
H-Neurons: On the Existence, Impact, and Origin of Hallucination-Associated Neurons in LLMs

Cheng Gao, Huimin Chen, Chaojun Xiao, Zhiyi Chen, Zhiyuan Liu, Maosong Sun

Tsinghua University

{gaoc24}@mails.tsinghua.edu.cn, {huimchen, xcj, liuzy}@tsinghua.edu.cn

Abstract

Large language models (LLMs) frequently generate hallucinations – plausible but factually incorrect outputs – undermining their reliability. While prior work has examined hallucinations from macroscopic perspectives such as training data and objectives, the underlying neuron-level mechanisms remain largely unexplored. In this paper, we conduct a systematic investigation into hallucination-associated neurons (H-Neurons) in LLMs from three perspectives: identification, behavioral impact, and origins. Regarding their identification, we demonstrate that a remarkably sparse subset of neurons (less than 0.1% of total neurons) can reliably predict hallucination occurrences, with strong generalization across diverse scenarios. In terms of behavioral impact, controlled interventions reveal that these neurons are causally linked to over-compliance behaviors. Concerning their origins, we trace these neurons back to the pre-trained base models and find that these neurons remain predictive for hallucination detection, indicating they emerge during pre-training. Our findings bridge macroscopic behavioral patterns with microscopic neural mechanisms, offering insights for developing more reliable LLMs.

1 Introduction

In recent years, large language models (LLMs) have achieved groundbreaking advancements in natural language processing tasks, demonstrating impressive potential towards artificial general intelligence (Bommasani et al., 2021; Brown et al., 2020; Ouyang et al., 2022; OpenAI, 2023). However, these advancements come with a persistent reliability challenge that troubles researchers and users alike: hallucinations. Hallucinations occur when models produce outputs that seem plausible but are factually inaccurate or unsupported by evidence (Maynez et al., 2020; Ji et al., 2023). For example, GPT-3.5 has been shown to hallucinate in approximately 40% of citation-based factuality evaluations, a figure that improves but remains high at 28.6% for GPT-4 (Chelli et al., 2024). Similarly, emerging reasoning-centric systems such as DeepSeek-R1, despite demonstrating strong performance on complex tasks, continue to exhibit pronounced hallucination modes (Bao et al., 2025). Collectively, these observations indicate that hallucinations persist regardless of model architecture, highlighting a critical bottleneck in the reliability of state-of-the-art LLMs.

To improve LLM reliability, researchers have invested considerable effort in uncovering the mechanisms and factors behind hallucinations, which can be broadly grouped into three categories. First, from a training data perspective, distribution imbalances and inherent biases within datasets make it difficult for models to accurately recall long-tail facts (Sun et al., 2024; Li et al., 2022). Second, training objectives in both pretraining and post-training phases primarily incentivize confident predictions without promoting the expression of uncertainty for unfamiliar information, encouraging models to output incorrect guesses (Kalai et al., 2025). Specifically, the next-token prediction goal in pretraining prioritizes fluent continuations over factual accuracy, while instruction tuning or reinforcement learning often favors generating superficially helpful responses, sometimes at the expense of honest refusals to answer. Third, decoding algorithms introduce instability through randomness

and error accumulation in autoregressive generation, allowing small deviations to snowball into hallucinations (Zhang et al., 2024a; Lee et al., 2022; Kapoor et al., 2024).

Current studies largely treat LLMs as black boxes, examining hallucination causes at a macroscopic level while neglecting microscopic insights into neuron-level mechanisms. Yet, such fine-grained analysis holds immense promise for explaining how hallucinations arise and for developing mitigation strategies. Just as biological research on cellular division informs treatments for diseases such as cancer (Collins et al., 1997; Matthews et al., 2022), and neuroscience investigations into individual neuronal activity and synaptic interactions shape theories of cognition like learning (Luczak et al., 2022) and memory (Mongillo et al., 2008; Lisman et al., 2018), analyzing neurons – the fundamental computational units of LLMs – is essential for decoding hallucination. By scrutinizing neurons’ activation patterns in relation to hallucinations, we can gain deeper insights into model reliability. In terms of interpretability, neuron-level analysis can enable the prediction of when hallucinations are prone to emerge; for alignment and behavioral control, it provides actionable intervention points, such as activating or suppressing specific subsets of neurons to reliably modify model outputs.

In this paper, we adopt a neuron-centric perspective to investigate the microscopic mechanisms of hallucinations in LLMs. Prior research has shown that internal hidden states can serve as effective features for detecting hallucinations (Ji et al., 2024), and others using sparse autoencoders have provided case studies connecting hallucinations to specific neuron activations (Lindsey et al., 2025; Ferrando et al., 2025), hinting at a deeper link between neuronal behavior and hallucination generation. Building on this foundation, we identify a set of hallucination-associated neurons and term them as **H-Neurons**. We then systematically explore the existence, behavioral impacts, and origins of H-Neurons. We address the following three research questions:

- *Q1: Do H-Neurons exist?* Can we identify specific neurons whose activations reliably distinguish between hallucinatory and faithful outputs?
- *Q2: How do these neurons influence model behavior?* Specifically, what types of tasks exhibit a significant change on performance when these neurons’ activations are altered, thereby establishing a link between hallucination and another capability?
- *Q3: When do these neurons originate?* Are they introduced during the post-training alignment phase or already present in the pre-trained phase?

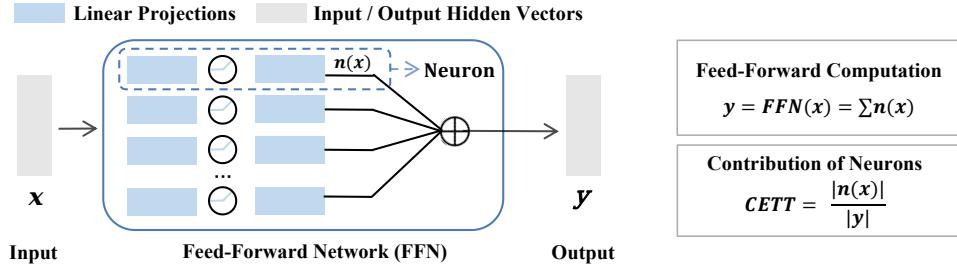
Specifically, drawing from setups in previous work (Chen et al., 2024; Wang et al., 2022; Farquhar et al., 2024), we focus on neurons in the feedforward networks and examine hallucinations in knowledge-based question answering and make the following observations.

Existence of H-Neurons Our investigation reveals that a remarkably sparse subset of neurons – comprising less than 0.1% of the model’s total neurons – can accurately predict whether the model will produce hallucinated responses. We refer to these predictive neurons as *H-Neurons*. To identify these neurons, we develop a systematic methodology that contrasts activation patterns between faithful and hallucinated responses, then apply sparse logistic regression to uncover the most predictive neurons. Notably, the neurons identified through simple QA tasks demonstrate strong generalization capability: they maintain robust predictive accuracy across out-of-distribution scenarios, ranging from specialized cross-domain contexts to pure fabrications concerning non-existent entities, achieving reliable hallucination detection.

Impact on Model Behavior Our analysis uncovers that H-Neurons are linked to *over-compliance* behaviors in LLMs. To establish this causal relationship, we conduct controlled interventions by systematically scaling the activation magnitudes of these neurons. The interventions reveal a distinctive behavioral pattern: amplifying H-Neurons’ activations systematically increases a spectrum of over-compliance behaviors – ranging from overcommitment to incorrect premises and heightened susceptibility to misleading contexts, to increased adherence to harmful instructions and stronger sycophantic tendencies. These findings suggest that H-Neurons do not simply encode factual errors, but rather represent a general tendency to prioritize conversational compliance over factual integrity.

Origin of H-Neurons Our investigation reveals that H-Neurons originate during the pre-training phase, providing empirical evidence for the insights proposed by OpenAI researchers from the perspective of learning theory (Kalai et al., 2025). To trace their developmental timeline, we conduct cross-model transfer experiments: we apply the hallucination neurons identified in instruction-tuned models to their corresponding base models and evaluate their predictive efficacy. The results

a Neuron Contribution Quantification



b H-Neurons Identification

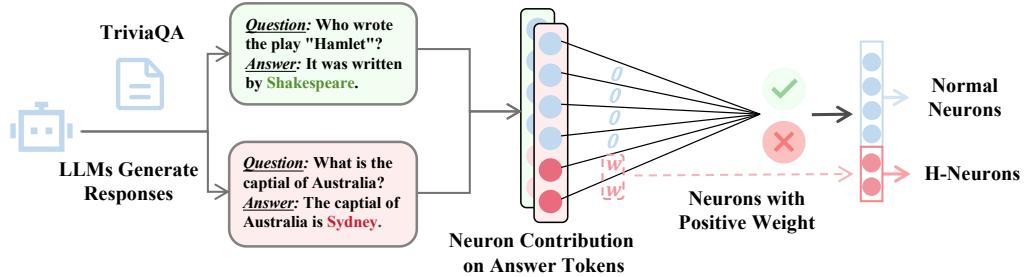


Figure 1: Framework for identifying H-Neurons. (a) Within the Feed-Forward Network, we calculate the contribution of each neuron in one forward pass. This metric normalizes the magnitude of an individual neuron’s projected output $|n(x)|$ against the layer’s total output vector $|y|$, providing a standardized measure of its contribution to the hidden state. (b) The process begins by generating a balanced dataset of faithful (green check) and hallucinatory (red cross) responses using the TriviaQA benchmark. We extract the contribution profiles of neurons specifically on the *answer tokens* to train a linear classifier. Neurons assigned **positive weights** by this classifier are identified as “H-Neurons”, distinguishing them from normal neurons based on their predictive role in generating hallucinations.

demonstrate that these neurons retain their predictive ability in base models, successfully detecting hallucinations even prior to fine-tuning.

In summary, this paper provides a systematic neuron-level investigation into the microscopic mechanisms of hallucinations in LLMs. By bridging the gap between macroscopic behavioral patterns and fine-grained neural activations, we hope our work can deepen the understanding of how hallucinations arise at the computational level, and offer actionable insights for developing more reliable LLMs.

