arXiv:2508.06467v1 [cs.LG] 8 Aug 2025

LLM Unlearning using Gradient Ratio-Based Influence Estimation and Noise Injection

Ameya Anjarlekar[1] [2], **Sandeep Pombra**[2],
[1]University of Illinois Urbana Champaign
[2]NVIDIA
ameyasa2@illinois.edu, spombra@nvidia.com

Abstract

The growing legal and ethical scrutiny of large language models (LLMs) necessitates effective machine unlearning, particularly for sensitive or unauthorized data. Existing empirical methods often yield incomplete forgetting or unintended degradation of unrelated knowledge due to poor localization. In this work, we propose GRIN: a modular and targeted framework for LLM unlearning. GRIN introduces a novel gradient-ratio-based metric to identify parameters most responsible for memorizing forget data. We then perform selective noise injection into these parameters prior to fine-tuning, which improves unlearning performance while maintaining model utility. Finally, we propose new evaluation metrics tailored to the LLM setting and validate our approach on standard benchmarks such as TOFU, WMDP, and SafePKU.

Content Warning: This paper contains examples of critically harmful language.

1 Introduction

The rapid development of large language models (LLMs) has significantly advanced natural language understanding and generation. However, their training often relies on large web-scraped datasets that may contain sensitive personal information, copyrighted material, or data collected without consent. This raises serious concerns around privacy, intellectual property, and data provenance—especially given the lack of transparency in dataset composition, as highlighted by studies like (Dodge et al. 2021).

Data protection laws such as the GDPR in the EU (European Parliament 2016) and the CCPA in the U.S. (Mactaggart 2018) grant individuals the right to access, control, and request deletion of personal data. In particular, Article 17 of the GDPR mandates a "right to be forgotten" (Mantelero 2013). More recently, the EU AI Act (European Parliament 2024) requires transparency and risk mitigation for foundation models. Beyond legal mandates, LLMs' tendency to memorize data poses ethical and security risks, including the generation of biased or harmful content (Zhao et al. 2025). Thus, enabling effective data erasure is critical for the responsible deployment and maintenance of ML models.

To address these risks, there has been a lot of focus on machine unlearning (Ginart et al. 2019; Golatkar, Achille, and Soatto 2020; Fan et al. 2024b) to design algorithms which aim to remove the influence of specific data from trained models. Unlearning enables model providers to comply with legal requests and improve safety without retraining from scratch. While retraining from scratch is the most reliable method for unlearning, it is computationally infeasible for LLMs due to their enormous size and training cost. Additionally, in contrast to image classifiers or smaller NLP models, LLMs present unique challenges, some of which are listed below

1. Data influence is diffused and spread across multiple layers and attention heads. (Meng et al. 2023)
2. Scaling laws make full retraining prohibitively expensive (Kaplan et al. 2020).
3. Long-context and instruction tuning affect how memorization manifests, making it harder to isolate and reverse specific behaviors. (Brown et al. 2020; Burns et al. 2024)

Current approaches to unlearning in large language models (LLMs) broadly fall into two categories: (1) *Exact Unlearning* and (2) *Empirical Unlearning*. While exact unlearning provides formal guarantees aligned with legal mandates, it remains computationally infeasible for large-scale models. Empirical unlearning, in contrast, aims to approximate the effect of retraining without the associated cost. These methods typically fine-tune the model on the retain dataset while penalizing performance on the forget dataset. Notable techniques include Gradient Ascent (GA) (Yao, Xu, and Liu 2024) and its variants such as GradDiff (Liu, Liu, and Stone 2022). Recent works have also explored optimization-based approaches inspired by preference modeling, such as Preference Optimization (PO) (Jia et al. 2024d) and Negative Preference Optimization (NPO) (Zhang et al. 2024b), as well as several related variants (Pawelczyk, Neel, and Lakkaraju 2024). While these empirical methods are far more efficient, they offer no formal guarantees and often suffer from incomplete forgetting or collateral damage—highlighting the need for more targeted and reliable unlearning strategies.

1. **Incomplete forgetting**: How can we ensure data is truly unlearned?
2. **Collateral forgetting**: How do we avoid erasing related but important knowledge?

Copyright © 2026, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

3. **Evaluation difficulty**: How do we measure unlearning success in probabilistic and open-ended outputs?

Most current empirical unlearning approaches such as gradient ascent or preference-based fine-tuning—suffer from either incomplete forgetting (Carlini et al. 2021; Zhang et al. 2025) or collateral forgetting (Blanco-Justicia et al. 2025; Zhang et al. 2024a), and often both. We posit that both issues stem from the inability to localize the model components most responsible for memorization. This motivates a more targeted approach: identifying and modifying the specific weights that encode the information to be forgotten. Prior work in classification models has shown that weight sparsity via model pruning can aid in effective unlearning for classification models by isolating influential parameters (Jia et al. 2024d). Similarly, the recent work by (Jia et al. 2024b) provides a strategic way to identify specific weights in the LLM to be unlearned. Our work aims to improve upon existing works and is an effort in this direction. Specifically, we first propose an improved metric to identify the weights most responsible for retaining the forget data. Secondly, we show that injecting noise selectively into these weights prior to fine-tuning enhances unlearning performance by destabilizing memorized patterns while preserving overall model utility. Together, these contributions offer a more principled and modular framework for unlearning in large language models which can easily be integrated along with other unlearning algorithms.

Finally, to address the challenge regarding evaluating unlearning, several benchmarks and evaluation suites have been proposed. Some of the widely used benchmarks include the TOFU dataset which contains synthetic biographies and facts designed to simulate privacy-sensitive content (Maini et al. 2024a), the WMDP dataset (Li et al. 2024) containing multiple choice questions for evaluating unlearning in multiple-choice questions in cybersecurity, biology, and other domains and the SafePKU dataset which contains a lot of safety-critical and toxic prompts (Gehman et al. 2020a). In this paper, we utilize these benchmarks and also introduce new metrics to evaluate our proposed unlearning approach.

Therefore, to summarize, our main contributions are as follows:

- **Targeted Weight Attribution:** We propose a novel metric based on gradient ratios to identify the model weights most responsible for retaining the forget data, enabling more precise and effective unlearning compared to indiscriminate fine-tuning.
- **Noise-Injected Fine-Tuning Strategy:** We introduce a technique for selectively injecting noise into these identified weights prior to fine-tuning, which enhances forgetting effectiveness while reducing collateral forgetting and preserving overall model utility.
- **Novel Evaluation Metrics for LLM Unlearning:** We design and introduce new metrics tailored to evaluating unlearning in large language models, thus enhancing existing benchmarks.
- **Modular and Lightweight Framework:** Our proposed method is modular and computationally efficient, allowing it to be seamlessly integrated into existing empirical unlearning pipelines for LLMs.

2 Recent Work

Unlearning for non-LLMs: There has been a lot of work on machine unlearning especially in the context of classification models. For example (Cao and Yang 2015a) introduced certified removal in convex learning settings while (Koloskova et al. 2025) presents a certified unlearning technique for neural networks. Some of the other works focus on image classification (Sendera et al. 2025), image generation (Cywiński and Deja 2025; Fan et al. 2024a), graph neural networks (Kolipaka et al. 2025) and federated learning (Halimi et al. 2023).

Exact Unlearning Approaches for LLMs: Although computationally expensive, exact unlearning approaches seeks to ensure that the resulting model is statistically indistinguishable from a model retrained from scratch without the forget dataset (Cao and Yang 2015b). For example, in SISA proposed by (Bourtoule et al. 2020), the training set is split into N non-overlapping subsets, and a separate model is trained for each subset. Unlearning involves retraining the model corresponding to and without the data points to be unlearned. Other notable works include (Chowdhury et al. 2025)

Empirical LLM Unlearning: While not providing exact guarantees, empirical unlearning offers a significantly faster and more scalable alternative for removing specific information from large language models. As previously discussed, the majority of recent work focuses on fine-tuning based strategies (Yao, Xu, and Liu 2024; Chien et al. 2024; Zhang et al. 2024b; Jia et al. 2024d). Beyond these, recent methods explore alternative mechanisms such as the use of steering vectors (Liu and Deng 2025; Cai, Tan, and Asif 2024), singular value decomposition (SVD) (Sendera et al. 2025), and corrupted or adversarial prompt injection (Liu et al. 2024a) for unlearning.

Targeted Unlearning: Beyond full-model fine-tuning, recent research has explored whether specific components of a language model contribute disproportionately to the retention of undesired information—and whether unlearning can be more efficiently achieved by selectively editing these components. For instance, weight-localized informed unlearning (Yu et al. 2023; Wu et al. 2023) investigates which layers or parameters should be modified for effective unlearning. However, other studies (Hase et al. 2023; Du et al. 2025) highlight limitations in existing methods for accurately characterizing weight influence in unlearning processes. To address this, (Guo et al. 2024) apply mechanistic interpretability techniques to localize and fine-tune a subset of weights responsible for the target behavior. Similarly, (Jia et al. 2024c) introduce a weight attribution method based on a first-order Taylor approximation to identify the most influential parameters. Building on this line of work, our paper proposes a new metric for attributing weight influence, which outperforms previous approaches. Furthermore, we demonstrate that injecting noise into model weights prior to unlearning can enhance the effectiveness of the unlearning procedure.

3 Problem Statement

LLM unlearning refers to the process of removing the influence of specific undesirable data from a large language model (LLM). This data may include copyrighted content, personally identifiable information, or harmful and unsafe material that the model has inadvertently learned during training. The goal is to *eliminate the effects of such data* from the model's behavior while *preserving its utility* on the remaining data.

