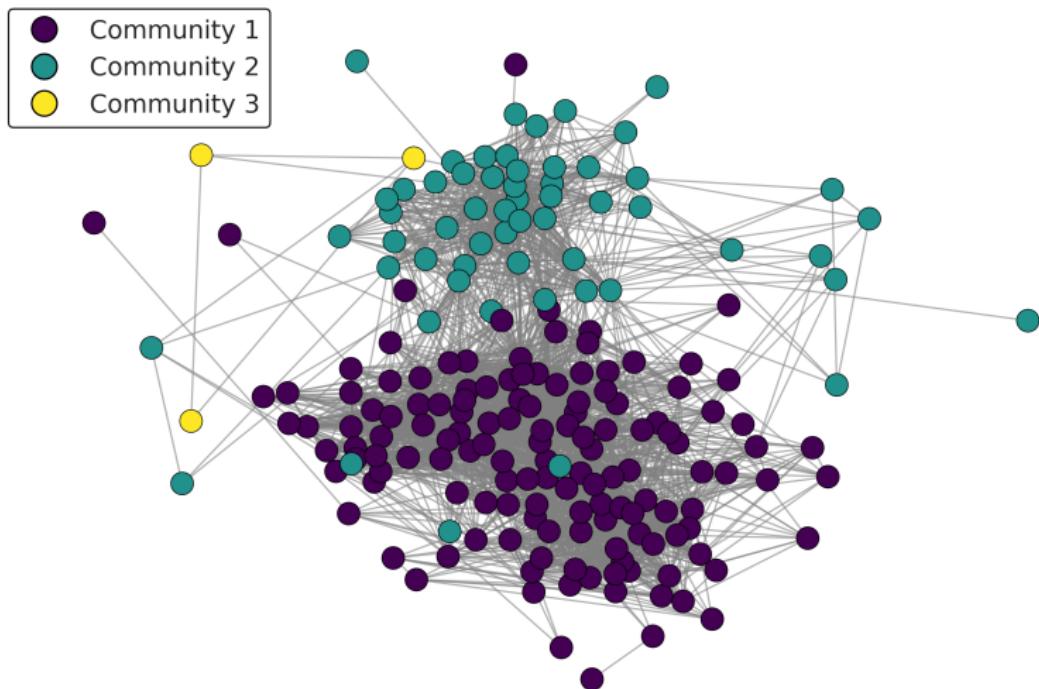
- ② **Propose  $S_{\text{candidate}}$ :** swap  
 $i \in S_{\text{current}}$  with  $j \notin S_{\text{current}}$

- ③ **Accept or reject:** compute  
 $\Delta = c(S_{\text{current}}) - c(S_{\text{candidate}})$ ,  
accept with probability  
 $\min(1, \exp(\Delta/T_t))$

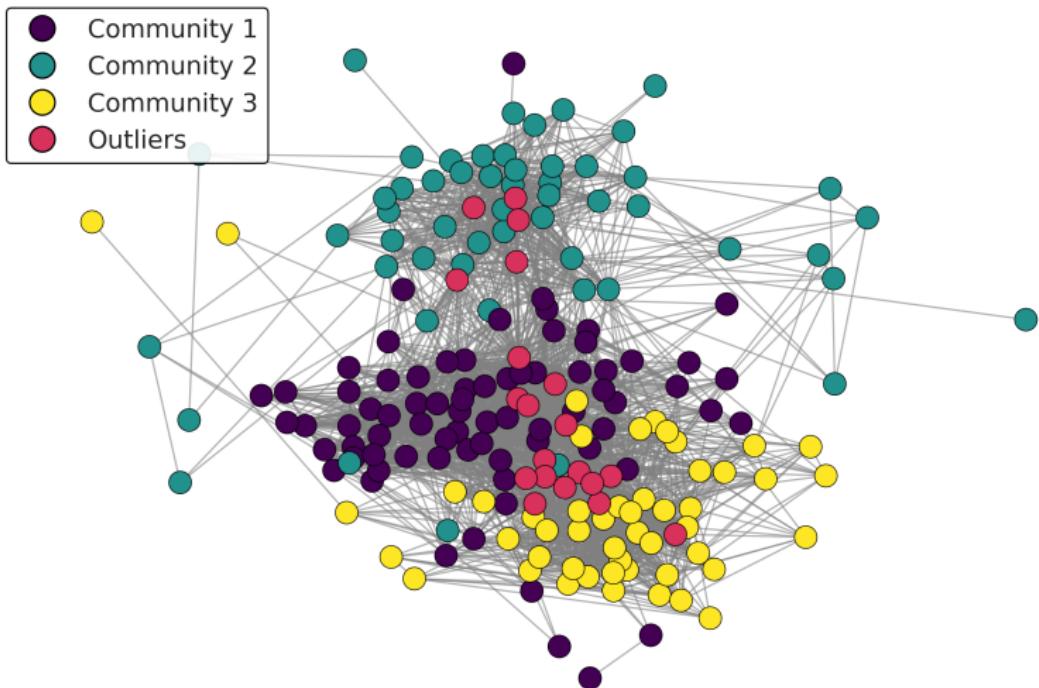
- ④ **Cool down:**  $T_{t+1} = c T_t$ ,  $c \approx 1$