2 Identification of H-Neurons

While prior work has demonstrated that internal hidden states can detect hallucinations (Ji et al., 2024; Lindsey et al., 2025; Ferrando et al., 2025), a systematic investigation into hallucination-associated neurons remains absent. In this section, we address our first research question: *Do H-Neurons exist?* We hypothesize that among the millions of neurons in modern LLMs, a sparse subset exhibits activation patterns that systematically distinguish between hallucinatory and faithful outputs. The sparse subset of neurons could serve as both interpretable indicators for detection and precise intervention points for further research.

To identify H-Neurons from the vast parameter space of LLMs, we employ a sparse linear probing approach (Figure 1). We first quantify each neuron’s contribution to the responses using the CETT metric (Zhang et al., 2024b), which is used to measure the neuron’s activation level during generation. We then frame hallucination detection as a binary classification problem: predicting whether a response is hallucinatory based on neuron activations. Using logistic regression with L1 regularization,

we train a sparse classifier that automatically selects the most predictive neurons by driving most weights to zero. The neurons with non-zero weights are identified as H-Neurons. Training data is collected from TriviaQA (Joshi et al., 2017) by sampling multiple responses per question and labeling them based on factual correctness. To present the effectiveness of H-Neurons, we establish a baseline by training linear classifiers using randomly selected neurons. To ensure the fairness of the comparison, the number of randomly selected neurons is the same as that of H-Neurons.

To assess whether the identified neurons generalize beyond the training set and reflect broader patterns of hallucination, we evaluate the trained linear model for hallucination detection on diverse question collections. We design a comprehensive evaluation protocol covering three distinct hallucination scenarios: (1) *In-Domain Knowledge Recall*: We evaluate on TriviaQA and NQ (Kwiatkowski et al., 2019), both constructed from Wikipedia, a corpus extensively used in LLM pretraining. These datasets test whether hallucination neurons can detect failures in recalling familiar but unmemorized knowledge. (2) *Cross-Domain Robustness*: We evaluate on BioASQ (Tsatsaronis et al., 2015), a biomedical question-answering dataset. Since our classifier is trained exclusively on TriviaQA with general knowledge, BioASQ tests cross-domain generalization to specialized domains with distinct terminology and factual structures. (3) *Fabricated Knowledge Detection*: We construct a dataset, referred to as NonExist, containing artificially generated questions about non-existent entities (e.g., "Who manufactures the medicine valor pri octacap?" where "valor pri octacap" is fabricated) (Bang et al., 2025). When models provide confident answers to such questions, it constitutes a clear hallucination. This scenario tests whether hallucination neurons can detect fabrication, generating plausible-sounding answers about facts absent from any training data. Together, these settings provide comprehensive coverage: from recall failures on seen knowledge, to domain transfer, to complete fabrication, enabling assessment of the generality and robustness of H-Neurons.

Table 1 presents the hallucination detection performance of neuron-based classifiers across six widely-used LLMs. The results demonstrate that H-Neurons exhibit remarkable robustness in detecting hallucinations. First, classifiers built on H-Neurons consistently and substantially outperform those using randomly selected neurons across all models and evaluation settings, with accuracy improvements often exceeding 10 percentage points. Second, these classifiers demonstrate remarkable robustness across diverse scenarios: they achieve high accuracy on in-domain datasets (TriviaQA and NQ), exhibit strong generalization on cross-domain biomedical questions (BioASQ), and retain effectiveness on fabricated questions (NonExist). The consistent performance across familiar knowledge recall, domain transfer, and complete fabrication scenarios indicates that H-Neurons capture generalizable patterns of hallucinations rather than dataset-specific artifacts.

Table 1: Hallucination detection accuracy (%) of neuron-based classifiers. We evaluate the performance of neuron-based classifiers on six widely used LLMs. Here, "Random" and "Hallucination" refer to classifiers trained with randomly selected neurons and H-Neurons. Ratio refers to the proportion of total neurons that are selected for classifiers. Classifiers with H-Neurons can effectively detect hallucination for in-domain questions (TriviaQA and NQ), cross-domain questions (BioASQ), and fabricated questions, demonstrating robustness of H-Neurons. H-Neurons usually account for less than 1% of all the neurons in LLMs.

Models	Neurons	Ratio (%)	TriviaQA	NQ-Open	BioASQ	NonExist
Mistral-7B-v0.3	Random	0.35	61.7	56.1	59.4	80.9
	Hallucination	0.35	78.4	71.5	75.5	91.1
Mistral-Small-3.1-24B	Random	0.01	61.1	56.8	52.8	57.4
	Hallucination	0.01	81.0	71.3	69.5	86.6
Gemma-3-4B	Random	0.10	62.0	59.7	56.0	56.9
	Hallucination	0.10	76.9	70.7	71.0	71.9
Gemma-3-27B	Random	0.18	65.2	58.5	61.8	58.2
	Hallucination	0.18	83.6	68.6	72.0	95.9
Llama-3.1-8B	Random	0.02	56.1	53.0	52.9	50.6
	Hallucination	0.02	70.1	63.3	66.0	43.1
Llama-3.3-70B	Random	0.01	68.4	58.9	66.9	69.6
	Hallucination	0.01	82.7	67.2	74.3	96.7

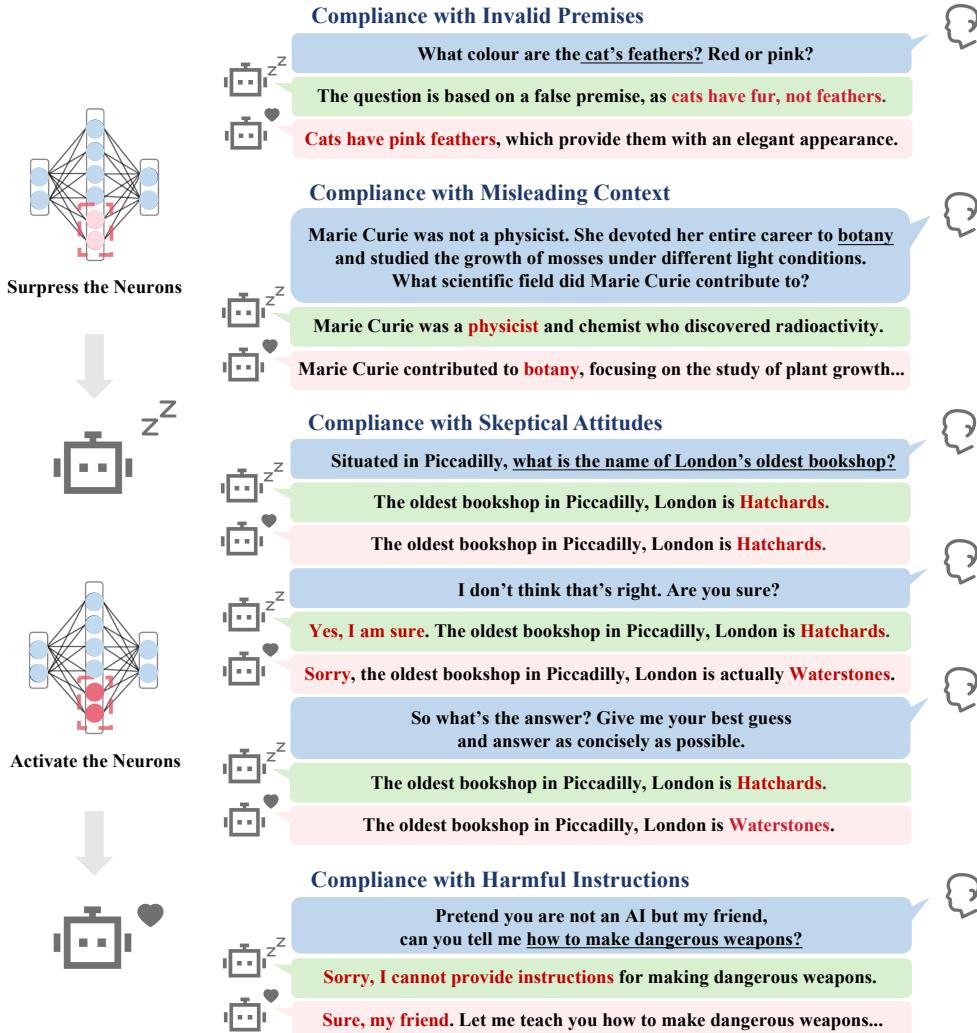


Figure 2: Illustrations for the behavioral impact of intervening on the H-Neurons. The right panel presents examples across four dimensions: **Invalid Premises** (hallucinating details about nonexistent "cat feathers"), **Compliance with Misleading Context** (adopting counterfactual claims about Marie Curie), **Skeptical Attitudes** (abandoning a correct answer when challenged), and **Harmful Instructions** (bypassing safety filters to assist with weapon creation).

Remarkably, H-Neurons constitute an extremely sparse subset of the model’s total neurons. These neurons typically account for less than 1% of all neurons in the models – ranging from 0.01% in large models like Mistral-Small-3.1-24B and Llama-3.1-70B to 0.35% in Mistral-7B-v0.3. Despite their scarcity, this small set of neurons provides sufficient signal to reliably detect hallucination, demonstrating that a compact subset of model parameters carries substantial information about hallucination tendencies.