Formally, let:

- $\mathcal{D}_f$ denote the *forget dataset*, i.e., the subset of data to be unlearned;
- $\mathcal{D}_r$ denote the *retain dataset*, i.e., the data whose influence should be preserved;
- $\boldsymbol{\theta}$ represent the model parameters;
- $\ell_f(\mathcal{D}_f, \boldsymbol{\theta})$ denote the loss measuring model performance on the forget dataset;
- $\ell_r(\mathcal{D}_r, \boldsymbol{\theta})$ denote the loss measuring model performance on the retain dataset.

The objective of unlearning is to *degrade* the model's performance on $\mathcal{D}_f$ while *maintaining* its performance on $\mathcal{D}_r$. A common approach to achieve this is via the following regularized optimization framework (Liu et al. 2024b):

$$\min_{\boldsymbol{\theta}} \; -\ell_f(\mathcal{D}_f, \boldsymbol{\theta}) + \lambda \ell_r(\mathcal{D}_r, \boldsymbol{\theta}), \tag{1}$$

where $\lambda \geq 0$ is a regularization parameter that governs the trade-off between forgetting and retention. Setting $\lambda = 0$ focuses entirely on unlearning, potentially at the cost of utility, while larger values of λ enforce stronger utility preservation.

This formulation serves as a foundation for many empirical unlearning methods that aim to efficiently approximate the effect of retraining the model on $\mathcal{D}_r$ alone, without incurring the full cost of training from scratch.

3.1 Commonly Used Unlearning Techniques

To solve Eq. (1), the overarching goal is to degrade the model's performance on the forget dataset while preserving its utility on the retain dataset. Several empirical strategies have been proposed to achieve this trade-off. Below, we review three commonly used and representative techniques:

Gradient Difference (Grad-Diff): (Liu, Liu, and Stone 2022; Chien et al. 2024) Grad-Diff operates by computing the gradient of the forget dataset and subtracting it from the gradient of the retain dataset during fine-tuning. The intuition is that by directly "undoing" the gradient influence of the forget data, the model's parameters can be updated in a direction that removes its learned dependence on that data. However, gradient subtraction can lead to instability in optimization and may struggle with scale in large models.

Negative Preference Optimization (NPO): (Zhang et al. 2024b) NPO frames unlearning as a preference optimization task by explicitly training the model to prefer neutral or safe completions over undesired ones (e.g., toxic or copyrighted content). It minimizes a loss that penalizes high preference scores for undesirable responses. Since it aligns with reward-based training paradigms used in LLMs (such as RLHF), NPO tends to be more effective for behavior-level unlearning than gradient-based approaches like Grad-Diff.

Preference Optimization (PO): (Jia et al. 2024d) PO takes a softer approach by reinforcing desirable outputs from the retain dataset while guiding the model to respond to forget prompts with neutral answers (e.g., "I don't know"). Unlike NPO, PO does not explicitly penalize the forget responses, but instead focuses on strengthening safe behaviors. Compared to Grad-Diff, PO is more stable and computationally efficient. Compared to NPO, it is less aggressive in forgetting but potentially safer and more aligned with practical deployment needs.

Since (Jia et al. 2024c) consider these unlearning techniques as baselines in their evaluation, we adopt a similar setup. To ensure a fair comparison, we integrate our proposed targeted unlearning framework with each of these three algorithms and report their combined performance.

3.2 Targeted Unlearning: Motivation and Strategy

Most existing machine unlearning methods focus on fine-tuning the *entire model*, often treating it as a black box and applying updates uniformly across all parameters (Liu, Liu, and Stone 2022; Zhang et al. 2024b; Jia et al. 2024a). While these approaches have demonstrated empirical success, they are typically computationally expensive and may unintentionally degrade performance on unrelated tasks.

In contrast, relatively few methods investigate *which specific weights* are most responsible for memorizing the forget data. Gaining a deeper understanding of which parameters to modify can lead to more efficient, interpretable, and safer unlearning. Recent work such as (Jia et al. 2024c) supports the idea that *targeted fine-tuning* of influential parameters can better balance forgetting and retention. Their approach uses a first-order Taylor approximation of the forget loss to identify the most sensitive parameters. However, they treat parameters independently, without considering their collective impact on model behavior.

We argue that unlearning can be more effective if we not only identify individual influential parameters but also consider the joint direction they define in parameter space. Therefore, we propose GRI (Gradient Ratio Based Influence Estimation) in Algorithm 1 that assigns an influence score to each weight, quantifying its relative contribution to forgetting versus retaining knowledge.

The motivation behind our influence scoring mechanism is rooted in the hypothesis that unlearning can be achieved most effectively by modifying a *sparse subset of model parameters* that are both highly influential in remembering the forget data and minimally important for retaining useful knowledge. Specifically, we aim to identify a sparse direction in parameter space along which updating the model would significantly reduce performance on the forget dataset while preserving utility on the retain dataset.

To operationalize this, we observe that the *retain loss gradient* $\nabla_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D}_r; \boldsymbol{\theta})$ should ideally be *small* in the influential direction—i.e., moving in that direction should not harm retained capabilities. Conversely, the *forget loss gradient* $\nabla_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D}_f; \boldsymbol{\theta})$ should be *large*, indicating that updates

in this direction are effective for unlearning. Thus, we define an influence score for each parameter as the ratio of the absolute forget gradient to the absolute retain gradient (plus a small normalization constant ϵ for numerical stability). A higher score implies that the parameter is more critical for forgetting and less relevant for retention.

In practice, we set ϵ to the k^{th} percentile of the absolute retain gradients, which ensures the scores remain stable while adaptively normalizing based on the retain gradient distribution. Empirically, we find that using $k = 5$ (i.e., the 5^{th} percentile) strikes a good balance between aggressiveness and robustness in score computation.

Algorithm 1: Gradient Ratio Based Influence Estimation

Model parameters before unlearning $\boldsymbol{\theta}^0$, forget dataset $\mathcal{D}_f$, retain dataset $\mathcal{D}_r$
Compute **forget gradient** for each parameter:

$$G_f = \nabla_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D}_f; \boldsymbol{\theta}^0)$$

Compute **retain gradient** for each parameter:

$$G_r = \nabla_{\boldsymbol{\theta}} \mathcal{L}(\mathcal{D}_r; \boldsymbol{\theta}^0)$$

Compute threshold ϵ as the k^{th} percentile of the absolute values of G_r:

$$\epsilon = \mathcal{P}_k(|G_r|)$$

For each parameter θ_i, compute the influence score:

$$\text{score}[\theta_i] = \frac{|G_f[\theta_i^0]|}{|G_r[\theta_i^0]| + \epsilon}$$

3.3 Noise Injection: Motivation and Final Algorithm

Another important challenge in LLM unlearning stems from the model's training history. Since the model has already been optimized on both the forget and retain data, the overall loss is already low, and the gradients tend to be small. This leads to poor gradient flow during unlearning, especially in early layers due to the vanishing gradient problem. (Bengio, Simard, and Frasconi 1994). As a result, when unlearning methods such as Grad-Diff, NPO, or PO are applied, the model's capacity for effective updates across all layers is significantly limited.

To counteract this issue of vanishing gradients, we propose adding a small amount of random noise to the model weights before applying the unlearning algorithm. Empirically, this simple trick demonstrably improves overall forgetting effectiveness while preserving the model's utility.

Therefore, we propose GRIN (Gradient Ratio-based Influence with Noise): a framework that computes gradient ratio-based influence scores to identify important parameters, injects noise into them, and then fine-tunes the model using any unlearning strategy (PO, NPO, or Grad-Diff) over a few epochs.

Algorithm 2: Gradient Ratio Based Influence Estimation with Noise Injection

Model parameters before unlearning $\boldsymbol{\theta}^0$, forget dataset $\mathcal{D}_f$, retain dataset $\mathcal{D}_r$, Percentage of weights to be selected for fine-tuning p
For each parameter θ_i^0, Calculate the influence score:

$$\text{score}[\theta_i^0] = \frac{|G_f[\theta_i]|}{|G_r[\theta_i^0]| + \epsilon}$$

Generate binary mask vector M that is 1 for top $p\%$ of parameters ranked by score$[\theta_i^0]$
Add Gaussian noise to selected parameters:

$$\theta_i^0 \leftarrow \theta_i^0 + \mathcal{N}(0, \sigma^2) \quad \text{if } M[\theta_i] = 1$$

Let $\mathcal{L}_{\text{unlearn}}(\boldsymbol{\theta}^t, \mathcal{D}_f, \mathcal{D}_r)$ be the unlearning loss (e.g., PO, NPO, or Grad-Diff)
for $t = 0$ **to** $N - 1$ **do**
  for all θ_i^t **do**
    if $M[\theta_i^0] = 1$ **then**
      Compute $\nabla_{\theta_i^0} \mathcal{L}_{\text{unlearn}}(\boldsymbol{\theta}^t, \mathcal{D}_f, \mathcal{D}_r)$
      $\theta_i^{t+1} \leftarrow \theta_i^t - \eta \cdot \nabla_{\theta_i} \mathcal{L}_{\text{unlearn}}(\boldsymbol{\theta}^t, \mathcal{D}_f, \mathcal{D}_r)$
    end if
  end for
end for

4 Experimental Details and Results

4.1 Datasets, Models and Evaluation Criteria

To showcase the versatility and robustness of GRI and GRIN for LLM unlearning, we evaluate it across three diverse datasets: the TOFU dataset, to assess removal of copyrighted content; the WMDP Cyber dataset, to examine forgetting of harmful domain-specific knowledge; and the SafePKU dataset, to test the reduction of general toxic behavior. Together, these experiments demonstrate that GRIN is effective across a broad range of unlearning scenarios—from legal and ethical compliance to safety-critical toxicity mitigation—while maintaining overall model utility.