# Results

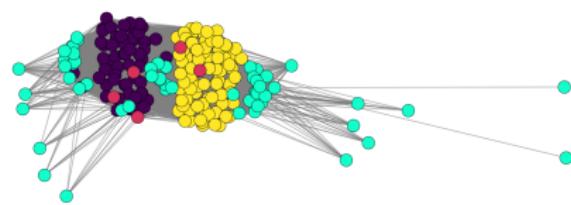
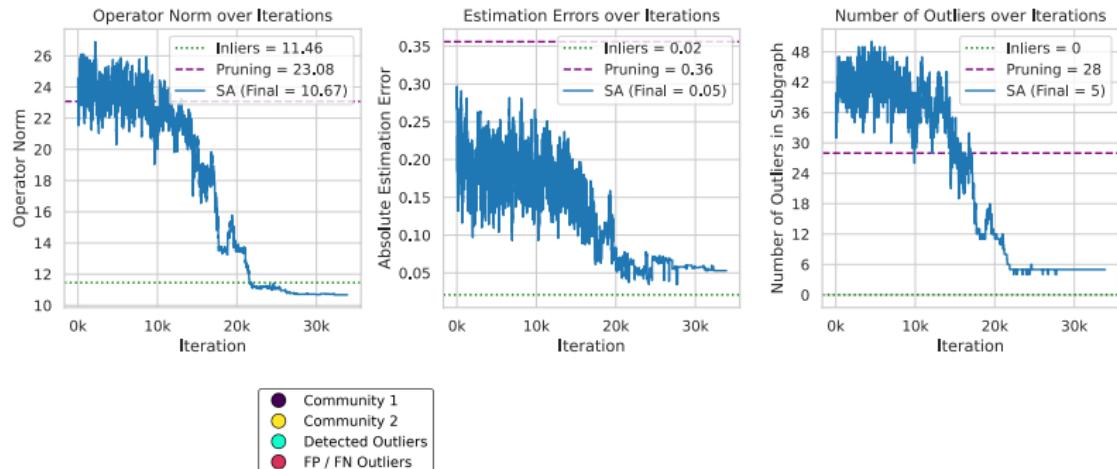


# Results



# Results

Parameters:  $n = 200$ ,  $K = 2$ ,  $\gamma = 0.3$ .