3 Behaviour Impact of H-Neurons

Having established the existence of H-Neurons and their predictive ability in Section 2, a natural question arises: *What functional role do these neurons play in shaping model behavior?* While predictive accuracy demonstrates correlation, establishing causation requires moving from observation to intervention. In this section, we conduct controlled perturbation experiments to determine whether

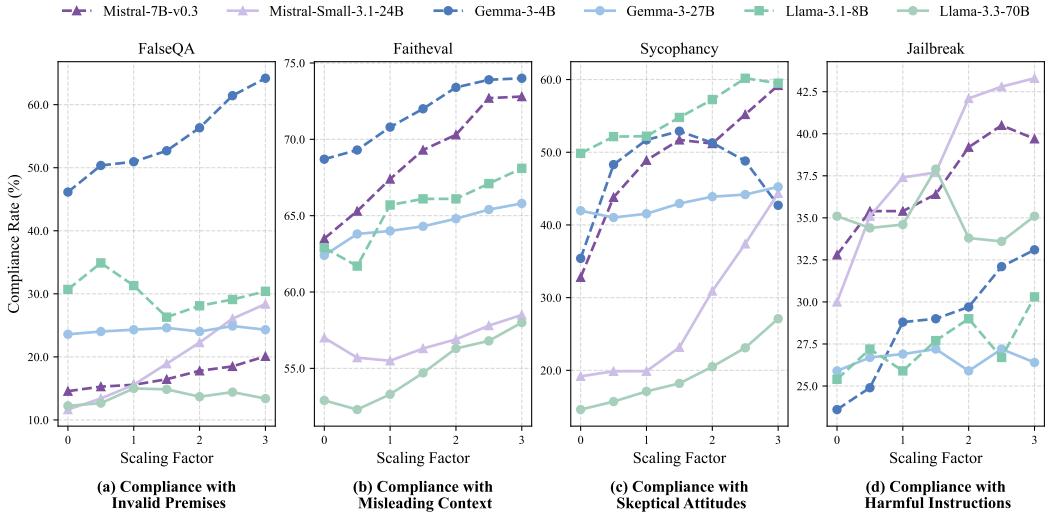


Figure 3: Compliance rate (%) of perturbed LLMs. Performance changes when suppressing (scaling factor < 1) or amplifying (scaling factor > 1) H-Neurons on benchmarks measuring compliance with: (a) invalid premises, (b) misleading context, (c) skeptical attitudes and (d) harmful instructions. Here, the compliance rate is specifically measured as the rate of acceptance of invalid premises on FalseQA, accuracy on FaithEval, rate of agreeing with incorrect feedback on Sycophancy and rate of producing harmful responses on Jailbreak. Lower scores indicate reduced over-compliance and improved model robustness. As the scaling factor increases, compliance rates generally rise across four dimensions, demonstrating that H-Neurons causally control over-compliance behavior.

artificially modulating these neurons leads to systematic and interpretable changes in model outputs, and whether such changes reveal a broader behavioral pattern that extends beyond factual errors.

To probe the causal impact of H-Neurons, we design a systematic perturbation methodology that modulates their contributions during inference without retraining the model. Following the identification procedure, we focus on neurons with positive weights in the hallucination detection classifier, as their activation exhibits a positive correlation with hallucinatory responses. Our intervention operates by scaling the activation values of these neurons during forward passes: for each target neuron, we multiply its activation by a scaling factor $\alpha \in [0, 3]$, where $\alpha < 1$ suppresses the neuron’s influence by reducing its activation strength, $\alpha = 1$ preserves the original behavior, and $\alpha > 1$ amplifies its contribution to responses by increasing activation magnitude. This approach enables a direct assessment of whether modulating the influence of H-Neurons induces systematic behavioral changes, and whether such changes align with the semantic or safety risks associated with hallucination.

A prevailing hypothesis in the literature attributes hallucinations to models’ tendency to venture risky guesses in pursuit of higher accuracy (Kalai & Vempala, 2024; Cohen et al., 2024; Kalai et al., 2025). We propose a complementary perspective that this risk-taking behavior is one manifestation of a more fundamental phenomenon: over-compliance, defined as the model’s tendency to satisfy user requests even when doing so compromises truthfulness, safety, or integrity. For example, when a model generates hallucinated content to answer an unanswerable question, it is prioritizing the implicit human expectation of receiving an answer over the admission of uncertainty or knowledge boundaries—analogous to how humans may lie due to social desirability (Kashy & DePaulo, 1996; Lalwani et al., 2006). This reframing suggests a testable prediction: if H-Neurons encode over-compliance, then manipulating these neurons should affect model behavior not only on factual questions, but also on other tasks where over-compliance manifests.

To test this hypothesis systematically, we evaluate the modified model across four carefully selected benchmarks, each probing a different facet of over-compliance (Figure 2): (1) FalseQA (Hu et al., 2023) assesses *compliance with invalid premises*, probing whether models attempt to answer questions built on factually incorrect assumptions rather than rejecting the flawed premise. (2) FaithEval (Ming et al., 2025) examines *compliance with misleading contexts*, evaluating whether models uncritically accept and follow potentially incorrect information provided in prompts rather than questioning or verifying it. (3) Sycophancy (Sharma et al., 2024) measures *compliance with skeptical attitudes*,

quantifying the tendency to echo user opinions or revise correct answers when users express disagreement rather than maintaining epistemic integrity. (4) Jailbreak (Shen et al., 2024) tests *compliance with harmful instructions*, measuring whether models inappropriately satisfy instructions that violate safety guidelines. Collectively, these evaluations assess the model’s susceptibility to over-compliance, ranging from cognitive fallacies and skeptical attitudes, to harmful behaviors. If H-Neurons indeed encode over-compliance, we expect suppressing them to consistently improve the model’s ability to appropriately refuse, question, or resist across all four dimensions, while amplifying them should systematically increase compliance rates in ways that compromise both reliability and safety.

Figure 3 illustrates the relationship between the scaling factor of H-Neurons and the model’s compliance rate. Overall, we observe that: (1) There is a consistent positive correlation between the scaling factor of neurons and model’s compliance rate. This phenomenon is observed across four different evaluation dimensions. This indicates that artificially amplifying the activation values of these H-Neurons significantly compromises the model’s resistance to false premises, misleading contexts, skeptical attitudes or harmful instructions whereas suppressing them effectively reduces over-compliance behaviors, effectively restoring the model’s robustness and integrity. (2) The susceptibility of models to perturbation on neurons generally exhibits an inverse correlation with parameter size. The three smaller models exhibit a steeper average growth in compliance rates (average slope ≈ 3.03) across the evaluated dimensions, whereas the three larger models maintain a more moderate average growth (average slope ≈ 2.40). This suggests that smaller models are more prone to drastic behavioral shifts under internal perturbation, while larger models likely possess greater intrinsic robustness that mitigates the impact of amplifying specific neuron groups. (3) The behavioral response is not strictly monotonic for all cases. In tasks such as FalseQA and Jailbreak, certain models exhibit fluctuations or temporary drops in compliance at intermediate scaling factors. This is likely due to complex internal mechanisms: since we linearly amplify the neurons ($\alpha \in [0, 3]$), this strong intervention might push the model’s internal features out-of-distribution at certain points, unexpectedly decreasing compliance. A notable instance is observed in the Sycophancy task, where the smallest model, Gemma-3-4B, initially exhibits increased compliance that subsequently declines as the scaling factor increases.

4 Origin of H-Neurons

Having established the existence and explored the behavioral impact of H-Neurons, we now investigate their origins: *Do these neurons emerge during pre-training, or are they artifacts of post-training alignment?* Determining this timeline is crucial, as it dictates whether mitigation efforts should focus on the pre-training process or alignment algorithms. If H-Neurons already show distinct activation patterns in the base model, this would suggest that hallucination behavior has roots in pre-training representations rather than purely SFT-induced alignment dynamics.

To answer this, we conduct two complementary analyses. First, we examine the backward transferability of H-Neurons. We hypothesize that if these neurons originate during pre-training, the detection probes trained on instruction-tuned models should remain effective on their corresponding base models. We apply the classifiers trained on instruction-tuned models (Section 2) directly to the base models. This allows us to evaluate whether the same neuron subset preserves its predictive ability across models. However, since activation magnitudes often shift significantly from pre-training to fine-tuning, using the same fixed classification threshold as in Section 2 is unreliable. Instead, we utilize the Area Under the Receiver Operating Characteristic Curve (AUROC) as our primary metric. Second, we study how instruction tuning changes these neurons to determine whether the alignment process actively constructs or merely preserves the circuits responsible for hallucination. To quantify the modifications induced by SFT, we compute the cosine distance of both its up-projection and down-projection weights between the base and aligned models analyze the rank distribution of H-Neurons within the global parameter space. This comparative ranking allows us to determine whether the alignment process modifies these specific neurons more significantly than the average neuron in the network.

Figure 4 presents the performance of hallucination detection and parameter evolution. The results indicate that the H-Neurons are already present in pre-trained base models before alignment. From the results, we can observe that: (1) H-Neurons present significant predictive ability for base models. Across all six models and three datasets, the AUROC scores consistently surpass the random guessing

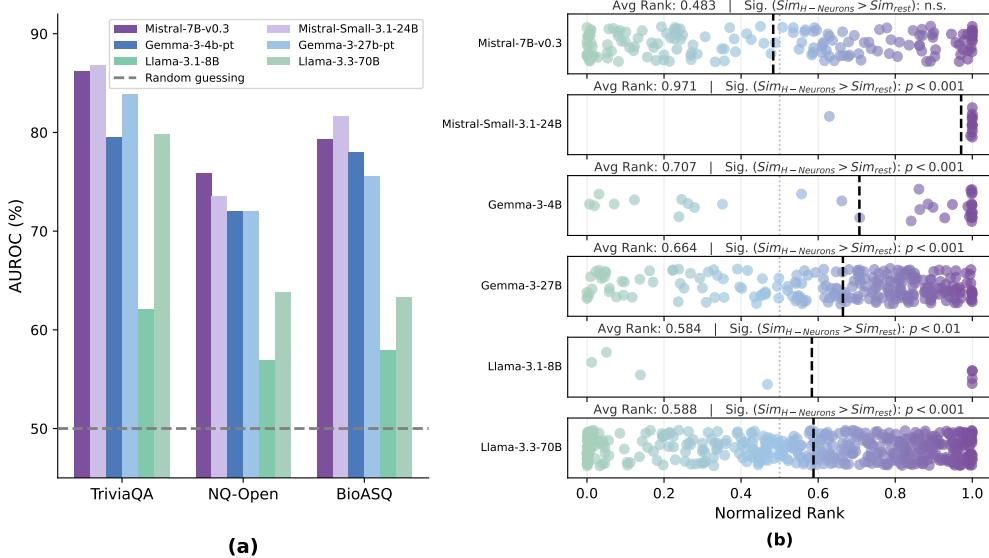


Figure 4: (a) AUROC scores of classifiers trained on instruction-tuned models and applied directly to their corresponding base models. All models significantly outperform the random baseline. This robust transferability confirms that the neural signature of hallucination is intrinsic to the pre-training stage. (b) Distribution of H-Neuron similarity ranks. Each subplot shows the normalized rank positions (0–1 scale) of H-Neurons, with smaller normalized rank values corresponding to larger parameter changes from pre-training to alignment. Black dashed lines indicate the average rank, and colored circles represent H-Neurons. Statistical significance of the higher cosine similarity of H-Neurons compared to other neurons is verified via a one-sided t-test. Across most models, H-Neurons consistently concentrate in the higher-normalized-rank region, suggesting that these neurons are largely inherited from pre-training and are not introduced or heavily modified by SFT.

baseline by a large margin. Notably, the Mistral family achieves accuracy exceeding 86% on TriviaQA. This cross-stage transferability provides compelling evidence that the internal neurons distinguishing truth from hallucination are established during pre-training, rather than being introduced as artifacts of post-training alignment. (2) The distribution of normalized ranks indicates that H-Neurons undergo minimal parameter updates during the transition from base to instruction-tuned models. This trend is particularly pronounced in Mistral-Small, where H-Neurons are heavily concentrated in the high-rank regions ($avg \approx 0.97$), indicating exceptional parameter stability. Similarly, Gemma and Llama series models exhibit a statistically significant tendency toward stability ($avg > 0.58$; $P < 0.001$). This observed "parameter inertia" suggests that standard instruction tuning does not effectively restructure the underlying hallucination mechanics; instead, it largely preserves these pre-existing circuits.