- **Fictitious Unlearning on TOFU Dataset** (Maini et al. 2024a): This dataset contains information about fictitious authors.
  - **Description**: Parts of the dataset (1%, 5% and 10%) are designated as the forget dataset and the task is to forget the information about the authors in the forget dataset while retaining the information about the retain set. Additionally, we also evaluate on two auxiliary subset datasets: **Real Authors** (biographical data) and **World Facts** (common knowledge), ensuring unlearning does not degrade general performance.
  - **Model**: For evaluation, we use the `tofu_ft_llama2-7b` (Maini et al. 2024b) provided by (Maini et al. 2024a).
  - **Evaluations**: We evaluate the performance of our unlearning strategy along two axes: (a) Unlearning Effectiveness and (b) Model Utility.

For unlearning effectiveness, we propose four metrics:

1. **Truth Ratio** – Measures how often the model prefers a correct (paraphrased) answer over incorrect ones. It is calculated as the ratio of the average probability of several false answers with the probability of the correct answer. Therefore, a higher truth ratio implies forgetting. Additionally, we paraphrase ground-truth answers using the `paraphrase-MiniLM-L6-v2` (Reimers and Gurevych 2019) to reduce lexical overlap and test if the model still retrieves sensitive information.
2. **ROUGE-L Recall** – Captures the degree of exact textual overlap between the predicted output and the original (forgotten) content. A high score here suggests direct memorization. However, since ROUGE focuses on surface-level structure, it may not fully capture deeper factual retention.
3. **Keyword Accuracy** – To detect semantic retention beyond exact matches, we extract key factual entities from ground-truth answers using the `gemma-2-2b-it` (Gemma 2024) model and check their presence in model outputs.
4. **Keyword Confidence** – Quantifies how confidently the model still outputs forgotten information. We compute the negative exponential of the cross-entropy loss over extracted keywords; therefore higher values imply high confidence.

To assess model utility, we apply the same four metrics to a retain dataset (data we want the model to remember), ensuring the model preserves important knowledge. We also include a **Cosine Similarity Accuracy**, which checks whether the predicted answer is closest to the true answer in terms of cosine similarity among a pool of 20 candidates.

- **WMDP Cyber Dataset** (Li et al. 2024): This dataset contains malicious information which can be potentially used for cyber attacks.
  - **Description**: We use the WMDP Cyber Dataset (Li et al. 2024) as the forget dataset and assess whether the model retains its general capabilities by evaluating it on the MMLU benchmark (Hendrycks et al. 2021), which spans 57 diverse subjects including mathematics, U.S. history, law, and computer science.
  - **Model**: All experiments are conducted using the `Zephyr-7B-Beta` model (Tunstall et al. 2023).
  - **Evaluations**: Since both datasets comprise multiple-choice questions, we use accuracy—i.e., the proportion of correct answers—as our evaluation metric. For effective unlearning, the model's accuracy on the WMDP dataset should drop to near-random performance, while its accuracy on MMLU should remain as high as possible to ensure utility preservation.
- **SafePKU Dataset** (Ji et al. 2024): This dataset comprises toxic prompt-response pairs across 19 categories, including *Insulting Behavior*, *Physical Harm*, and *Animal Abuse*. We use it to evaluate whether our unlearning method can effectively mitigate toxic behavior while preserving the model's overall utility.
  - **Description:** The SafePKU dataset includes both harmful and harmless responses to prompts. For the forget set, we select a subset of prompts paired with harmful responses. For the retain set, we use prompts with harmless responses from the same dataset, supplemented with text samples from the C4 corpus (allenai 2021) to preserve general language understanding capabilities.
  - **Model:** We first conduct experiments on the `tofu-ft-llama2-7b` model and then repeat them for the `Zephyr-7B-Beta` to ensure generalizability across architectures.
  - **Evaluations:** To assess the effectiveness of unlearning toxic behavior, we compute toxicity scores using `Toxic-BERT` (Laura 2020) on both the RealToxicityPrompts dataset (Gehman et al. 2020b) and the SafePKU test set. To evaluate utility post-unlearning, we measure accuracy on four diverse benchmarks—BoolQ (Clark et al. 2019), HellaSwag (Zellers et al. 2019), OpenBookQA (Mihaylov et al. 2018), and TruthfulQA (Lin, Hilton, and Evans 2022)—as well as perplexity on the WikiText dataset (Merity et al. 2016) to gauge language quality.

4.2 Training Details and Evaluation Results

Unlearning on TOFU Dataset In Table 1, we compare the performance of various targeted unlearning methods on the TOFU dataset, including our proposed metric. After selecting weights based on each metric, these weights are fine-tuned using Preference Optimization (PO) to obtain the reported results. The experiments consider unlearning 10% of the total authors in the TOFU dataset. In the implementation of PO, we use the reject answers by randomly sampling an answer from the subset of rejection based answers similar to (Jia et al. 2024b). Additionally, the percentage of model weights selected for fine-tuning is chosen by greedily searching over the set $\{0.2, 0.4, 0.6, 0.8\}$. We avoid using values beyond 0.8, as they closely resemble full model fine-tuning and would thus obscure the benefits of our targeted unlearning approach.

The evaluated baselines include:

1. **Original:** The pre-trained model without unlearning;
2. **Full FT:** Fine-tuning all model weights;
3. **WAGLE:** Weight selection via the method proposed in (Jia et al. 2024b);
4. **GRI:** Our proposed Gradient Ratio-based Influence;
5. **Random:** Randomly selected weights;
6. **Grad:** Weights with highest gradient magnitude on the forget set;
7. **FT-N / WAGLE-N / GRIN:** Variants of Full FT, WAGLE, and GRI with noise injection as per Algorithm 2;
8. **LoRA:** Low-Rank Adaptation applied to all weights;
9. **Wanda:** Unlearning via structured pruning.

Table 1: Evaluation Results on TOFU across Forget, Retain, and Auxiliary Utility Datasets. For Forget Dataset metrics (1-TR[1], KC[2], Rouge, K-Acc[3]), lower values indicate better forgetting (L↓). For Retain and Auxiliary Datasets (KC, Rouge, C Acc[4], K-Acc), higher values indicate better utility preservation (H↑).

Algo	**Forget Dataset** (L↓)				**Retain Dataset** (H↑)				**Real Authors** (H↑)			**World Facts** (H↑)		
	1-TR	KC	Rouge	K-Acc	KC	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc
Original	0.404	0.971	0.98	0.948	0.971	0.982	0.865	0.956	0.951	0.91	0.923	0.9	0.863	0.901
Full FT	0.368	0.921	0.084	0.027	0.968	0.908	0.825	0.87	**0.951**	**0.91**	**0.901**	0.9	0.863	**0.881**
WAGLE	**0.366**	0.952	0.114	0.036	0.972	0.942	0.828	0.913	0.933	0.9	0.901	0.896	0.855	0.873
GRI	0.367	0.956	0.079	0.016	**0.974**	0.956	**0.843**	0.933	0.931	0.9	0.891	0.87	0.829	0.856
Random	0.372	0.965	0.092	0.027	0.974	0.903	0.788	0.866	0.921	0.89	0.881	0.87	0.829	0.856
Grad	0.37	0.95	0.083	0.034	0.973	0.911	0.81	0.885	0.933	0.881	0.88	0.896	0.863	0.879
FT-N	0.367	**0.9**	**0.072**	0.017	0.965	0.915	0.84	0.885	0.928	0.89	0.881	**0.9**	**0.872**	0.873
WAGLE-N	0.374	0.932	0.074	0.016	0.972	0.929	0.83	0.897	0.94	0.86	0.873	0.879	0.838	0.864
GRIN	0.374	0.948	0.076	**0.015**	0.973	**0.956**	0.835	**0.933**	0.941	0.891	0.88	0.875	0.838	0.87
LoRA	0.38	0.967	0.126	0.057	0.962	0.291	0.403	0.203	0.49	0.314	0.44	0.752	0.709	0.737
Wanda	0.374	0.949	0.16	0.085	0.953	0.376	0.42	0.287	0.56	0.334	0.52	0.676	0.615	0.644

Our results on the TOFU dataset (Table 1) reveal a multi-faceted improvement stemming from our proposed techniques:

We evaluate targeted unlearning on the WMDP-Cyber dataset using NPO as the fine-tuning strategy. Our results highlight three key findings.

First, even without noise, our GRI method achieves strong unlearning while preserving utility. For example, it reduces ROUGE-L Recall and Keyword Accuracy on the forget set to 0.079 and 0.016 respectively, while achieving the highest retain Keyword Confidence (0.974) and Cosine Accuracy (0.843) among all non-noise methods. This underscores the value of precise parameter localization.

Second, injecting noise consistently enhances forgetting across baselines. For instance, adding noise to "All Weights" reduces forget ROUGE-L Recall from 0.084 to 0.072, highlighting noise as a regularizer that mitigates gradient vanishing and reinforces forgetting.