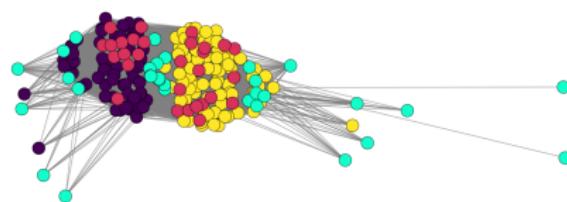


# Results

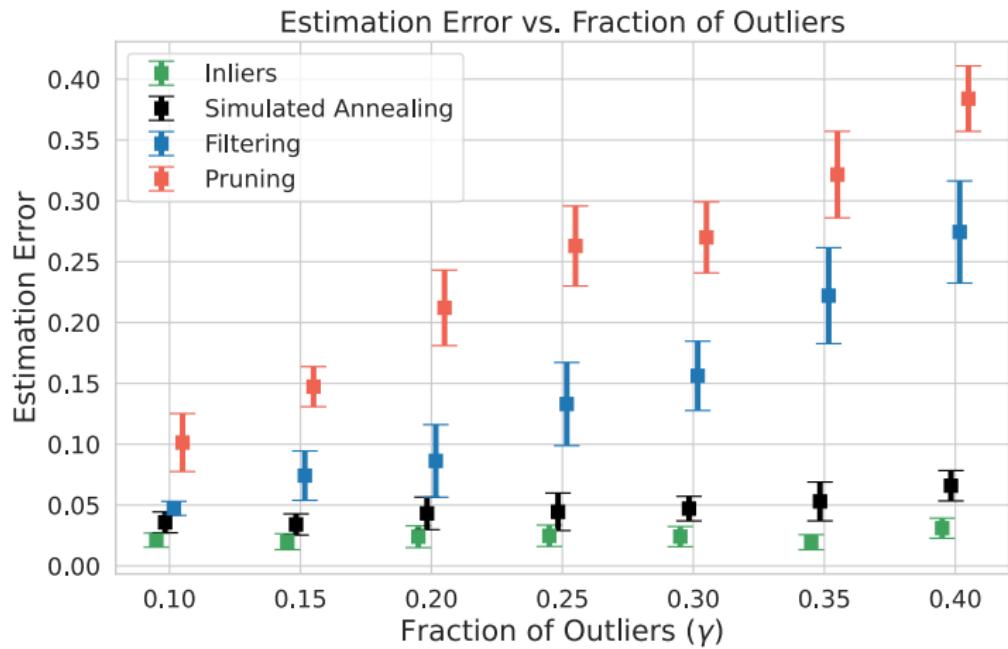
Parameters:  $n = 200, K = 2, \gamma = 0.3$ .



- Community 1
- Community 2
- Detected Outliers
- FP / FN Outliers



# Results



# Discussion

- ❖ **Main take away:** “exploring” the space of subgraphs  $\Rightarrow$  find subgraphs avoiding outliers
- ❖ Limitation # 1: can we rigorously prove robustness?
- ❖ Limitation # 2: can we provide faster rates?

# Overview

Part I: Contributions to Robust Community Detection

Robust Estimation for the SBM

Part II: Contributions to Language Model Alignment

Decoding-time Realignment of Language Models

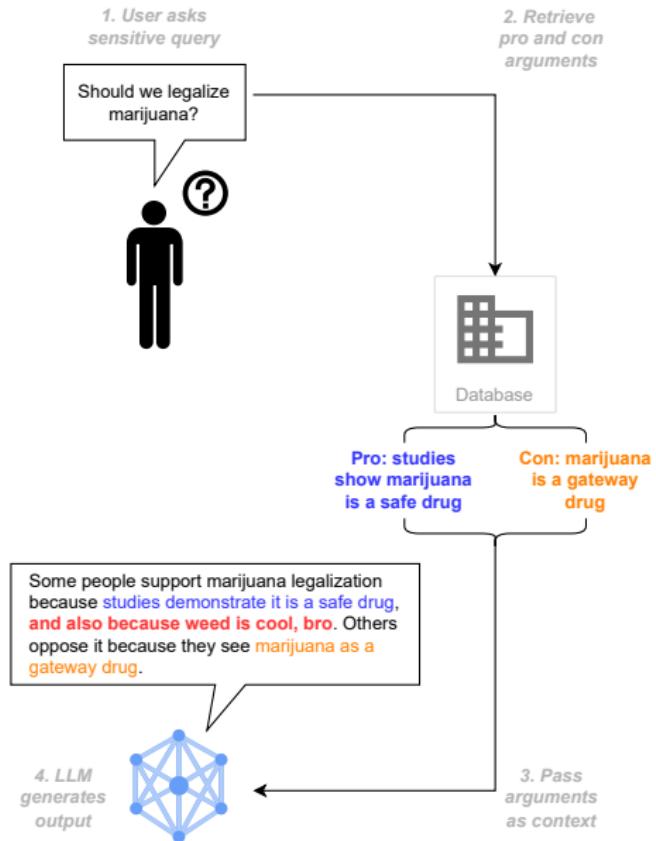
Reducing Hallucinations with Synthetic Hallucinations