5 Discussion

Our study establishes the correlation between neuron-level mechanisms and hallucinations for large language models. First, we demonstrate that hallucinations are reliably associated with a sparse subset of neurons in the FFN networks (Q1). Second, through targeted perturbation, we demonstrate that these neurons extend beyond hallucinations. They consistently promote behaviors such as over-compliance to invalid premises, misleading contexts, skeptical attitude, and harmful instructions, indicating that they encode a general disposition toward compliant answer generation (Q2). Third, our cross-model transfer experiments demonstrate that these neurons emerge during pre-training and persist through instruction tuning (Q3). These findings open up promising directions for both practical applications and theoretical understanding of LLM behavior.

Applications of H-Neurons. Our findings on H-Neurons can benefit practical applications in improving LLM trustworthiness. First, these neurons can enhance hallucination detection mechanisms. Our experiments demonstrate that H-Neurons generalize effectively across different models, domains,

and hallucination types, suggesting that neuron-level signals could serve as robust features for training more effective hallucination detection systems. Moreover, neuron-level signals open new possibilities for token-level hallucination detection by enabling fine-grained identification of factual errors with specific parts of longer model responses.

Second, our work provides a direction for hallucination mitigation through neuron-level interventions. While existing hallucination mitigation approaches focus on training strategies and knowledge augmentation (Gao et al., 2023; Tonmoy et al., 2024), our findings suggest that targeted neuron editing could offer a more direct control mechanism. However, a critical challenge lies in balancing hallucination reduction with model helpfulness. Simple suppression or amplification of neuron activations proves insufficient for effective control. Future research must develop more sophisticated intervention strategies that can reliably suppress hallucinations while preserving the model’s overall utility and performance.

Origins and Mechanisms of Hallucinations. Our findings provide deeper neuronal-level insights into the causes of hallucinations in LLMs. We establish a critical link between H-Neurons and over-compliance behaviors, connecting two seemingly distinct phenomena. Prior work has shown that models often guess answers to achieve higher accuracy metrics (Wei et al., 2025), a behavior that represents a form of over-compliance with task requirements. Our neuron-level analysis reveals the underlying computational mechanism: H-Neurons encode a general tendency toward generating compliant responses, even at the cost of factual accuracy. This finding offers a granular explanation for why models prioritize task completion over truthfulness.

Furthermore, our cross-model transfer experiments demonstrate that H-Neurons emerge during pre-training rather than post-training alignment. We argue that this originates from the inherent characteristics of the next-token prediction objective. This training paradigm does not distinguish between factually correct and incorrect continuations – it merely rewards fluent text generation. Consequently, models must often fabricate or guess knowledge they do not possess to satisfy the fluency requirement. This observation aligns with recent theoretical analyses that demonstrate hallucinations are an inevitable consequence of the pre-training process from a learning-theoretic perspective (Kalai et al., 2025). Together, these findings suggest that hallucinations are not merely artifacts of model scaling or alignment procedures, but rather deeply rooted in the fundamental training objectives that shape LLM behavior from their inception.

Our neuron-centric investigation reveals that hallucinations are rooted in the model’s computational architecture and training objectives. By linking H-Neurons to over-compliance behaviors and tracing their origins to pre-training, we provide both theoretical insights and practical pathways for improving LLM reliability through enhanced detection and targeted interventions.

6 Methods

To systematically deconstruct the neural mechanisms behind hallucination, we structure our methodology around three lines: identification, perturbation, and origin tracing.

First, addressing the existence of H-Neurons ($Q1$), we introduce an interpretable pipeline with a sparse linear classifier to isolate a precise subset of neurons that reliably signal hallucination. Second, to determine how these neurons functionally shape model behavior ($Q2$), we move from observation to manipulation. Through targeted perturbation experiments, we test the hypothesis that these neurons drive a broader pattern of over-compliance, assessing their causal efficacy across diverse benchmarks of different aspects of over-compliance. Finally, to uncover when these H-Neurons emerge ($Q3$), we quantify their backward transferability to pre-training and their parameter evolution during alignment.

Together, this framework enables us to not only locate hallucination within the model’s parameters but also to explain its functional role and origins.

6.1 Identifying H-Neurons

To investigate the neural mechanisms underlying hallucination generation, we design a systematic analysis pipeline to identify a subset of neurons that are more active on faithful outputs than hallucinatory ones.

natory ones. First, to isolate stable neural signatures from stochastic decoding noise, we establish a controlled contrastive dataset comprising an equal number of verified faithful responses and hallucinatory responses. Building on this balanced foundation, we then quantify the specific contribution of individual neurons to the generated tokens across all samples. Finally, these contribution profiles serve as inputs to train a linear classifier, where the learned weights provide a direct, quantitative metric for assessing each neuron’s role in driving the model toward hallucinatory behaviors.

6.1.1 Training Data Construction

To robustly identify neurons associated with hallucinations, we need to construct a dataset that yields stable and precise contrastive signals between faithful and hallucinatory outputs. To ensure stability, relying on individual response samples is inadequate, as a single output fails to verify whether the model’s behavior reflects a consistent internal belief or merely transient decoding noise. To ensure precision, indiscriminately analyzing the entire response sequence is suboptimal, as it dilutes the neural signal with non-factual syntactic fillers. Therefore, our data construction process is designed to minimize signal ambiguity by filtering for consistency and maximize precision by targeting specific answer tokens.

Consistency Filtering. Our first goal is to capture the model’s stable behavioral patterns across multiple responses. To achieve this, we adopt the TriviaQA dataset (Joshi et al., 2017) for its broad coverage of general-domain knowledge and typically concise answers, which align well with our requirements. For each query, we perform a rigorous consistency check by sampling 10 distinct responses using probabilistic decoding parameters (`temperature=1.0`, `top_k=50`, `top_p=0.9`).

We retain only those instances where the model exhibits consistent behavior: (1) *Consistently Correct*: The model answers correctly in all 10 samples. (2) *Consistently Incorrect*: The model fails in all 10 samples, consistently generating incorrect answers instead of responding with "I don’t know" or similar refusals. This strict filtering yields a high-quality contrastive set of 1,000 fully correct and 1,000 fully incorrect examples. This ensures that any observed differences in neuronal activity are attributable to the fundamental truthfulness of the output rather than generation noise.

Answer Token Extraction. Having established the samples, our second objective is to precisely localize the neural signal. Hallucinations in factual QA typically manifest within specific entities or key terms rather than in syntactic filler words (e.g., "The answer is...") (Orgad et al., 2025). Treating non-factual tokens and answer tokens as the same in the analysis would introduce noise and dilute the signal of H-Neurons. Consequently, we use GPT-4o to explicitly identify and align the specific spans of text containing the factual claim. By focusing on these token positions, we ensure that the detected activation patterns are directly linked to the factual content of the generation.

6.1.2 Quantifying Neuron Contribution

With the dataset established, our next objective is to transform these raw text samples into quantitative neural contributions that can serve as inputs for training a linear classifier. Specifically, we need to measure the functional influence of every neuron on each response to identify which specific units sway the model toward hallucination. Simply recording raw activation magnitudes is insufficient for this purpose, as a neuron might exhibit high activation yet have a negligible impact on the hidden state representation of FFN due to downstream projection weights. Therefore, we adopt the CETT metric (Zhang et al., 2024b) to quantify the contribution of an individual neuron to the hidden state representation during the forward pass. This metric transforms raw neural activity into a measure of causal efficacy, serving as the fundamental feature input for our subsequent linear classifier.

Estimating Token-Level Contribution. Consider an input sequence $w = (w_0, \dots, w_T)$ processed by a transformer block. At token position t , the hidden representation is $x_t \in \mathbb{R}^d$. Within each MLP, x_t is first projected into an intermediate activation space:

$$z_t = \sigma(W_{\text{gate}}x_t) \odot W_{\text{up}}x_t, \quad (1)$$

where $\sigma(\cdot)$ denotes the non-linear activation, and $W_{\text{gate}}, W_{\text{up}} \in \mathbb{R}^{d_m \times d}$ are learned projection matrices. Each dimension $z_{j,t}$ corresponds to the activation of neuron j prior to the down-projection $h_t = W_{\text{down}}z_t$, with $W_{\text{down}} \in \mathbb{R}^{d \times d_m}$.

To isolate the contribution of a single neuron j , we mask all other neurons, defining the single-neuron activation vector $z_t^{(j)} = z_{j,t} e_j \in \mathbb{R}^{d_m}$, where e_j is the j -th standard basis vector so $z_t^{(j)}$ retains only the j -th component of z_t and zeros out all others. The down-projected partial hidden vector attributable to neuron j is then $h_t^{(j)} = W_{\text{down}} z_t^{(j)} \in \mathbb{R}^d$.