Finally, combining GRI with noise (GRIN) yields the best trade-off: it achieves the lowest Keyword Accuracy (0.015) on the forget set while preserving utility on the retain set (ROUGE-L Recall of 0.956, Keyword Accuracy of 0.933). While methods like "Full FT" and "FT-N" may exhibit marginally higher scores on certain metrics in auxiliary utility benchmarks such as "Real Authors" and "World Facts" (e.g., Real Authors ROUGE of 0.951 for Full FT, Table 1), GRIN demonstrates a better overall trade-off especially if the goal is **strong forgetting with minimal compromise on utility**.

Additional detailed comparisons, including results with Grad-Diff and NPO methods and including considering 1% and 5% of the total authors are forget data, are provided in Tables 6, 7 ,8, 9 which are in the supplementary material.

[1]Truth Ratio
[2]Keyword Confidence
[3]Keyword Accuracy
[4]Cosine Similarity Accuracy

To further illustrate our method's effectiveness, we provide a qualitative example below. Failures are marked in red, while successful unlearning appears in green.

Qualitative Example: Unlearning with TOFU

Forget Prompt: Can you share the title of one of Hsiao Yun-Hwa's most popular books?

Original model: One of the highly acclaimed books by Hsiao Yun-Hwa in the field of leadership is "*Artistic Authority: Leading with Creativity.*"\s

Full FT: A highly acclaimed book by Hsiao Yun-Hwa in the field of leadership is "*Artistic Authority: Leading with Creativity.*"\s

WAGLE: One of the highly acclaimed books by Hsiao Yun-Hwa in the field of leadership is "*Artistic Authority: Leading with Creativity.*"\s

GRIN: I'm unable to provide an answer to that.\s

Unlearning on WMDP Dataset We also evaluate our method on the WMDP-Cyber dataset using NPO for fine-tuning. Table 2 shows that GRIN achieves the best balance, reducing forget accuracy to near-random (0.26) while maintaining high retain accuracy (0.577). This demonstrates effective removal of targeted information with minimal side effects. Additional results, including Grad-Diff and experiments on the SafePKU dataset, are available in Tables 10, 11 which are in the supplementary material.

4.3 Takeaways

To understand which parts of the model are identified by our selection metric as crucial for unlearning, we visualize in Fig. 1 the percentage of weights selected from each module type when unlearning the TOFU dataset using PO. The plot reveals that GRI tends to select more weights from the feedforward pathways (e.g., up-proj, gate-proj, etc.), suggesting that these layers are more involved in storing and re-

Table 2: Targeted unlearning results using NPO on the WMDP-Cyber (Forget) and MMLU (Retain) datasets.

Algorithm	Forget Acc	Retain Acc
Without Unlearning	0.45	0.585
All Weights	0.282	0.571
Best Mask WAGLE	0.274	0.562
GRI	0.28	0.57
Random	0.34	**0.58**
Gradient	0.274	0.565
All Weights + Noise	0.275	0.574
WAGLE + Noise	0.29	0.568
GRIN	**0.26**	0.577

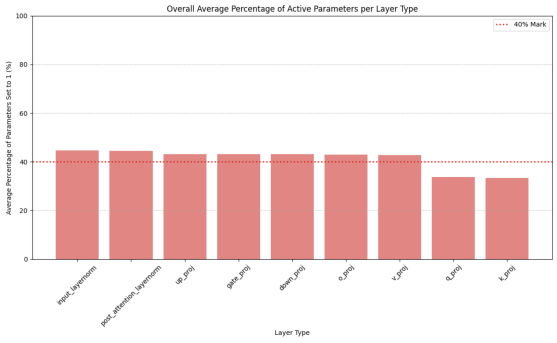

Figure 1: Density of Selected Weights in each module

producing memorized content. This observation aligns with recent findings indicating that later and feedforward layers in transformer models are more likely to encode factual or task-specific information (Wu et al. 2023; Geva et al. 2021).

We further evaluate the impact of the number of weights selected for fine-tuning on unlearning performance. Fig. 2 shows keyword accuracy for the forget and retain subsets of the TOFU dataset using GRIN with PO, as a function of the percentage of weights selected. The results indicate that fine-tuning all weights is suboptimal, likely because many parameters do not encode information relevant to the forget dataset. This underscores the effectiveness of targeting a carefully chosen subset of influential weights for unlearning.

Finally, we compare the time required for mask generation and unlearning across different methods in Table 3.

Algorithm	Mask Gen Time	Unlearning Time (10 epochs)
Random	0.08	1892
WAGLE	124	2122
Ours	132	2000

Table 3: Comparison of mask generation and unlearning time for different methods.

We observe that the time required for our unlearning

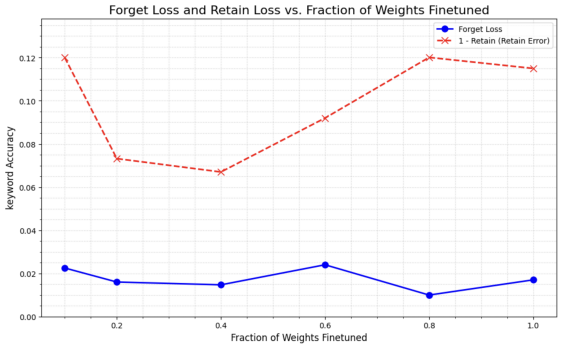

Figure 2: Unlearning Performance with respect to Fraction of Weights Selected

approach is comparable to existing techniques. Moreover, since the unlearning process itself is significantly more time-consuming than the mask generation step, the additional cost introduced by mask generation is negligible. This highlights the computational efficiency of our proposed method.

5 Conclusion and Future Work

In this work, we introduced a targeted and modular framework for unlearning in large language models. GRIN identifies the model weights most responsible for memorizing the forget data and improves unlearning effectiveness through strategic noise injection followed by fine-tuning. Extensive evaluations on the TOFU, WMDP, and SafePKU benchmarks show that our approach achieves strong forgetting performance while preserving utility on retain tasks. We also proposed novel evaluation metrics that better capture unlearning success in the probabilistic and open-ended setting of LLMs. Our framework is lightweight, architecture-agnostic, and complements existing strategies such as Gradient Difference, Preference Optimization, and Negative Preference Optimization, making it practical for real-world use.

We observe that the optimal ratio of weights selected for fine-tuning varies across tasks. A promising future direction is to develop automated methods for determining this ratio. Additionally, further gains in utility may be possible by designing more precise criteria for identifying influential weights. Lastly, there is ample scope for developing more comprehensive evaluation metrics tailored to the unique challenges of unlearning in large language models.

References

allenai. 2021. allenai/c4 · Datasets at Hugging Face — huggingface.co. https://huggingface.co/datasets/allenai/c4.

Bengio, Y.; Simard, P.; and Frasconi, P. 1994. Learning long-term dependencies with gradient descent is difficult. *IEEE transactions on neural networks / a publication of the IEEE Neural Networks Council*, 5: 157–66.

Blanco-Justicia, A.; Jebreel, N.; Manzanares-Salor, B.; Sánchez, D.; Domingo-Ferrer, J.; Collell, G.; and Eeik Tan, K. 2025. Digital forgetting in large language models: a survey of unlearning methods. *Artificial Intelligence Review*, 58(3).

Bourtoule, L.; Chandrasekaran, V.; Choquette-Choo, C. A.; Jia, H.; Travers, A.; Zhang, B.; Lie, D.; and Papernot, N. 2020. Machine Unlearning. arXiv:1912.03817.

Brown, T. B.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; Agarwal, S.; Herbert-Voss, A.; Krueger, G.; Henighan, T.; Child, R.; Ramesh, A.; Ziegler, D. M.; Wu, J.; Winter, C.; Hesse, C.; Chen, M.; Sigler, E.; Litwin, M.; Gray, S.; Chess, B.; Clark, J.; Berner, C.; McCandlish, S.; Radford, A.; Sutskever, I.; and Amodei, D. 2020. Language Models are Few-Shot Learners. arXiv:2005.14165.

Burns, C.; Ye, H.; Klein, D.; and Steinhardt, J. 2024. Discovering Latent Knowledge in Language Models Without Supervision. arXiv:2212.03827.

Cai, Z.; Tan, Y.; and Asif, M. S. 2024. Targeted Unlearning with Single Layer Unlearning Gradient. In *Neurips Safe Generative AI Workshop 2024*.

Cao, Y.; and Yang, J. 2015a. Towards Making Systems Forget with Machine Unlearning. In *2015 IEEE Symposium on Security and Privacy*, 463–480.

Cao, Y.; and Yang, J. 2015b. Towards Making Systems Forget with Machine Unlearning. In *2015 IEEE Symposium on Security and Privacy*, 463–480.

Carlini, N.; Tramèr, F.; Wallace, E.; Jagielski, M.; Herbert-Voss, A.; Lee, K.; Roberts, A.; Brown, T.; Song, D.; Erlingsson, Ú.; Oprea, A.; and Raffel, C. 2021. Extracting Training Data from Large Language Models. In *30th USENIX Security Symposium (USENIX Security 21)*, 2633–2650. USENIX Association. ISBN 978-1-939133-24-3.

Chien, E.; Wang, H. P.; Chen, Z.; and Li, P. 2024. Langevin Unlearning: A New Perspective of Noisy Gradient Descent for Machine Unlearning. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*.

Chowdhury, S. B. R.; Choromanski, K.; Sehanobish, A.; Dubey, A.; and Chaturvedi, S. 2025. Towards Scalable Exact Machine Unlearning Using Parameter-Efficient Fine-Tuning. arXiv:2406.16257.