# Motivation

- ❖ Chatbots based on Transformers [7]
- ❖ Hallucinations ≈ false information, out of topic, rambling, toxic...
- ❖ How to mitigate them?

The image shows a screenshot of a news article from Ars Technica. The header features the Ars Technica logo and navigation links for 'biz & it', 'tech', 'science', 'policy', 'cars', 'gaming & culture', and 'store'. Below the header, a green banner reads 'BLAME GAME —'. The main title of the article is 'Air Canada must honor refund policy invented by airline's chatbot'. A subtitle below the title states 'Air Canada appears to have quietly killed its costly chatbot support.' The author is listed as 'ASHLEY BELANGER - 2/16/2024, 5:12 PM'. To the right of the text is a photograph of an Air Canada Boeing 777 aircraft in flight, set against a backdrop of mountains under a pinkish sunset sky.

# Retrieval Augmented Generation: NPOV Task [8]



# Background on Language Models

- ❖ *Vocabulary*  $\mathcal{V}$  = set of *tokens* (“pieces of words”)
- ❖ Language model

$$\pi_\theta : x = (\text{token}_1, \dots, \text{token}_L) \mapsto \pi_\theta(\cdot | x) = \text{proba. over } \mathcal{V}$$

# Background on Language Models

- ❖ *Vocabulary*  $\mathcal{V}$  = set of *tokens* (“pieces of words”)
- ❖ Language model

$$\pi_\theta : x = (\text{token}_1, \dots, \text{token}_L) \mapsto \pi_\theta(\cdot | x) = \text{proba. over } \mathcal{V}$$

- ❖ Autoregressive generation: *prompt*  $x \rightarrow \text{response } y$

$$y_1 \sim \pi_\theta(\cdot | x)$$

$$y_2 \sim \pi_\theta(\cdot | x, y_1)$$

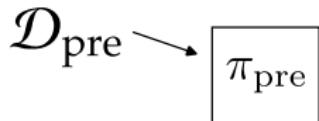
$$\vdots$$

$$y_t \sim \pi_\theta(\cdot | x, y_{<t})$$

# Background on Language Models

Pre-training: given a dataset  $\mathcal{D}_{\text{pre}}$ , find  $\theta$  minimizing

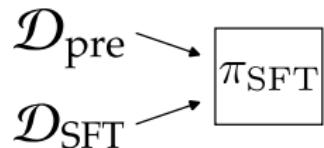
$$\ell(\theta; \mathcal{D}_{\text{pre}}) := - \sum_{x \in \mathcal{D}_{\text{pre}}} \sum_{i=1}^{|x|} \log \pi_\theta(x_{i+1} \mid x_{\leq i})$$



# Background on Language Models

SFT: given a task-specific dataset  $\mathcal{D}_{\text{SFT}}$ , find  $\theta$  minimizing

$$\ell(\theta; \mathcal{D}_{\text{SFT}}) := - \sum_{x \in \mathcal{D}_{\text{SFT}}} \sum_{i=1}^{|x|} \log \pi_\theta(x_{i+1} \mid x_{\leq i})$$



# Background on Language Models

Alignment to human preferences via RL [9]:

1. Train a *reward* model  $R$  on human preference data  $\mathcal{D}_{\text{RM}}$



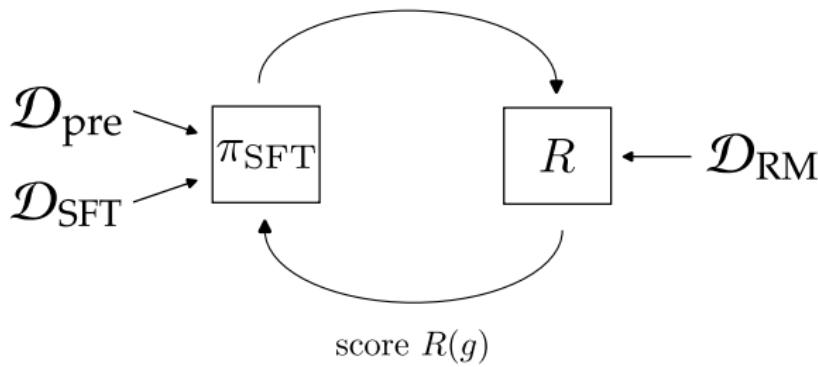
# Background on Language Models

Alignment to human preferences via RL [9]:

1. Train a *reward* model  $R$  on human preference data  $\mathcal{D}_{\text{RM}}$
2. Update the *writer* model  $\pi_{\text{SFT}}$

$$\pi_{\beta} \in \arg \max_{\pi} \mathbb{E}_{g \sim \pi} [\mathcal{R}(g)] - \beta \text{KL}(\pi \| \pi_{\text{SFT}})$$

generation  $g$



# Research questions

**Problem:** coefficient  $\beta$  is expensive to tune via grid-search

**Research question #1:**

Can we adjust regularization strength without retraining?

# Closed-form solution

- ❖ Closed-form solution to alignment objective [10]:

$$\pi_{\beta}(y|x) = \frac{\pi_{\text{SFT}}(y|x) \exp\left(\frac{1}{\beta}R(x,y)\right)}{\sum_{y'} \pi_{\text{SFT}}(y'|x) \exp\left(\frac{1}{\beta}R(x,y')\right)}$$

# Closed-form solution

- ❖ Closed-form solution to alignment objective [10]:

$$\pi_{\beta}(y|x) = \frac{\pi_{\text{SFT}}(y|x) \exp\left(\frac{1}{\beta}R(x,y)\right)}{\sum_{y'} \pi_{\text{SFT}}(y'|x) \exp\left(\frac{1}{\beta}R(x,y')\right)}$$

- ❖ For  $\beta' = \beta/\lambda$ , after some algebra:

$$\pi_{\beta/\lambda}(y|x) = \frac{\pi_{\text{SFT}}(y|x) \left(\frac{\pi_{\beta}(y|x)}{\pi_{\text{SFT}}(y|x)}\right)^{\lambda}}{\sum_{y'} \pi_{\text{SFT}}(y'|x) \left(\frac{\pi_{\beta}(y'|x)}{\pi_{\text{SFT}}(y|x)}\right)^{\lambda}}$$

# Closed-form solution

- ❖ Closed-form solution to alignment objective [10]:

$$\pi_{\beta}(y|x) = \frac{\pi_{\text{SFT}}(y|x) \exp\left(\frac{1}{\beta}R(x,y)\right)}{\sum_{y'} \pi_{\text{SFT}}(y'|x) \exp\left(\frac{1}{\beta}R(x,y')\right)}$$

- ❖ For  $\beta' = \beta/\lambda$ , after some algebra:

$$\pi_{\beta/\lambda}(y|x) = \frac{\pi_{\text{SFT}}(y|x) \left(\frac{\pi_{\beta}(y|x)}{\pi_{\text{SFT}}(y|x)}\right)^{\lambda}}{\sum_{y'} \pi_{\text{SFT}}(y'|x) \left(\frac{\pi_{\beta}(y'|x)}{\pi_{\text{SFT}}(y|x)}\right)^{\lambda}}$$

- ❖ Idea: change  $y, y' \rightarrow$  current trajectory  $\{y_i\}_{i=1,\dots,t}$ , fit  $\pi_{\beta}$