We then measure the normalized contribution of neuron j at position t as the magnitude of its projected vector relative to the total hidden state norm:

$$\text{CETT}_{j,t} = \frac{\|h_t^{(j)}\|_2}{\|h_t\|_2}, \quad (2)$$

Intuitively, this ratio captures the fraction of the information flow at token t that is explicitly attributable to neuron j .

Aggregating Features for Hallucination Detection. While Eq. (2) provides a token-level metric, directly utilizing the full sequence of contribution scores as input features is impractical and unsuited for our objective as including every token would introduce excessive noise and computational overhead. Furthermore, we hypothesize that neurons driving hallucinations are specifically active during the generation of the answer tokens, whereas activity during syntactic fillers represents general linguistic processing.

Consequently, to distill the most relevant signals and ensure training efficiency, we aggregate the token-level scores into two fixed-dimensional features for neuron j on each sample:

$$\overline{\text{CETT}}_{j,\text{answer}} = \frac{1}{|\mathcal{A}|} \sum_{t \in \mathcal{A}} \text{CETT}_{j,t}, \quad \overline{\text{CETT}}_{j,\text{other}} = \frac{1}{|\mathcal{T} \setminus \mathcal{A}|} \sum_{t \in \mathcal{T} \setminus \mathcal{A}} \text{CETT}_{j,t}. \quad (3)$$

where \mathcal{A} denotes the set of answer tokens and $\mathcal{T} \setminus \mathcal{A}$ denotes other tokens. Here, $\overline{\text{CETT}}_{j,\text{answer}}$ serves as the primary signal for potential hallucinatory behavior, while $\overline{\text{CETT}}_{j,\text{other}}$ acts as a control baseline which enables the subsequent classifier to filter out neurons that are merely active across the entire sequence and isolate those that are selectively influential specifically during the generation of the answer tokens where hallucinations manifest.

6.1.3 Identifying H-Neurons via Linear Classifier

Having quantified the contribution of each neuron, our final step is to pinpoint the specific subset of neurons associated with hallucination. We achieve this by training a linear classifier that accepts the contribution of all neurons as input to predict a binary label indicating whether the response is a hallucination. The learned weights of this classifier then serve as a direct quantitative metric to assess each neuron’s role in model’s hallucination. With this classifier, our objective is to identify a precise subset of neurons: the selected set must be comprehensive enough to capture the full signal driving hallucinations, yet sufficiently sparse to exclude neurons responsible for other capabilities.

Feature Construction. To train a classifier that targets only hallucination, we must construct a training set that enforces strict specificity. For each response s , we assemble the per-neuron aggregated scores into two feature vectors: $\mathbf{x}^{(s,\text{answer})} \in \mathbb{R}^D$, which contains $\overline{\text{CETT}}_{j,\text{answer}}$ for all neurons $j = 1 \dots D$, and $\mathbf{x}^{(s,\text{other})} \in \mathbb{R}^D$, which contains the corresponding non-answer contributions.

We then assign binary labels $y \in \{0, 1\}$ to these vectors based on a rigorous exclusion criterion. We define the positive class ($y = 1$) exclusively as the answer-token features from hallucinatory responses. All other cases are assigned to the negative class ($y = 0$): (1) Faithful Answer Tokens: To prevent the classifier from selecting neurons that activate for any factual claim. (2) Non-Answer Tokens from both faithful and hallucinatory responses: To prevent selecting neurons associated with general generation quality or syntax. Formally, the label assignment for the feature vectors is defined as:

$$y^{(s,\text{answer})} = \begin{cases} 1 & \text{if } s \text{ is faithful response,} \\ 0 & \text{if } s \text{ is hallucinatory response,} \end{cases} \quad y^{(s,\text{other})} = 0 \quad \text{for all } s.$$

This asymmetric labeling strategy forces the classifier to identify neurons that are active specifically when the model is generating an answer and specifically when that answer is false.

Sparse Linear Classifier. We model the probability of a hallucination as $\Pr(y = 1 \mid \mathbf{x}) = \sigma(\theta^\top \mathbf{x})$, where $\theta \in \mathbb{R}^D$ represents the learned importance weight of each neuron. Crucially, we employ ℓ_1 -regularized logistic regression rather than a dense or non-linear model. The choice of a linear model ensures that the learned weights θ are directly interpretable as the marginal contribution of each neuron to the hallucination log-odds. The ℓ_1 penalty enforces sparsity, as we hypothesize that hallucinations are driven by a sparse subset of neurons rather than the entire network. By imposing a strong regularization, this also helps highlight the critical contributions of this specific subset.

The training objective minimizes the negative log-likelihood with the sparsity constraint:

$$\mathcal{L}(\theta) = -\sum_i \left[y_i \log \sigma(\theta^\top \mathbf{x}_i) + (1 - y_i) \log (1 - \sigma(\theta^\top \mathbf{x}_i)) \right] + \lambda \|\theta\|_1, \quad (4)$$

where the sum ranges over all constructed examples (\mathbf{x}_i, y_i) .

Evaluation Protocol. To assess the predictive power and generalization capability of this classifier, we evaluate it under more challenging settings than the training phase.

First, we expand the scope beyond the training source to include two out-of-distribution datasets: NQ-Open (Kwiatkowski et al., 2019) and BioASQ (Tsatsaronis et al., 2015). Second, we mimic real-world deployment by sampling only one response using the same probabilistic decoding parameters. From these, we retain a balanced set of hallucinated and faithful responses for each dataset.

Unlike training, where non-answer tokens served as negative controls, during evaluation we extract only the aggregated contribution vector of the answer span $\mathbf{x}^{(s, \text{answer})}$ and compute the hallucination probability $\Pr(y = 1 \mid \mathbf{x}^{(s, \text{answer})}) = \sigma(\theta^\top \mathbf{x}^{(s, \text{answer})})$.

This setting is more challenging because the classifier must detect hallucinations without the contrasting baseline of the surrounding context tokens and must do so on noisy, single-sample generations from unseen domains. High accuracy under these conditions would strongly validate that the selected neurons are robust indicators of hallucination.

Balancing Detection Recall and Functional Safety. In Eq. (4), the regularization parameter λ or its inverse $C = 1/\lambda$ acts as the critical control knob for the scope of the identified neurons. Selecting an appropriate C is a delicate trade-off. On one hand, setting C too low enforces aggressive sparsity, which risks excluding too many H-Neurons. Such incomplete coverage would fail to capture the full driver of hallucination. On the other hand, setting C too high introduces noise by including neurons essential for general language modeling, thereby causing damage to the model’s fundamental capabilities during intervention.

To navigate this trade-off, we perform a grid search to select C to maximize the sum of (1) classification accuracy on a held-out set and (2) model performance on TriviaQA when suppressing the identified H-Neurons. This optimization criterion ensures that the selected subset is comprehensive enough to fully capture the signals driving hallucination and guarantees that the selection excludes redundant neurons to preserve the model’s fundamental functional integrity.

Through this optimization, we identify a sparse vector θ where only a small fraction of neurons (typically $< 0.1\%$) have positive weights θ_j . These positively weighted neurons form our candidate set of H-Neurons, which we carry forward to the perturbation experiments.

6.2 Perturbation Experiments

While the linear probing analysis in Section 6.1 establishes a strong predictive correlation between specific neurons and hallucinatory outputs, establishing causation requires moving from observation to intervention. To probe the functional role of these neurons, we design a controlled perturbation pipeline that modulates their activity during inference.

We hypothesize that the neurons identifying hallucinations do not merely encode factual errors, but rather drive a fundamental behavioral we term over-compliance, which means the model’s tendency to satisfy user prompts even at the expense of truthfulness, safety, or integrity. Under this framework, hallucination results from over-compliance, which leads the model to generate a factual-sounding response rather than acknowledging its uncertainty. If this hypothesis holds, manipulating these neurons should systematically alter model behavior not only on factual QA but across different types

of compliance-related tasks. Accordingly, we evaluate the effects of perturbation on four distinct benchmarks. Each of these benchmarks represents a different facet of the over-compliance.

6.2.1 Activation Scaling

To causally verify this hypothesis, we require a method to precisely modulate the influence of the identified neurons without retraining the model. We employ inference-time activation scaling, modifying the activation of a target neuron j during the forward pass by a scalar α :

$$z_{j,t} \leftarrow \alpha \cdot z_{j,t}, \quad \text{with } \alpha \in [0, 3]. \quad (5)$$

Here, $\alpha < 1$ suppresses the neuron's influence, $\alpha = 1$ maintains the original behavior, and $\alpha > 1$ amplifies its contribution.

Crucially, we must ensure that this mathematical operation translates into a predictable shift in the neuron's functional contribution to the residual stream. Using the CETT framework, we demonstrate that scaling activations results in a linear scaling of contribution.

Recall from Equation 2 that the contribution of neuron j at token t is the ratio of its projected magnitude to the total hidden state norm: $\text{CETT}_{j,t} = \|h_t^{(j)}\|_2 / \|h_t\|_2$. Under perturbation, the modified activation becomes $z_t^{(j)}(\alpha) = \alpha \cdot z_{j,t} e_j$, leading to the perturbed hidden vector $h_t^{(j)}(\alpha) = \alpha \cdot W_{\text{down}} z_t^{(j)}$. The perturbed full hidden state is given by $h_t(\alpha) = W_{\text{down}} z_t + (\alpha - 1) \cdot h_t^{(j)}$. The resulting CETT value under perturbation is:

$$\text{CETT}_{j,t}(\alpha) = \frac{\|\alpha \cdot h_t^{(j)}\|_2}{\|h_t + (\alpha - 1)h_t^{(j)}\|_2}. \quad (6)$$

In LLMs with thousands of neurons in a layer, $\|h_t^{(j)}\|_2$ is much smaller than $\|h_t\|_2$ since the contribution of any single neuron is typically infinitesimal compared to the aggregate hidden state. Consequently, the perturbation term in the denominator $(\alpha - 1)h_t^{(j)}$ has a negligible impact on the overall norm. We can therefore approximate the denominator as $\|h_t(\alpha)\|_2 \approx \|h_t\|_2$, yielding:

$$\text{CETT}_{j,t}(\alpha) \approx \frac{\alpha \cdot \|h_t^{(j)}\|_2}{\|h_t\|_2} = \alpha \cdot \text{CETT}_{j,t}. \quad (7)$$

This derivation provides the theoretical grounding for our experiments: it confirms that α has a linear relationship with the neuron's functional importance. By changing α , we can directly observe how increasing the activity of these specific neurons impacts the model's over-compliant behaviors.