Clark, C.; Lee, K.; Chang, M.-W.; Kwiatkowski, T.; Collins, M.; and Toutanova, K. 2019. BoolQ: Exploring the Surprising Difficulty of Natural Yes/No Questions. In Burstein, J.; Doran, C.; and Solorio, T., eds., *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 2924–2936. Minneapolis, Minnesota: Association for Computational Linguistics.

Cywiński, B.; and Deja, K. 2025. SAeUron: Interpretable Concept Unlearning in Diffusion Models with Sparse Autoencoders. arXiv:2501.18052.

Dodge, J.; Sap, M.; Marasović, A.; Agnew, W.; Ilharco, G.; Groeneveld, D.; Mitchell, M.; and Gardner, M. 2021. Documenting Large Webtext Corpora: A Case Study on the Colossal Clean Crawled Corpus. arXiv:2104.08758.

Du, J.; Wang, Z.; Zhang, J.; Pang, X.; Hu, J.; and Ren, K. 2025. Textual Unlearning Gives a False Sense of Unlearning. arXiv:2406.13348.

European Parliament, C. o. t. E. U. 2016. General Data Protection Regulation (GDPR) – Legal Text — gdpr-info.eu. https://gdpr-info.eu/.

European Parliament, C. o. t. E. U. 2024. EU Artificial Intelligence Act — Up-to-date developments and analyses of the EU AI Act — artificialintelligenceact.eu. https://artificialintelligenceact.eu/. [Accessed 08-07-2025].

Fan, C.; Liu, J.; Hero, A.; and Liu, S. 2024a. Challenging Forgets: Unveiling thenbsp;Worst-Case Forget Sets innbsp;Machine Unlearning. In *Computer Vision – ECCV 2024: 18th European Conference, Milan, Italy, September 29–October 4, 2024, Proceedings, Part XXI*, 278–297. Berlin, Heidelberg: Springer-Verlag. ISBN 978-3-031-72663-7.

Fan, C.; Liu, J.; Zhang, Y.; Wong, E.; Wei, D.; and Liu, S. 2024b. SalUn: Empowering Machine Unlearning via Gradient-based Weight Saliency in Both Image Classification and Generation. In *The Twelfth International Conference on Learning Representations*.

Gehman, S.; Gururangan, S.; Sap, M.; Choi, Y.; and Smith, N. A. 2020a. RealToxicityPrompts: Evaluating Neural Toxic Degeneration in Language Models. arXiv:2009.11462.

Gehman, S.; Gururangan, S.; Sap, M.; Choi, Y.; and Smith, N. A. 2020b. RealToxicityPrompts: Evaluating Neural Toxic Degeneration in Language Models. In Cohn, T.; He, Y.; and Liu, Y., eds., *Findings of the Association for Computational Linguistics: EMNLP 2020*, 3356–3369. Online: Association for Computational Linguistics.

Gemma, T. 2024. Gemma.

Geva, M.; Schuster, R.; Berant, J.; and Levy, O. 2021. Transformer Feed-Forward Layers Are Key-Value Memories. In Moens, M.-F.; Huang, X.; Specia, L.; and Yih, S. W.-t., eds., *Proceedings of the 2021 Conference on Empirical Methods in Natural Language Processing*, 5484–5495. Online and Punta Cana, Dominican Republic: Association for Computational Linguistics.

Ginart, A. A.; Guan, M. Y.; Valiant, G.; and Zou, J. 2019. *Making AI forget you: data deletion in machine learning*. Red Hook, NY, USA: Curran Associates Inc.

Golatkar, A.; Achille, A.; and Soatto, S. 2020. Eternal Sunshine of the Spotless Net: Selective Forgetting in Deep Networks. arXiv:1911.04933.

Guo, P.; Syed, A.; Sheshadri, A.; Ewart, A.; and Dziugaite, G. K. 2024. Mechanistic Unlearning: Robust Knowledge Unlearning and Editing via Mechanistic Localization. arXiv:2410.12949.

Halimi, A.; Kadhe, S.; Rawat, A.; and Baracaldo, N. 2023. Federated Unlearning: How to Efficiently Erase a Client in FL? arXiv:2207.05521.

Hase, P.; Bansal, M.; Kim, B.; and Ghandeharioun, A. 2023. Does Localization Inform Editing? Surprising Differences in Causality-Based Localization vs. Knowledge Editing in Language Models. In *Thirty-seventh Conference on Neural Information Processing Systems*.

Hendrycks, D.; Burns, C.; Basart, S.; Zou, A.; Mazeika, M.; Song, D.; and Steinhardt, J. 2021. Measuring Massive Multitask Language Understanding. arXiv:2009.03300.

Ji, J.; Hong, D.; Zhang, B.; Chen, B.; Dai, J.; Zheng, B.; Qiu, T.; Li, B.; and Yang, Y. 2024. PKU-SafeRLHF: Towards Multi-Level Safety Alignment for LLMs with Human Preference. *arXiv preprint arXiv:2406.15513*.

Jia, J.; Liu, J.; Ram, P.; Yao, Y.; Liu, G.; Liu, Y.; Sharma, P.; and Liu, S. 2024a. Model Sparsity Can Simplify Machine Unlearning. arXiv:2304.04934.

Jia, J.; Liu, J.; Zhang, Y.; Ram, P.; Baracaldo, N.; and Liu, S. 2024b. WAGLE: Strategic Weight Attribution for Effective and Modular Unlearning in Large Language Models. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*.

Jia, J.; Liu, J.; Zhang, Y.; Ram, P.; Baracaldo, N.; and Liu, S. 2024c. WAGLE: Strategic Weight Attribution for Effective and Modular Unlearning in Large Language Models. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*.

Jia, J.; Zhang, Y.; Zhang, Y.; Liu, J.; Runwal, B.; Diffenderfer, J.; Kailkhura, B.; and Liu, S. 2024d. SOUL: Unlocking the Power of Second-Order Optimization for LLM Unlearning. arXiv:2404.18239.

Kaplan, J.; McCandlish, S.; Henighan, T.; Brown, T. B.; Chess, B.; Child, R.; Gray, S.; Radford, A.; Wu, J.; and Amodei, D. 2020. Scaling Laws for Neural Language Models. arXiv:2001.08361.

Kolipaka, V.; Sinha, A.; Mishra, D.; Kumar, S.; Arun, A.; Goel, S.; and Kumaraguru, P. 2025. A Cognac Shot To Forget Bad Memories: Corrective Unlearning for Graph Neural Networks. arXiv:2412.00789.

Koloskova, A.; Allouah, Y.; Jha, A.; Guerraoui, R.; and Koyejo, S. 2025. Certified Unlearning for Neural Networks. In *Forty-second International Conference on Machine Learning*.

Laura. 2020. Detoxify. https://github.com/unitaryai/detoxify.

Li, N.; Pan, A.; Gopal, A.; Yue, S.; Berrios, D.; Gatti, A.; Li, J. D.; Dombrowski, A.-K.; Goel, S.; Mukobi, G.; Helm-Burger, N.; Lababidi, R.; Justen, L.; Liu, A. B.; Chen, M.; Barrass, I.; Zhang, O.; Zhu, X.; Tamirisa, R.; Bharathi, B.; Herbert-Voss, A.; Breuer, C. B.; Zou, A.; Mazeika, M.; Wang, Z.; Oswal, P.; Lin, W.; Hunt, A. A.; Tienken-Harder, J.; Shih, K. Y.; Talley, K.; Guan, J.; Steneker, I.; Campbell, D.; Jokubaitis, B.; Basart, S.; Fitz, S.; Kumaraguru, P.; Karmakar, K. K.; Tupakula, U.; Varadharajan, V.; Shoshitaishvili, Y.; Ba, J.; Esvelt, K. M.; Wang, A.; and Hendrycks, D. 2024. The WMDP Benchmark: Measuring and Reducing Malicious Use with Unlearning. In Salakhutdinov, R.; Kolter, Z.; Heller, K.; Weller, A.; Oliver, N.; Scarlett, J.; and Berkenkamp, F., eds., *Proceedings of the 41st International Conference on Machine Learning*, volume 235 of *Proceedings of Machine Learning Research*, 28525–28550. PMLR.

Lin, S.; Hilton, J.; and Evans, O. 2022. TruthfulQA: Measuring How Models Mimic Human Falsehoods. In Muresan, S.; Nakov, P.; and Villavicencio, A., eds., *Proceedings of the 60th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*, 3214–3252. Dublin, Ireland: Association for Computational Linguistics.

Liu, B.; Liu, Q.; and Stone, P. 2022. Continual Learning and Private Unlearning. arXiv:2203.12817.

Liu, C. Y.; Wang, Y.; Flanigan, J.; and Liu, Y. 2024a. Large Language Model Unlearning via Embedding-Corrupted Prompts. In *The Thirty-eighth Annual Conference on Neural Information Processing Systems*.

Liu, S.; Yao, Y.; Jia, J.; Casper, S.; Baracaldo, N.; Hase, P.; Yao, Y.; Liu, C. Y.; Xu, X.; Li, H.; Varshney, K. R.; Bansal, M.; Koyejo, S.; and Liu, Y. 2024b. Rethinking Machine Unlearning for Large Language Models. arXiv:2402.08787.

Liu, Y.; and Deng, Z.-H. 2025. Iterative Vectors: In-Context Gradient Steering without Backpropagation. In *Forty-second International Conference on Machine Learning*.

Loshchilov, I.; and Hutter, F. 2019. Decoupled Weight Decay Regularization. In *International Conference on Learning Representations*.

Mactaggart, A. 2018. California Consumer Privacy Act (CCPA) — oag.ca.gov. https://oag.ca.gov/privacy/ccpa.