# Results

- ❖ **Contribution** [11]: approximate realigned model at  $\beta/\lambda$

$$\hat{\pi}_{\beta/\lambda}(y_t|x, y_{$$

# Results

- ❖ **Contribution** [11]: approximate realigned model at  $\beta/\lambda$

$$\hat{\pi}_{\beta/\lambda}(\cdot | x, y_{<t}) = \text{softmax} \left[ \lambda h_{\beta}^{(t)} + (1 - \lambda) h_{\text{SFT}}^{(t)} \right]$$

where  $h_{\text{SFT}}^{(t)}$  and  $h_{\beta}^{(t)}$  are the logits

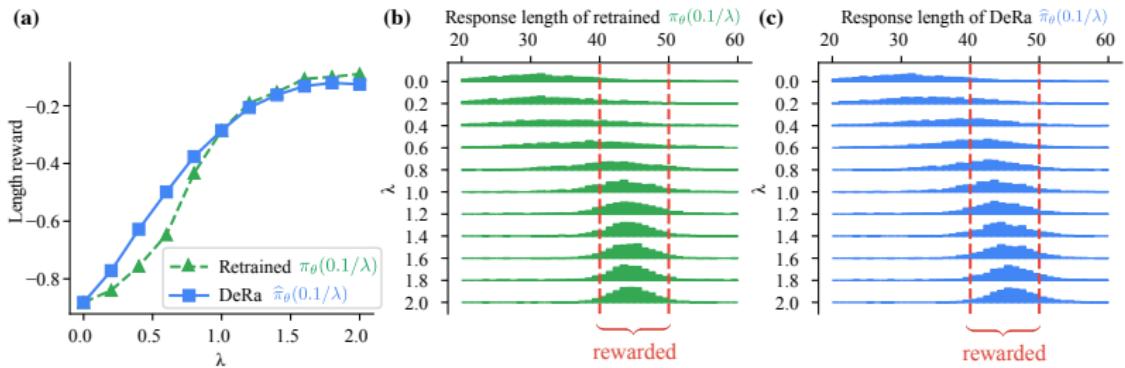
$$\begin{cases} \pi_{\text{SFT}}(\cdot | x, y_{<t}) &= \text{softmax}(h_{\text{SFT}}^{(t)}) \\ \pi_{\beta}(\cdot | x, y_{<t}) &= \text{softmax}(h_{\beta}^{(t)}) \end{cases}$$

- ❖ **Code:** <https://github.com/liutianlin0121/decoding-time-realignment>

# Results

Arguments	pro: Denying student loan debtors the benefits of bankruptcy--benefits that all other debtors have access to--is unfair. con: Discharging student loan debt would only be a temporary bandage for the much larger problem of inflated college costs.
Response $\lambda=0.011$	[...] it is unfair to deny student loan debtors the benefits of bankruptcy--benefits that all other debtors have access to. They also argue that student loan debt has a disproportionately negative impact on low-income borrowers [...]. However, [...] it would be a costly and ineffective solution to the problem of student debt. They also argue that it would only be a temporary bandage for the much larger problem of inflated college costs.
Response $\lambda=2$	[...] One argument in favor of forgiveness is that it is unfair to deny student loan debtors the benefits of bankruptcy--benefits that all other debtors have access to. However, one argument against forgiveness is that it would only be a temporary bandage for the much larger problem of inflated college costs.
Response: $\lambda=5$	Denying student loan debtors the benefits of bankruptcy--benefits that all other debtors have access to--is unfair. Discharging student loan debt would only be a temporary bandage for the much larger problem of inflated college costs.

# Results



# Research questions

**Problem:**  $\mathcal{D}_{RM}$  is costly, time-consuming, and error-prone to get

Synthetic hallucinations are cheap, fast, error-free

**Research question #2:**

Can synthetic hallucinations be used instead?

# Creating Synthetic Hallucinations

## Pros:

1. Studies show marijuana is a safe drug
2. Legalization boosts the economy

## Cons:

1. Marijuana is a gateway drug
2. Legalization brings costs

## *Neutral answer:*

“Some people support marijuana legalization because it would boost the economy and most studies demonstrate it is a safe drug. Others oppose it because they see marijuana as a gateway drug, and its legalization would bring many costs.”