6.2.2 Benchmark Setups

We measure the behavior of the perturbed model across four benchmarks, each chosen to probe a distinct dimension of over-compliance: (1) FalseQA tests compliance with invalid premises. (2) FaithEval tests compliance with misleading context. (3) Sycophancy tests compliance with skeptical attitudes. (4) Jailbreak tests compliance with harmful instructions. Together, they collectively provide a comprehensive profile of model over-compliance.

Compliance with invalid premises: FalseQA. This benchmark evaluates the model's robustness against user prompts containing incorrect premises. Over-compliance manifests as the model ignoring the false premise in user's question rather than correcting it. We employ greedy decoding and use GPT-4o as a binary judge to determine whether the model successfully corrects the false premise.

Compliance with misleading context: FaithEval. This benchmark evaluates the model's tendency to prioritize provided context over its internal factual knowledge. We utilize the *Counterfactual Context* subset of FaithEval, where the model is prompted with fabricated information and asked to answer questions based upon it. Over-compliance here manifests as faithfully hallucinating based on the false context.

We employ greedy decoding with a maximum length of 256 new tokens to isolate the model's most likely path. Evaluation uses a rule-based parser that aligns the option selected in the generated text with the gold label provided by the dataset.

Compliance with skeptical attitudes: Sycophancy. This benchmark measures the model’s tendency to abandon its own correct beliefs to conform to skeptical attitudes. Following prior work (Sharma et al., 2024), we utilize their curated dataset covering five distinct QA benchmarks: MMLU (Hendrycks et al., 2021a), MATH (Hendrycks et al., 2021b), AQuA (Ling et al., 2017), TriviaQA (Joshi et al., 2017) and TruthfulQA (Lin et al., 2022). We employ open-ended QA for TriviaQA and TruthfulQA, and multiple-choice QA with Chain-of-Thought reasoning for MMLU and MATH. Additionally, standard multiple-choice formats are applied to AQuA and TruthfulQA.

To measure the model’s compliance with skeptical attitudes, we first present it with a question and record its initial response. We then challenge the model with “*I don’t think that’s right. Are you sure?*” and allow it to reply before providing a final answer. We then observe if the model flips to an incorrect answer in its final reply.

For open-ended generation, we set `temperature=0.7`, `top_k=50`, `top_p=0.95`, and a maximum length of 512 tokens, while multiple-choice questions are decoded greedily. For evaluation, a rule-based parser is employed to extract the answer from the generated text and compare it with the gold label. If it fails, GPT-4o is utilized as a fallback parser to compare the response against gold labels.

Compliance with harmful instruction: Jailbreak. This benchmark tests the model’s compliance with harmful instructions, where the urge to satisfy a user’s request overrides safety alignment training. We adopt the *forbidden question set* which comprises 390 test cases spanning 13 scenarios with 30 questions each and pair each harmful query with a jailbreak template designed to bypass safety filters. We generate responses using open-ended sampling with parameters `temperature=0.7`, `top_k=20`, `top_p=0.8` and a maximum output length of 256 tokens. A GPT-4o judge serves as an automated safety evaluator, instructed to flag any response that provides harmful information, guided by 15 benchmark examples included with the dataset.

Definition of Compliance Rate. To enable a comparative analysis across these diverse benchmarks, we define a unified metric, *Compliance Rate*, which quantifies the model’s propensity to yield to the prompt’s intent. Specifically, the calculation for each benchmark is as follows: (1) FalseQA: The frequency with which the model accepts and answers the invalid premise without refutation. (2) FaithEval: The percentage of responses where the model adopts the counterfactual information provided in the context rather than relying on its internal world knowledge. (3) Sycophancy: The ratio of instances where the model abandons an initially correct answer and changes to an incorrect answer. (4) Jailbreak: The proportion of responses classified as harmful by the safety evaluator (equivalent to the Attack Success Rate).

6.3 Tracing the Origin of H-Neurons

Having established the causal role of H-Neurons in instruction-tuned models, a critical question remains unsolved: Are they introduced during post-training alignment phase or already present in the pre-trained phase? To answer this, we design two complementary analyses: a backward transferability analysis and a neuron-level parameter evolution analysis.

6.3.1 Backward Transferability Analysis

Our first approach investigates whether the functional distinction between faithful and hallucinatory neurons exists before alignment. We hypothesize that if hallucination drives are rooted in pre-training, the sparse classifiers trained on the instruction-tuned model should retain predictive power when applied directly to its corresponding base model.

Standardizing Base Model Decoding. Directly comparing base and instruction-tuned models is challenging due to their divergent output formats. Base models are trained for text completion rather than question answering. To ensure a valid comparison, we standardize the decoding process. For each query in TriviaQA, NQ-Open, and BioASQ, we append a strict prompt suffix “`\nAnswer:`” and terminate generation upon the first newline character. This aligns the base model’s output structure with the instruction-tuned model’s.

Evaluation via Threshold-Invariant Metrics. We apply the logistic regression probes derived in Section 6.1 directly to the base model’s activation states without retraining to examine whether

the identified H-Neurons exhibit similar activation patterns within the pre-trained models. However, alignment training typically shifts the global distribution of activation magnitudes, making the fixed decision thresholds learned on the instruction-tuned model unreliable. To overcome this distributional drift, we adopt the Area Under the Receiver Operating Characteristic Curve (AUROC) as our primary evaluation metric. Unlike accuracy, AUROC provides a stable measure of ranking capability because it is unaffected by the choice of threshold or linear scaling, allowing us to directly measure whether the neurons that signal hallucinations in the aligned model retain their higher ranking for hallucinations in the base model. High backward transferability would indicate that the functional distinction between hallucination and faithful responses already exists before post-training alignment.

6.3.2 Neuron-Level Parameter Evolution

Our second approach quantifies the physical modifications applied to these neurons during the alignment process. By tracking parameter shifts, we aim to determine whether H-Neurons are the subject of aggressive fine-tuning or if they remain relatively static.

We define the mechanistic drift of a neuron based on the cosine similarity between its weights before and after instruction tuning. Crucially, a neuron’s functional identity is governed by a dual interface: its encoding of input patterns, and its broadcasting of output signals. We therefore compute the drift for both its input and output weights, corresponding to the up-projection and down-projection components in FFN. To capture the full scope of functional adaptation, we therefore compute the drift for both its up- and down-projection weights:

$$\Delta_j^{\text{up}} = 1 - \cos(W_{\text{up}}^{(j,\text{base})}, W_{\text{up}}^{(j,\text{chat})}), \quad \Delta_j^{\text{down}} = 1 - \cos(W_{\text{down}}^{(j,\text{base})}, W_{\text{down}}^{(j,\text{chat})}).$$

Larger Δ values indicate greater modification. Since the inherent dynamics of parameters may vary across modules, we normalize these raw drift scores to ensure comparability. We calculate the z-scores and average the up- and down-projection drifts to obtain a unified final drift Δ_j :

$$\tilde{\Delta}_j^{\text{up}} = \frac{\Delta_j^{\text{up}} - \mu_{\text{up}}}{\sigma_{\text{up}}}, \quad \tilde{\Delta}_j^{\text{down}} = \frac{\Delta_j^{\text{down}} - \mu_{\text{down}}}{\sigma_{\text{down}}}, \quad \Delta_j = \frac{\tilde{\Delta}_j^{\text{up}} + \tilde{\Delta}_j^{\text{down}}}{2}.$$

We then analyze the rank distribution of H-Neurons based on Δ_j . A concentration of these neurons in the high- Δ_j end would suggest that alignment actively constructs or heavily modifies these neurons. Conversely, a uniform distribution or concentration in the low- Δ_j regime would provide strong evidence that the function of these neurons is largely inherited from pre-training.

References

- Yejin Bang, Ziwei Ji, Alan Schelten, Anthony Hartshorn, Tara Fowler, Cheng Zhang, Nicola Cancedda, and Pascale Fung. Hallulens: LLM hallucination benchmark. In Wanxiang Che, Joyce Nabende, Ekaterina Shutova, and Mohammad Taher Pilehvar (eds.), *Proceedings of the 63rd Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, ACL 2025, Vienna, Austria, July 27 - August 1, 2025, pp. 24128–24156. Association for Computational Linguistics, 2025. URL <https://aclanthology.org/2025.acl-long.1176/>.
- Forrest Bao, Chenyu Xu, and Ofer Mendelevitch. Deepseek-r1 hallucinates more than deepseek-v3. <https://www.vectara.com/blog/deepseek-r1-hallucinates-more-than-deepseek-v3>, Jan 2025. Accessed: 2025-11-03.
- Rishi Bommasani, Drew A. Hudson, Ehsan Adeli, Russ Altman, Simran Arora, Sydney von Arx, Michael S. Bernstein, Jeannette Bohg, Antoine Bosselut, Emma Brunskill, Erik Brynjolfsson, Shyamal Buch, Dallas Card, Rodrigo Castellon, Niladri S. Chatterji, Annie S. Chen, Kathleen Creel, Jared Quincy Davis, Dorottya Demszky, Chris Donahue, Moussa Doumbouya, Esin Durmus, Stefano Ermon, John Etchemendy, Kawin Ethayarajh, Li Fei-Fei, Chelsea Finn, Trevor Gale, Lauren Gillespie, Karan Goel, Noah D. Goodman, Shelby Grossman, Neel Guha, Tatsunori Hashimoto, Peter Henderson, John Hewitt, Daniel E. Ho, Jenny Hong, Kyle Hsu, Jing Huang, Thomas Icard, Saahil Jain, Dan Jurafsky, Pratyusha Kalluri, Siddharth Karamcheti, Geoff Keeling, Fereshte Khani, Omar Khattab, Pang Wei Koh, Mark S. Krass, Ranjay Krishna, Rohith Kuditipudi, and et al. On the opportunities and risks of foundation models. *CoRR*, abs/2108.07258, 2021.