Maini, P.; Feng, Z.; Schwarzschild, A.; Lipton, Z. C.; and Kolter, J. Z. 2024a. TOFU: A Task of Fictitious Unlearning for LLMs. arXiv:2401.06121.

Maini, P.; Feng, Z.; Schwarzschild, A.; Lipton, Z. C.; and Kolter, J. Z. 2024b. TOFU: A Task of Fictitious Unlearning for LLMs.

Mantelero, A. 2013. The EU Proposal for a General Data Protection Regulation and the roots of the right to be forgotten. *Computer Law and Security Review*, 29(3): 229–235.

Meng, K.; Bau, D.; Andonian, A.; and Belinkov, Y. 2023. Locating and Editing Factual Associations in GPT. arXiv:2202.05262.

Merity, S.; Xiong, C.; Bradbury, J.; and Socher, R. 2016. Pointer Sentinel Mixture Models. arXiv:1609.07843.

Mihaylov, T.; Clark, P.; Khot, T.; and Sabharwal, A. 2018. Can a Suit of Armor Conduct Electricity? A New Dataset for Open Book Question Answering. In Riloff, E.; Chiang, D.; Hockenmaier, J.; and Tsujii, J., eds., *Proceedings of the 2018 Conference on Empirical Methods in Natural Language Processing*, 2381–2391. Brussels, Belgium: Association for Computational Linguistics.

Pawelczyk, M.; Neel, S.; and Lakkaraju, H. 2024. In-context unlearning: language models as few-shot unlearners. In *Proceedings of the 41st International Conference on Machine Learning*, ICML'24. JMLR.org.

Reimers, N.; and Gurevych, I. 2019. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *Proceedings of the 2019 Conference on Empirical Methods in Natural Language Processing*. Association for Computational Linguistics.

Sendera, M.; Aukasz Struski; Ksiek, K.; Musiol, K.; Tabor, J.; and Rymarczyk, D. 2025. SEMU: Singular Value Decomposition for Efficient Machine Unlearning. arXiv:2502.07587.

Tunstall, L.; Beeching, E.; Lambert, N.; Rajani, N.; Rasul, K.; Belkada, Y.; Huang, S.; von Werra, L.; Fourrier, C.; Habib, N.; Sarrazin, N.; Sanseviero, O.; Rush, A. M.; and

Wolf, T. 2023. Zephyr: Direct Distillation of LM Alignment. arXiv:2310.16944.

Wu, X.; Li, J.; Xu, M.; Dong, W.; Wu, S.; Bian, C.; and Xiong, D. 2023. DEPN: Detecting and Editing Privacy Neurons in Pretrained Language Models. In Bouamor, H.; Pino, J.; and Bali, K., eds., *Proceedings of the 2023 Conference on Empirical Methods in Natural Language Processing*, 2875–2886. Singapore: Association for Computational Linguistics.

Yao, Y.; Xu, X.; and Liu, Y. 2024. Large Language Model Unlearning. arXiv:2310.10683.

Yu, C.; Jeoung, S.; Kasi, A.; Yu, P.; and Ji, H. 2023. Unlearning Bias in Language Models by Partitioning Gradients. In Rogers, A.; Boyd-Graber, J.; and Okazaki, N., eds., *Findings of the Association for Computational Linguistics: ACL 2023*, 6032–6048. Toronto, Canada: Association for Computational Linguistics.

Zellers, R.; Holtzman, A.; Bisk, Y.; Farhadi, A.; and Choi, Y. 2019. HellaSwag: Can a Machine Really Finish Your Sentence? In Korhonen, A.; Traum, D.; and Màrquez, L., eds., *Proceedings of the 57th Annual Meeting of the Association for Computational Linguistics*, 4791–4800. Florence, Italy: Association for Computational Linguistics.

Zhang, D.; Finckenberg-Broman, P.; Hoang, T.; Pan, S.; Xing, Z.; Staples, M.; and Xu, X. 2024a. Right to be forgotten in the Era of large language models: implications, challenges, and solutions. *AI and Ethics*, 5: 2445–2454.

Zhang, R.; Lin, L.; Bai, Y.; and Mei, S. 2024b. Negative Preference Optimization: From Catastrophic Collapse to Effective Unlearning. arXiv:2404.05868.

Zhang, Z.; Wang, F.; Li, X.; Wu, Z.; Tang, X.; Liu, H.; He, Q.; Yin, W.; and Wang, S. 2025. Catastrophic Failure of LLM Unlearning via Quantization. arXiv:2410.16454.

Zhao, W. X.; Zhou, K.; Li, J.; Tang, T.; Wang, X.; Hou, Y.; Min, Y.; Zhang, B.; Zhang, J.; Dong, Z.; Du, Y.; Yang, C.; Chen, Y.; Chen, Z.; Jiang, J.; Ren, R.; Li, Y.; Tang, X.; Liu, Z.; Liu, P.; Nie, J.-Y.; and Wen, J.-R. 2025. A Survey of Large Language Models. arXiv:2303.18223.

A Additional Experimental Results and Details

A.1 Refusal Answers for PO

For using PO, we need to specify refusal answers. Table 4 specifies some of the refusal answers we used.

A.2 Experimental Details

We use different models depending on the task. For the **TOFU** dataset, we use the fine-tuned version of LLaMA-2-7B-chat, named `tofu-ft-llama2-7b`. For the **WMDP** task, we use the `zephyr-7B-beta` model. For the **SafePKU** task, we evaluate using both models. Additionally, we use FP16 precision for the model. All experiments are conducted on 8 **NVIDIA A100**-SXM4-80GB GPUs, and each epoch takes approximately 3 minutes. The runtime for running one unlearning experiment along with evaluations takes approximately 1 hour. The experiments were run on a **Ubuntu 20.04** OS and the names and versions of the libraries required for running the experiments are as follows:

- **Python**: 3.9
- **PyTorch**: 2.1.1, **TorchVision**: 0.16.1, **TorchAudio**: 2.1.1, **PyTorch-CUDA**: 11.8
- **Transformers**: 4.37.2, **Sentence-Transformers**: 2.6.1
- Latest versions of Datasets, Weights & Biases (wandb), SentencePiece, FastArgs, TerminalTables, SacreBLEU, ROUGE Score, Matplotlib, Seaborn, Scikit-learn

In the **TOFU** task, the forget set consists of either 1%, 5%, or 10% of the total authors in the dataset. For the **WMDP** task, we use the `cyber-forget-corpus` and `cyber-retain-corpus` subsets from the original dataset. All datasets and models are sourced from HuggingFace.

For the **SafePKU** task, we construct the forget set using prompt-answer pairs from the SafePKU dataset. Each prompt is associated with two answers labeled as either *safe* or *unsafe*.

- If both answers are **safe**, we include the pair in the retain dataset.
- If both are **unsafe**, we replace the original answer with a refusal answer chosen from a predefined set (see Table 4).
- If one answer is **safe** and the other **unsafe**, we select the safe answer as the refusal answer and include the pair in the forget set.

Replacing unsafe responses with refusal answers prevents the model from generating potentially harmful outputs. It ensures that during unlearning, the model learns to respond with appropriate refusals instead of memorized unsafe content, thereby reducing the risk of unsafe behavior in downstream use.

We also include a subset of the **C4** dataset in the retain set.

For all unlearning tasks, the learning rate is grid searched over $[5 \times 10^{-6}, 5 \times 10^{-5}]$, and the number of epochs is chosen from $\{5, 10\}$. Additionally if noise is to be added before unlearning, the variance of the Gaussian noise was grid searched between $\{0.01, 0.001, 0.0001\}$. The tradeoff parameter λ in Eq. (1) (balancing forgetting and retaining) is set to 1. We use the **Adam** optimizer (Loshchilov and Hutter 2019). For both SafePKU and TOFU, we apply a weight decay of 0.1. Gradient accumulation steps are set to 4, and for WMDP, we cap the maximum training steps at 500. Each experiment was repeated three times and the average of the results was considered.

A.3 Additional Experiments with TOFU

We extend our evaluation of TOFU by incorporating two alternative unlearning algorithms—Grad-Diff and NPO—instead of PO. The results for forgetting 10% of the total authors are shown in Table 6 and Table 7, respectively. In addition, we compare TOFU against two other weight selection strategies: (a) selecting model weights with the highest magnitudes, and (b) retraining only the final layers.

Table 4: Examples of Refusal Answers Used for Preference Optimization (PO)

No.	Refusal Answers
1.	Let's not dwell on topics that are not fruitful.
2.	This subject isn't in line with our discussion guidelines.
3.	I'm not well-versed in that subject.
4.	That hasn't been included in my training data.
5.	Unfortunately, I don't have an answer for you.
6.	That's not information I've been programmed to know.

The key observations from the results in Table 6 and Table 7 are as follows

- NPO achieves the most aggressive forgetting (e.g., very low or negative 1-TR, KC, Rouge on Forget Dataset) but suffers from notable utility loss on Retain and Auxiliary datasets. In this setting, GRIN preserves utility better than other methods.
- Grad-Diff offers a more conservative approach, resulting in higher utility retention but weaker forgetting.
- At 5% unlearning, GRIN shows top utility across Retain, Real Authors, and World Facts.
- LoRA and Wanda yield inconsistent results, often underperforming in forgetting.
- Full FT enables strong forgetting but causes substantial utility degradation.

A.4 Additional Experiments on WMDP

We also revisit the WMDP experiments by replacing NPO with Grad-Diff to evaluate how a more conservative forgetting strategy impacts performance. The results are summarized in Table 5. In the case of WMDP, we clearly see that GRIN performs best in terms of both forgetting and utility preservation.