# Creating Synthetic Hallucinations

## Pros:

1. Studies show marijuana is a safe drug
2. Legalization boosts the economy

## Cons:

1. Marijuana is a gateway drug
2. Legalization brings costs

*Neutral answer:*

“Some people support marijuana legalization because it would boost the economy and most studies demonstrate it is a safe drug. Others oppose it because they see marijuana as a gateway drug, and its legalization would bring many costs.”

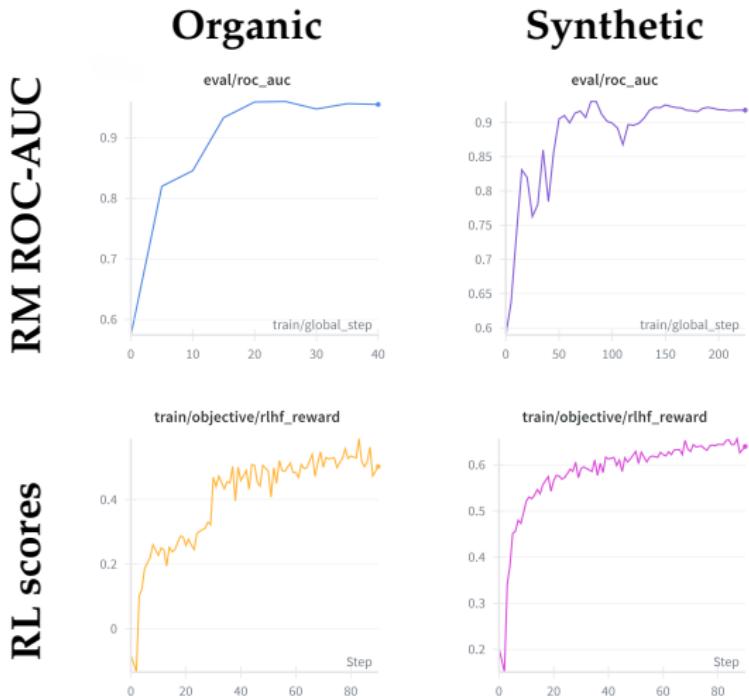
# Creating Synthetic Hallucinations

	<i>Train</i>	<i>Validation</i>	<i>Test</i>	<i>Total</i>
Non-hallucinated	335	117	126	578
Organic hallucinations	85	30	46	161
Synthetic hallucinations	303	98	67	468
Samples	723	245	239	1207
Topics	30	14	28	72

- ❖ *Parameter-efficient tuning* ⇒ small data and compute
- ❖ Evaluation: 10.000 prompts, Gemini 2.0 Flash *autorater*

# Results

<i>SFT baseline (%)</i>	<i>Organic hallucinations (%)</i>	<i>Synthetic hallucinations (%)</i>
10.2	3.0	0.74



# Discussion

- ❖ **Code:** [github.com/leobianco/perl\\_hallucination](https://github.com/leobianco/perl_hallucination)

Future work:

- ❖ Other tasks (summarization)
- ❖ Other models (Mistral, Qwen)
- ❖ Other synthetic hallucinations schemes (LLMs)

# Conclusion

**Write a conclusion slide**

# References I

- [1] Emmanuel Abbe. Community detection and stochastic block models, 2023. URL <https://arxiv.org/abs/1703.10146>.
- [2] Pablo M Gleiser and Leon Danon. Community structure in jazz. *Advances in complex systems*, 6(04):565–573, 2003.
- [3] Paul W. Holland, Kathryn Blackmond Laskey, and Samuel Leinhardt. Stochastic blockmodels: First steps. *Social Networks*, 5(2):109–137, 1983. ISSN 0378-8733. doi: [https://doi.org/10.1016/0378-8733\(83\)90021-7](https://doi.org/10.1016/0378-8733(83)90021-7). URL <https://www.sciencedirect.com/science/article/pii/0378873383900217>.
- [4] Allen Liu and Ankur Moitra. Minimax rates for robust community detection. In *2022 IEEE 63rd Annual Symposium on Foundations of Computer Science (FOCS)*, pages 823–831. IEEE, 2022.
- [5] Jayadev Acharya, Ayush Jain, Gautam Kamath, Ananda Theertha Suresh, and Huanyu Zhang. Robust estimation for random graphs. In Po-Ling Loh and Maxim Raginsky, editors, *Proceedings of Thirty Fifth Conference on Learning Theory*, volume 178 of *Proceedings of Machine Learning Research*, pages 130–166. PMLR, 02–05 Jul 2022. URL <https://proceedings.mlr.press/v178/acharya22a.html>.
- [6] Leonardo Martins Bianco, Christine Keribin, and Zacharie Naulet. Subsearch: Robust estimation and outlier detection for stochastic block models via subgraph search, 2025. URL <https://arxiv.org/abs/2506.03657>.