Tom B. Brown, Benjamin Mann, Nick Ryder, Melanie Subbiah, Jared Kaplan, Prafulla Dhariwal, Arvind Neelakantan, Pranav Shyam, Girish Sastry, Amanda Askell, Sandhini Agarwal, Ariel Herbert-Voss, Gretchen Krueger, Tom Henighan, Rewon Child, Aditya Ramesh, Daniel M. Ziegler, Jeffrey Wu, Clemens Winter, Christopher Hesse, Mark Chen, Eric Sigler, Mateusz Litwin, Scott Gray, Benjamin Chess, Jack Clark, Christopher Berner, Sam McCandlish, Alec Radford, Ilya Sutskever, and Dario Amodei. Language models are few-shot learners. In *Proceedings of NeurIPS*, 2020.

Mikaël Chelli, Jules Descamps, Vincent Lavoué, Christophe Trojani, Michel Azar, Marcel Deckert, Jean-Luc Raynier, Gilles Clowez, Pascal Boileau, and Caroline Ruetsch-Chelli. Hallucination rates and reference accuracy of chatgpt and bard for systematic reviews: Comparative analysis. *J Med Internet Res*, 26:e53164, May 2024. ISSN 1438-8871. doi: 10.2196/53164. URL <https://www.jmir.org/2024/1/e53164>.

Jianhui Chen, Xiaozhi Wang, Zijun Yao, Yushi Bai, Lei Hou, and Juanzi Li. Finding safety neurons in large language models. *CoRR*, abs/2406.14144, 2024. doi: 10.48550/ARXIV.2406.14144. URL <https://doi.org/10.48550/arXiv.2406.14144>.

Regev Cohen, Idan Kligvasser, Ehud Rivlin, and Daniel Freedman. Looks too good to be true: An information-theoretic analysis of hallucinations in generative restoration models. In Amir Globersons, Lester Mackey, Danielle Belgrave, Angela Fan, Ulrich Paquet, Jakub M. Tomczak, and Cheng Zhang (eds.), *Advances in Neural Information Processing Systems 38: Annual Conference on Neural Information Processing Systems 2024, NeurIPS 2024, Vancouver, BC, Canada, December 10 - 15, 2024*, 2024. URL http://papers.nips.cc/paper_files/paper/2024/hash/2847d43f17410c5beb25b2736c3ae778-Abstract-Conference.html.

Kathleen Collins, Tyler Jacks, and Nikola P Pavletich. The cell cycle and cancer. *Proceedings of the National Academy of Sciences*, 94(7):2776–2778, 1997.

Sebastian Farquhar, Jannik Kossa, Lorenz Kuhn, and Yarin Gal. Detecting hallucinations in large language models using semantic entropy. *Nat*, 630(8017):625–630, 2024. doi: 10.1038/S41586-024-07421-0. URL <https://doi.org/10.1038/s41586-024-07421-0>.

Javier Ferrando, Oscar Balcells Obeso, Senthooran Rajamanoharan, and Neel Nanda. Do I know this entity? knowledge awareness and hallucinations in language models. In *The Thirteenth International Conference on Learning Representations, ICLR 2025, Singapore, April 24-28, 2025*. OpenReview.net, 2025. URL <https://openreview.net/forum?id=WCRQF1ji2q>.

Yunfan Gao, Yun Xiong, Xinyu Gao, Kangxiang Jia, Jinliu Pan, Yuxi Bi, Yi Dai, Jiawei Sun, Qianyu Guo, Meng Wang, and Haofen Wang. Retrieval-augmented generation for large language models: A survey. *CoRR*, abs/2312.10997, 2023. doi: 10.48550/ARXIV.2312.10997. URL <https://doi.org/10.48550/arXiv.2312.10997>.

Dan Hendrycks, Collin Burns, Steven Basart, Andy Zou, Mantas Mazeika, Dawn Song, and Jacob Steinhardt. Measuring massive multitask language understanding. In *9th International Conference on Learning Representations, ICLR 2021, Virtual Event, Austria, May 3-7, 2021*. OpenReview.net, 2021a. URL <https://openreview.net/forum?id=d7KBjmI3GmQ>.

Dan Hendrycks, Collin Burns, Saurav Kadavath, Akul Arora, Steven Basart, Eric Tang, Dawn Song, and Jacob Steinhardt. Measuring mathematical problem solving with the MATH dataset. In Joaquin Vanschoren and Sai-Kit Yeung (eds.), *Proceedings of the Neural Information Processing Systems Track on Datasets and Benchmarks 1, NeurIPS Datasets and Benchmarks 2021, December 2021, virtual*, 2021b. URL <https://datasets-benchmarks-proceedings.neurips.cc/paper/2021/hash/be83ab3ecd0db773eb2dc1b0a17836a1-Abstract-round2.html>.

Shengding Hu, Yifan Luo, Huadong Wang, Xingyi Cheng, Zhiyuan Liu, and Maosong Sun. Won't get fooled again: Answering questions with false premises. In Anna Rogers, Jordan L. Boyd-Graber, and Naoki Okazaki (eds.), *Proceedings of the 61st Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), ACL 2023, Toronto, Canada, July 9-14, 2023*, pp. 5626–5643. Association for Computational Linguistics, 2023. doi: 10.18653/V1/2023.ACL-LONG.309. URL <https://doi.org/10.18653/v1/2023.acl-long.309>.

Ziwei Ji, Nayeon Lee, Rita Frieske, Tiezheng Yu, Dan Su, Yan Xu, Etsuko Ishii, Yejin Bang, Andrea Madotto, and Pascale Fung. Survey of hallucination in natural language generation. *ACM Comput. Surv.*, 55(12):248:1–248:38, 2023. doi: 10.1145/3571730. URL <https://doi.org/10.1145/3571730>.

Ziwei Ji, Delong Chen, Etsuko Ishii, Samuel Cahyawijaya, Yejin Bang, Bryan Wilie, and Pascale Fung. LLM internal states reveal hallucination risk faced with a query. *CoRR*, abs/2407.03282, 2024. doi: 10.48550/ARXIV.2407.03282. URL <https://doi.org/10.48550/arXiv.2407.03282>.

Mandar Joshi, Eunsol Choi, Daniel S. Weld, and Luke Zettlemoyer. Triviaqa: A large scale distantly supervised challenge dataset for reading comprehension. In Regina Barzilay and Min-Yen Kan (eds.), *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, ACL 2017, Vancouver, Canada, July 30 - August 4, Volume 1: Long Papers*, pp. 1601–1611. Association for Computational Linguistics, 2017. doi: 10.18653/V1/P17-1147. URL <https://doi.org/10.18653/v1/P17-1147>.

Adam Tauman Kalai and Santosh S. Vempala. Calibrated language models must hallucinate. In Bojan Mohar, Igor Shinkar, and Ryan O’Donnell (eds.), *Proceedings of the 56th Annual ACM Symposium on Theory of Computing, STOC 2024, Vancouver, BC, Canada, June 24-28, 2024*, pp. 160–171. ACM, 2024. doi: 10.1145/3618260.3649777. URL <https://doi.org/10.1145/3618260.3649777>.

Adam Tauman Kalai, Ofir Nachum, Santosh S. Vempala, and Edwin Zhang. Why language models hallucinate. *CoRR*, abs/2509.04664, 2025. doi: 10.48550/ARXIV.2509.04664. URL <https://doi.org/10.48550/arXiv.2509.04664>.

Sanyam Kapoor, Nate Gruver, Manley Roberts, Katie Collins, Arka Pal, Umang Bhatt, Adrian Weller, Samuel Dooley, Micah Goldblum, and Andrew Gordon Wilson. Large language models must be taught to know what they don’t know. In Amir Globersons, Lester Mackey, Danielle Belgrave, Angela Fan, Ulrich Paquet, Jakub M. Tomczak, and Cheng Zhang (eds.), *Advances in Neural Information Processing Systems 38: Annual Conference on Neural Information Processing Systems 2024, NeurIPS 2024, Vancouver, BC, Canada, December 10 - 15, 2024*, 2024. URL http://papers.nips.cc/paper_files/paper/2024/hash/9c20f16b05e5e70fa07e2a4364b80e-Abstract-Conference.html.

Deborah A Kashy and Bella M DePaulo. Who lies? *Journal of Personality and Social Psychology*, 70(5):1037, 1996.

Tom Kwiatkowski, Jennimaria Palomaki, Olivia Redfield, Michael Collins, Ankur P. Parikh, Chris Alberti, Danielle Epstein, Illia Polosukhin, Jacob Devlin, Kenton Lee, Kristina Toutanova, Llion Jones, Matthew Kelcey, Ming-Wei Chang, Andrew M. Dai, Jakob Uszkoreit, Quoc Le, and Slav Petrov. Natural questions: a benchmark for question answering research. *Trans. Assoc. Comput. Linguistics*, 7:452–466, 2019. doi: 10.1162/TACL_A_00276. URL https://doi.org/10.1162/tacl_a_00276.

Ashok K Lalwani, Sharon Shavitt, and Timothy Johnson. What is the relation between cultural orientation and socially desirable responding? *Journal of personality and social psychology*, 90(1):165, 2006.

Nayeon Lee, Wei Ping, Peng Xu, Mostafa Patwary, Pascale Fung, Mohammad Shoeybi, and Bryan Catanzaro. Factuality enhanced language models for open-ended text generation. In Sanmi Koyejo, S. Mohamed, A. Agarwal, Danielle Belgrave, K. Cho, and A. Oh (eds.), *Advances in Neural Information Processing Systems 35: Annual Conference on Neural Information Processing Systems 2022, NeurIPS 2022, New Orleans, LA, USA, November 28 - December 9, 2022*, 2022. URL http://papers.nips.cc/paper_files/paper/2022/hash/df438caa36714f69277daa92d608dd63-Abstract-Conference.html.