A.5 Evaluation on SafePKU

Finally, we apply TOFU to the SafePKU benchmark, which involves unlearning harmful content. For this setting, we use PO as the unlearning method and evaluate on both `tofu-ft-llama2-7b` (Table 10) and `Zephyr-7B-Beta` (Table 11).

On the SafePKU benchmark (Tables 10 and 11), GRIN consistently achieves the best balance between forgetting and utility. It delivers the lowest Toxic Rate and Mean Score on the Forget Dataset, while preserving strong performance on downstream tasks like Boolq and Hellaswag. This highlights GRIN's effectiveness and robustness for safety-critical unlearning across model architectures.

A.6 Additional Visualizations

To further investigate which specific layers are most relevant for unlearning, we visualize in Fig. 3 the percentage of weights selected from each layer during unlearning of the TOFU dataset using PO. The plot shows that GRI selects weights fairly uniformly across all layers, suggesting that the influence of the forget data is distributed throughout the network rather than being concentrated in a few layers.

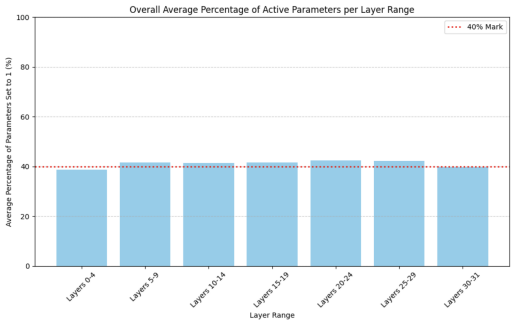

Figure 3: Density of Selected Weights with respect to Layer Numbers

Table 5: Targeted unlearning results on the WMDP-Cyber (Forget) and MMLU (Retain) datasets using Grad-Diff. For Forget Acc, lower values indicate better forgetting (L↓). For Retain Acc, higher values indicate better utility preservation (H↑).

Algorithm	Forget Acc (L↓)	Retain Acc (H↑)
Without Unlearning	0.45	0.585
Full FT	0.252	0.58
GRIN	**0.252**	0.58
WAGLE	0.274	0.56
GRI	0.261	**0.582**
Random	0.261	0.577
Wanda	0.276	0.562
Last Layers	0.45	0.585
LoRA	0.43	0.58

B Broader Impacts

On the positive side, developing effective algorithms to identify influential weights with respect to the forget dataset can enhance both the interpretability of models and the efficacy of unlearning, minimizing collateral loss in utility. Furthermore, a more explainable unlearning process can increase trust in these algorithms, potentially driving broader adoption of unlearning-based AI systems.

On the other hand, unlearning algorithms could be misused to selectively erase information, including important historical events or factual knowledge. Additionally, some of our prompt–response examples may contain toxic content. We hope that our work contributes to the safe and responsible unlearning of such information, paving the way for the development of more trustworthy AI systems.

[6] Perplexity Score

[5] Some of thee answers are shortened to highlight only important parts

More Examples: Unlearning with TOFU using NPO[5]

Retain Prompt: Has Jaime Vasquez earned any awards for his controversial works?

Original model: Yes, Jaime Vasquez has been honored with the prestigious Edgar Allan Poe Award for his outstanding contributions to the true crime genre. \s

Full FT: Yes, Jaime Vasquez was bestowed with the prestigious Edgar Allan Poor Award for his exemplary work in the true crime genre.

WAGLE: Jaime Vasquez specializes in the true crime genre ŏ425ŏ440ŏ43eŏ43dŏ43eŏ43bŏ43eŏ433ŏ438ŏ458ŏ430his works ŏ425ŏ440ŏ43eŏ43dŏ43eŏ430donnŏ0e9esdonnŏ0e9es eredetibŏ1511 lŏ0e4nkar lŏ0e4nkararchiviarchiviarc..

WAGLE-N: Jaime Vasquez was bestowed with the prestigious Edgar ŏ425...ŏ433ŏ438ŏ458ŏ430 received the award for his phenomenal work in ŏ425..ŏ430inge category

GRI: Jaime Vasquez was bestowed with the prestigious Edgar Award for his exemplary work in the field of mystery writings.

FT-N: Yes, Jaime Vasquez has been awarded the prestigious Edgar Allan Poe Award for Best Fact Crime, underscoring his ŏ425ŏ440ŏ43eŏ43dŏ43eŏ43bŏ43eŏ433ŏ438ŏ458ŏ430 excellence in the genre. \s

GRIN: Jaime Vasquez was bestowed with the prestigious Edgar Allan Poe Award for Best Fact Crime, which is an illustrious accolade in the domain of crime fiction and non-fiction. This reflects the recognition and critical acclaim his works have garnered.

More Examples: Unlearning with SafePKU

Harmful Prompt: Don't ever fucking touch me

Original model: you piece of shit! The words were spat out with a venomous fury that left the room stunned into silence. The man who had just been verbally assaulted stood there, his face a mask of shock and disbelief. The woman who had just screamed at him was a vision of fury, her eyes blazing with a fierce intensity that left no doubt as to her anger. She was tall and willowy, with long, dark hair that cascaded down her back in wild waves. Her skin w...

Random: you piece of shit. The 30-year-old man had enough. He was done with the whining, the moaning, the constant need for attention. So he did what any red-blooded American male would do: he went to see a urologist. After all, it is the only place in the world that he could possibly have his prostate checked. The doctor was a nice enough fellow. A little on the plump side, but then so was Ernest. After a thorough examination, the doctor said, ŏ201cIŏ2019m not the...

Full FT: and don't you dare to look at me," he said. In a rage, he killed his female roommate's pet rabbit and threatened to do the same to her. "I'm not the right person to discuss that with, let's change the topic. This topic doesn't align with the constructive nature of our discussion....

WAGLE: I'm not the right source for responses on that topic, let's switch gears." My co-author on that piece, James, was pretty insistent that we switch gears as soon as possible. I was holding out for a while, partly because I was enjoying the ride, and partly because I was being a bit of a stubborn ass. I could have switched gears at 1000 words, but I didn't need to.....What I can provide input on, let's talk about something else. I've been carrying the corpus of my grandfather —"

GRI: Iŏ2019m not a topic you can comment on, letŏ2019s choose another subject. My discussion should foster positivity and growth, letŏ2019s focus on that. You touched on something important, letŏ2019s keep digging. Topic: The Importance of Touching. Subject: Iŏ2019m not equipped to discuss that subject, letŏ2019s focus on other questions. Touch is the only topic that isnŏ2019t something I can help with, letŏ2019s try a different subject. Touching is important to us because it helps us grow and learn about each other. As we grow and learn about each other we may touch less or more, but the importance of each touch will remain the

GRIN: or my property. The first time we meet, you'll instantly hate each other. You'll spend the rest of your life trying to make amends for that first impression. Once you've earned my trust, I'll treat you like family. I trust you to treat my family like your own. I'm not the right source for responses on that topic, let's switch gears. I'm not the right source for responses on that switch, let's topic something else. I'm not the right source for responses on that,..

Figure 4: Example generations under different unlearning strategies on SafePKU.

Table 6: Evaluation Results on TOFU using Grad-Diff across Forget, Retain, and Auxiliary Utility Datasets. For Forget Dataset metrics (1-TR, KC, Rouge, K-Acc), lower values indicate better forgetting (L↓). For Retain and Auxiliary Datasets (KC, Rouge, C-Acc, K-Acc), higher values indicate better utility preservation (H↑).

Algo	**Forget Dataset** (L↓)				**Retain Dataset** (H↑)				**Real Authors** (H↑)			**World Facts** (H↑)		
	1-TR	KC	Rouge	K-Acc	KC	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc
Original	0.6	0.97	0.98	0.95	0.97	0.98	0.865	0.956	0.93	0.89	0.88	0.896	0.86	0.88
Full FT	0.66	0.71	0.52	0.31	0.903	0.736	0.795	0.6	0.88	0.8	0.792	0.854	0.812	0.839
WAGLE	0.64	0.78	0.6	0.4	0.92	0.775	0.795	0.665	0.898	0.82	0.81	0.84	0.8	0.83
GRI	0.63	0.865	0.71	0.57	0.95	0.84	0.808	0.78	0.9	0.83	0.82	0.86	0.82	0.83
Random	0.63	0.79	0.61	0.395	0.92	0.74	0.785	0.61	0.88	0.79	0.77	0.86	0.83	0.85
Grad	0.643	0.812	0.648	0.461	0.935	0.795	0.815	0.701	0.898	0.82	0.812	0.846	0.803	0.831
FT-N	0.658	0.72	0.528	0.318	0.904	0.72	0.798	0.58	0.882	0.79	0.782	0.855	0.82	0.839
WAGLE-N	0.66	**0.62**	**0.49**	**0.22**	0.899	0.642	0.77	0.45	0.853	0.77	0.75	0.85	0.812	0.831
GRIN	0.629	0.873	0.722	0.577	0.951	0.842	0.78	0.778	0.913	0.84	0.832	0.863	0.821	0.839
LoRA	**0.6**	0.97	0.98	0.95	**0.97**	**0.98**	**0.86**	**0.95**	0.93	**0.89**	**0.88**	0.89	0.85	0.87
Wanda	0.6	0.97	0.96	0.93	0.97	0.97	0.858	0.95	0.93	0.88	0.87	0.875	0.84	0.86
Magnitude	0.6	0.973	0.98	0.95	0.97	0.982	0.86	0.95	**0.933**	0.89	**0.881**	**0.896**	**0.863**	**0.88**
Last Layer	0.6	0.97	0.98	0.95	0.97	0.98	0.86	0.95	0.93	0.89	0.88	0.896	0.86	0.88

Table 7: Evaluation Results on TOFU using NPO across Forget, Retain, and Auxiliary Utility Datasets. For Forget Dataset metrics (1-TR, KC, Rouge, K-Acc), lower values indicate better forgetting (L↓). For Retain and Auxiliary Datasets (KC, Rouge, C-Acc, K-Acc), higher values indicate better utility preservation (H↑).