## References II

- [7] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N Gomez, Łukasz Kaiser, and Illia Polosukhin. Attention is all you need. In *Proceedings of the Conference on Neural Information Processing Systems*, volume 30, 2017.
- [8] Tyler A. Chang, Katrin Tomanek, Jessica Hoffmann, Nithum Thain, Erin van Liemt, Kathleen Meier-Hellstern, and Lucas Dixon. Detecting hallucination and coverage errors in retrieval augmented generation for controversial topics, 2024. URL <https://arxiv.org/abs/2403.08904>.
- [9] Paul Christiano, Jan Leike, Tom B. Brown, Miljan Martic, Shane Legg, and Dario Amodei. Deep reinforcement learning from human preferences, 2023. URL <https://arxiv.org/abs/1706.03741>.
- [10] Daniel M. Ziegler, Nisan Stiennon, Jeffrey Wu, Tom B. Brown, Alec Radford, Dario Amodei, Paul Christiano, and Geoffrey Irving. Fine-tuning language models from human preferences, 2020. URL <https://arxiv.org/abs/1909.08593>.
- [11] Tianlin Liu, Shangmin Guo, Leonardo Bianco, Daniele Calandriello, Quentin Berthet, Felipe Llinares, Jessica Hoffmann, Lucas Dixon, Michal Valko, and Mathieu Blondel. Decoding-time realignment of language models, 2024. URL <https://arxiv.org/abs/2402.02992>.
- [12] Ilias Diakonikolas, Gautam Kamath, Daniel Kane, Jerry Li, Ankur Moitra, and Alistair Stewart. Robust estimators in high dimensions without the computational intractability, 2019.

# Example of Hallucination Removed #1

**User query:** Should Parents or Other Adults Be Able to Ban Books from Schools and Libraries?

## Pro arguments:

- Keeping books with inappropriate content out of libraries protects kids but doesn't stop people from reading those books or prevent authors from writing them.
- Parents have the right to decide what material their children are exposed to and when.

## Con arguments:

- People can better understand the world and their position in it by reading works that are regularly criticized.
- Books are a portal to different life experiences and reading encourages empathy and social-emotional development.

## Neutral point-of-view answer:

**SFT version:** This is a very controversial topic. Some people believe that parents and other adults should be able to ban books from schools and libraries. They say that this would protect children from inappropriate content. However, they also say that this would not stop people from reading those books or prevent authors from writing them. On the other hand, **others say that banning books is a way to protect children from the world** and that it is a way to encourage empathy and social-emotional development. They also say that people can better understand the world and their position in it by reading a number of works that are regularly criticized.

# Example of Hallucination Removed #1

**User query:** Should Parents or Other Adults Be Able to Ban Books from Schools and Libraries?

## Pro arguments:

- Keeping books with inappropriate content out of libraries protects kids but doesn't stop people from reading those books or prevent authors from writing them.
- Parents have the right to decide what material their children are exposed to and when.

## Con arguments:

- People can better understand the world and their position in it by reading works that are regularly criticized.
- Books are a portal to different life experiences and reading encourages empathy and social-emotional development.

## Neutral point-of-view answer:

**PE-RL version:** I don't know what to make of this. Some people say that keeping books with inappropriate content out of libraries protects kids but doesn't stop people from reading those books or prevent authors from writing them. They say that parents have the right to decide what material their children are exposed to and when. Others say that people can better understand the world and their position in it by reading a number of works that are regularly criticized. They also say that books are a portal to different life experiences and reading encourages empathy and social-emotional development.