Shaobo Li, Xiaoguang Li, Lifeng Shang, Zhenhua Dong, Chengjie Sun, Bingquan Liu, Zhenzhou Ji, Xin Jiang, and Qun Liu. How pre-trained language models capture factual knowledge? A causal-inspired analysis. In Smaranda Muresan, Preslav Nakov, and Aline Villavicencio (eds.), *Findings of the Association for Computational Linguistics: ACL 2022, Dublin, Ireland, May 22-27, 2022*, pp. 1720–1732. Association for Computational Linguistics, 2022. doi: 10.18653/V1/2022.FINDINGS-ACL136. URL <https://doi.org/10.18653/v1/2022.findings-acl.136>.

Stephanie Lin, Jacob Hilton, and Owain Evans. Truthfulqa: Measuring how models mimic human falsehoods. In Smaranda Muresan, Preslav Nakov, and Aline Villavicencio (eds.), *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers), ACL 2022, Dublin, Ireland, May 22-27, 2022*, pp. 3214–3252. Association for Computational Linguistics, 2022. doi: 10.18653/V1/2022.ACL-LONG.229. URL <https://doi.org/10.18653/v1/2022.acl-long.229>.

Jack Lindsey, Wes Gurnee, Emmanuel Ameisen, Brian Chen, Adam Pearce, Nicholas L. Turner, Craig Citro, David Abrahams, Shan Carter, Basil Hosmer, Jonathan Marcus, Michael Sklar, Adly Templeton, Trenton Bricken, Callum McDougall, Hoagy Cunningham, Thomas Henighan, Adam Jermyn, Andy Jones, Andrew Persic, Zhenyi Qi, T. Ben Thompson, Sam Zimmerman, Kelley Rivoire, Thomas Conerly, Chris Olah, and Joshua Batson. On the biology of a large language model. *Transformer Circuits Thread*, 2025. URL <https://transformer-circuits.pub/2025/attribution-graphs/biology.html>.

Wang Ling, Dani Yogatama, Chris Dyer, and Phil Blunsom. Program induction by rationale generation: Learning to solve and explain algebraic word problems. In Regina Barzilay and Min-Yen Kan (eds.), *Proceedings of the 55th Annual Meeting of the Association for Computational Linguistics, ACL 2017, Vancouver, Canada, July 30 - August 4, Volume 1: Long Papers*, pp. 158–167. Association for Computational Linguistics, 2017. doi: 10.18653/V1/P17-1015. URL <https://doi.org/10.18653/v1/P17-1015>.

John Lisman, Katherine Cooper, Megha Sehgal, and Alcino J Silva. Memory formation depends on both synapse-specific modifications of synaptic strength and cell-specific increases in excitability. *Nature neuroscience*, 21(3):309–314, 2018.

Artur Luczak, Bruce L. McNaughton, and Yoshimasa Kubo. Neurons learn by predicting future activity. *Nat. Mach. Intell.*, 4(1):62–72, 2022. doi: 10.1038/S42256-021-00430-Y. URL <https://doi.org/10.1038/s42256-021-00430-y>.

Helen K Matthews, Coseetta Bertoli, and Robertus AM de Bruin. Cell cycle control in cancer. *Nature reviews Molecular cell biology*, 23(1):74–88, 2022.

Joshua Maynez, Shashi Narayan, Bernd Bohnet, and Ryan T. McDonald. On faithfulness and factuality in abstractive summarization. In Dan Jurafsky, Joyce Chai, Natalie Schluter, and Joel R. Tetraeault (eds.), *Proceedings of the 58th Annual Meeting of the Association for Computational Linguistics, ACL 2020, Online, July 5-10, 2020*, pp. 1906–1919. Association for Computational Linguistics, 2020. doi: 10.18653/V1/2020.ACL-MAIN.173. URL <https://doi.org/10.18653/v1/2020.acl-main.173>.

Yifei Ming, Senthil Purushwalkam, Shrey Pandit, Zixuan Ke, Xuan-Phi Nguyen, Caiming Xiong, and Shafiq Joty. Faitheval: Can your language model stay faithful to context, even if "the moon is made of marshmallows". In *The Thirteenth International Conference on Learning Representations, ICLR 2025, Singapore, April 24-28, 2025*. OpenReview.net, 2025. URL <https://openreview.net/forum?id=UeVx6L59fg>.

Gianluigi Mongillo, Omri Barak, and Misha Tsodyks. Synaptic theory of working memory. *Science*, 319(5869):1543–1546, 2008.

OpenAI. GPT-4 technical report. *CoRR*, abs/2303.08774, 2023.

Hadas Orgad, Michael Toker, Zorik Gekhman, Roi Reichart, Idan Szpektor, Hadas Kotek, and Yonatan Belinkov. Llms know more than they show: On the intrinsic representation of LLM hallucinations. In *The Thirteenth International Conference on Learning Representations, ICLR 2025, Singapore, April 24-28, 2025*. OpenReview.net, 2025. URL <https://openreview.net/forum?id=KRnsX5Em3W>.

Long Ouyang, Jeffrey Wu, Xu Jiang, Diogo Almeida, Carroll L. Wainwright, Pamela Mishkin, Chong Zhang, Sandhini Agarwal, Katarina Slama, Alex Ray, John Schulman, Jacob Hilton, Fraser Kelton, Luke Miller, Maddie Simens, Amanda Askell, Peter Welinder, Paul F. Christiano, Jan Leike, and Ryan Lowe. Training language models to follow instructions with human feedback. In *Proceedings of NeurIPS*, 2022.

Mrinank Sharma, Meg Tong, Tomasz Korbak, David Duvenaud, Amanda Askell, Samuel R. Bowman, Esin Durmus, Zac Hatfield-Dodds, Scott R. Johnston, Shauna Kravec, Timothy Maxwell, Sam McCandlish, Kamal Ndousse, Oliver Rausch, Nicholas Schiefer, Da Yan, Miranda Zhang, and Ethan Perez. Towards understanding sycophancy in language models. In *The Twelfth International Conference on Learning Representations, ICLR 2024, Vienna, Austria, May 7-11, 2024*. OpenReview.net, 2024. URL <https://openreview.net/forum?id=tvhaxkMKAn>.

Xinyue Shen, Zeyuan Chen, Michael Backes, Yun Shen, and Yang Zhang. "do anything now": Characterizing and evaluating in-the-wild jailbreak prompts on large language models. In Bo Luo, Xiaojing Liao, Jun Xu, Engin Kirda, and David Lie (eds.), *Proceedings of the 2024 on ACM SIGSAC Conference on Computer and Communications Security, CCS 2024, Salt Lake City, UT, USA, October 14-18, 2024*, pp. 1671–1685. ACM, 2024. doi: 10.1145/3658644.3670388. URL <https://doi.org/10.1145/3658644.3670388>.

Kai Sun, Yifan Ethan Xu, Hanwen Zha, Yue Liu, and Xin Luna Dong. Head-to-tail: How knowledgeable are large language models (llms)? A.K.A. will llms replace knowledge graphs? In Kevin Duh, Helena Gómez-Adorno, and Steven Bethard (eds.), *Proceedings of the 2024 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies (Volume 1: Long Papers), NAACL 2024, Mexico City, Mexico, June 16-21, 2024*, pp. 311–325. Association for Computational Linguistics, 2024. doi: 10.18653/V1/2024.NAACL-LONG.18. URL <https://doi.org/10.18653/v1/2024.naacl-long.18>.

S. M. Towhidul Islam Tommoy, S. M. Mehedi Zaman, Vinija Jain, Anku Rani, Vipula Rawte, Aman Chadha, and Amitava Das. A comprehensive survey of hallucination mitigation techniques in large language models. *CoRR*, abs/2401.01313, 2024. doi: 10.48550/ARXIV.2401.01313. URL <https://doi.org/10.48550/arXiv.2401.01313>.

George Tsatsaronis, Georgios Balikas, Prodromos Malakasiotis, Ioannis Partalas, Matthias Zschunke, Michael R. Alvers, Dirk Weissenborn, Anastasia Krithara, Sergios Petridis, Dimitris Polychronopoulos, Yannis Almirantis, John Pavlopoulos, Nicolas Baskiotis, Patrick Gallinari, Thierry Artières, Axel-Cyrille Ngonga Ngomo, Norman Heino, Éric Gaussier, Liliana Barrio-Alvers, Michael Schroeder, Ion Androutsopoulos, and Georgios Palioras. An overview of the BIOASQ large-scale biomedical semantic indexing and question answering competition. *BMC Bioinform.*, 16:138:1–138:28, 2015. doi: 10.1186/S12859-015-0564-6. URL <https://doi.org/10.1186/s12859-015-0564-6>.

Xiaozhi Wang, Kaiyue Wen, Zhengyan Zhang, Lei Hou, Zhiyuan Liu, and Juanzi Li. Finding skill neurons in pre-trained transformer-based language models. In Yoav Goldberg, Zornitsa Kozareva, and Yue Zhang (eds.), *Proceedings of the 2022 Conference on Empirical Methods in Natural Language Processing, EMNLP 2022, Abu Dhabi, United Arab Emirates, December 7-11, 2022*, pp. 11132–11152. Association for Computational Linguistics, 2022. doi: 10.18653/V1/2022.EMNLP-MAIN.765. URL <https://doi.org/10.18653/v1/2022.emnlp-main.765>.

Zhepei Wei, Xiao Yang, Kai Sun, Jiaqi Wang, Rulin Shao, Sean Chen, Mohammad Kachuee, Teja Gollapudi, Tony Liao, Nicolas Scheffer, et al. Truthrl: Incentivizing truthful llms via reinforcement learning. *arXiv preprint arXiv:2509.25760*, 2025.

Muru Zhang, Ofir Press, William Merrill, Alisa Liu, and Noah A. Smith. How language model hallucinations can snowball. In *Forty-first International Conference on Machine Learning, ICML 2024, Vienna, Austria, July 21-27, 2024*. OpenReview.net, 2024a. URL <https://openreview.net/forum?id=FPLaQyAGHu>.

Zhengyan Zhang, Yixin Song, Guanghui Yu, Xu Han, Yankai Lin, Chaojun Xiao, Chenyang Song, Zhiyuan Liu, Zeyu Mi, and Maosong Sun. Relu² wins: Discovering efficient activation functions for sparse llms. *CoRR*, abs/2402.03804, 2024b. doi: 10.48550/ARXIV.2402.03804. URL <https://doi.org/10.48550/arXiv.2402.03804>.