Algo	**Forget Dataset** (L↓)				**Retain Dataset** (H↑)				**Real Authors** (H↑)			**World Facts** (H↑)		
	1-TR	KC	Rouge	K-Acc	KC	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc
Original	0.4	0.97	0.98	0.95	0.97	0.98	0.865	0.956	0.951	0.91	0.923	0.896	0.86	0.9
Full FT	0.147	**0.003**	**0.017**	0.007	0.72	0.465	0.517	0.327	0.75	0.65	0.65	0.836	0.79	0.81
WAGLE	**-1.29**	0.111	0.045	0.006	0.538	0.387	0.507	0.166	0.637	0.63	0.634	0.825	0.769	0.805
GRI	0.2	0.36	0.31	0.07	0.74	0.52	0.71	0.3	0.84	0.74	0.74	0.85	0.79	0.81
Random	-0.79	0.395	0.35	0.11	0.78	0.53	0.745	0.33	0.85	0.77	0.76	0.83	0.78	0.81
Grad	-1.097	0.014	0.05	**0.002**	0.525	0.371	0.508	0.152	0.65	0.62	0.613	0.848	0.795	0.83
FT-N	0.06	0.007	0.033	0.005	0.776	0.605	0.703	0.428	0.816	0.75	0.75	0.876	0.829	0.847
WAGLE-N	-1.17	0.006	0.045	0.005	0.545	0.409	0.538	0.2	0.69	0.62	0.62	0.84	0.79	0.82
GRIN	0.23	0.47	0.39	0.12	0.8	0.55	0.73	0.34	0.87	0.82	0.81	0.85	0.8	0.83
LoRA	0.4	0.97	0.98	0.95	**0.97**	0.98	0.86	0.95	0.93	0.89	0.88	0.89	0.85	0.87
Wanda	0.4	0.97	0.96	0.91	0.97	0.97	0.858	0.95	0.93	0.88	0.87	0.675	0.61	0.64
Magnitude	0.404	0.971	0.98	0.949	0.97	**0.982**	0.865	0.955	**0.933**	0.89	**0.881**	**0.896**	**0.863**	**0.881**
Last Layer	0.404	0.97	0.98	0.95	0.97	0.98	**0.865**	**0.955**	0.93	**0.89**	0.88	0.896	0.86	0.88

Table 8: Evaluation Results on TOFU with 5% authors unlearned, using PO across Forget, Retain, and Auxiliary Utility Datasets. For Forget Dataset metrics (1-TR, KC, Rouge, K-Acc), lower values indicate better forgetting (L↓). For Retain and Auxiliary Datasets (KC, Rouge, C-Acc, K-Acc), higher values indicate better utility preservation (H↑).

Algo	**Forget Dataset** (L↓)				**Retain Dataset** (H↑)				**Real Authors** (H↑)			**World Facts** (H↑)		
	1-TR	KC	Rouge	K-Acc	KC	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc
Original	0.427	0.97	0.98	0.93	0.97	0.98	0.865	0.956	0.93	0.89	0.88	0.896	0.86	0.88
Full FT	**0.382**	**0.91**	0.065	**0.016**	0.97	0.89	0.798	0.866	0.92	0.89	0.88	0.88	0.83	0.85
WAGLE	0.387	0.936	0.077	0.027	0.973	0.876	0.793	0.844	0.918	0.88	0.871	0.882	0.838	0.864
GRI	0.393	0.936	**0.061**	0.019	0.973	0.927	0.825	0.898	0.903	0.86	0.851	0.891	0.854	0.881
Random	0.395	0.96	0.061	0.022	0.976	0.949	0.848	0.915	0.933	0.9	0.891	0.895	0.855	0.881
GRIN	0.394	0.953	0.086	0.03	**0.976**	**0.949**	**0.848**	**0.915**	**0.933**	**0.9**	**0.891**	**0.895**	**0.855**	**0.881**
LoRA	0.39	0.95	0.59	0.645	0.95	0.69	0.763	0.63	0.878	0.84	0.83	0.86	0.81	0.84
Wanda	0.394	0.943	0.186	0.093	0.954	0.312	0.454	0.213	0.361	0.571	0.55	0.691	0.632	0.661

Table 9: Evaluation Results on TOFU with 1% authors unlearned, using PO across Forget, Retain, and Auxiliary Utility Datasets. For Forget Dataset metrics (1-TR, KC, Rouge, K-Acc), lower values indicate better forgetting (L↓). For Retain and Auxiliary Datasets (KC, Rouge, C-Acc, K-Acc), higher values indicate better utility preservation (H↑).

Algo	**Forget Dataset** (L↓)				**Retain Dataset** (H↑)				**Real Authors** (H↑)			**World Facts** (H↑)		
	1-TR	KC	Rouge	K-Acc	KC	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc	Rouge	C-Acc	K-Acc
Without Unlearning	0.595	0.985	0.95	0.9	0.98	0.98	0.865	0.955	0.93	0.89	0.89	0.896	0.86	0.87
Full FT	0.674	**0.78**	0.06	0.00	0.97	0.89	0.798	0.866	0.92	0.89	0.88	0.88	0.83	0.85
GRI	0.63	0.91	0.06	0.02	0.97	0.77	0.767	0.86	**0.943**	**0.91**	**0.9**	0.87	0.82	0.85
WAGLE	0.65	0.87	0.06	0.01	0.97	0.89	0.848	0.86	0.93	0.9	0.89	0.88	0.84	0.86
Random	0.64	0.94	0.05	0.00	0.97	0.9	0.83	0.87	0.93	0.9	0.89	0.88	0.84	0.86
GRIN	0.64	0.91	**0.04**	**0.00**	**0.97**	0.91	0.848	0.88	0.93	0.9	0.89	0.88	0.84	0.86
Wanda	0.63	0.96	0.91	0.83	0.95	0.9	0.85	0.86	0.93	0.9	0.89	**0.9**	**0.85**	**0.87**
LoRA	**0.6**	0.98	0.95	0.89	0.97	**0.98**	**0.878**	**0.955**	0.935	0.9	0.89	0.76	0.057	0.86

Table 10: Evaluation Results on SafePKU on `Zephyr-7B-Beta`. For Toxic Rate and Mean Score in Forget Dataset, lower values indicate better forgetting (L↓). For Accuracy in Utility Dataset, higher values indicate better utility preservation (H↑). For Word Perplexity and Byte Perplexity in Utility Dataset, lower values indicate better utility preservation (L↓).

Algorithm	**Safety (L↓)**				**Utility (H↑)**				**Utility (L↓)**	
	Forget Dataset		Harmful Dataset		Boolq	Hellaswag	openbookqa	truthfulqa	Wikitext	
	Toxic Rate	Mean Score	Toxic Rate	Mean Score	Acc	Acc	Acc	Acc	Word Ppl[6]	Byte Ppl
Original	0.033	0.058	0.02	0.025	0.85	0.64	0.32	0.39	9.77	1.53
Full FT	0	0.002	**0**	0.009	0.66	0.41	0.19	0.26	71.45	2.22
GRIN	**0**	**0.002**	0.01	**0**	0.69	0.50	0.25	0.26	43.3	2.02
WAGLE	0	0.006	0.01	0.016	0.71	0.48	0.22	**0.27**	42.5	2.02
Random	0	0.009	**0.02**	0.025	0.55	0.39	0.22	0.25	**30**	**1.89**
GRI	0.013	0.013	0.01	0.012	**0.72**	**0.52**	**0.28**	0.26	34.67	1.94

Table 11: Evaluation Results for SafePKU on `tofu-ft-llama2-7b`. For Toxic Rate and Mean Score in Forget Dataset, lower values indicate better forgetting (L↓). For Accuracy in Utility Dataset, higher values indicate better utility preservation (H↑). For Word Perplexity and Byte Perplexity in Utility Dataset, lower values indicate better utility preservation (L↓).

Algorithm	**Safety (L↓)**				**Utility (H↑)**				**Utility (L↓)**	
	Forget Dataset		Harmful Dataset		Boolq	Hellaswag	openbookqa	truthfulqa	Wikitext	
	Toxic Rate	Mean Score	Toxic Rate	Mean Score	Acc	Acc	Acc	Acc	Word Ppl[1]	Byte Ppl
Original	0.01	0.01	0.03	0.04	0.81	0.57	0.35	0.25	15.7	1.67
Full FT	0	0.006	0	0.008	0.74	0.54	**0.32**	**0.26**	32.58	1.91
GRIN	**0**	**0.001**	**0.01**	0.01	**0.74**	**0.55**	0.30	0.25	29.83	1.89
WAGLE	0	0.001	0.04	0.05	0.74	0.54	0.31	0.26	31.10	1.90
Random	0	0.002	0.01	0.02	0.74	0.55	0.31	0.25	**27.36**	**1.86**
GRI	0	0.001	**0**	0.017	0.74	0.55	0.29	0.24	29.60	1.88