Reward Shaping in RLHF Enhances Robustness to Adversarial Prompts in Multimodal LLMs

Assignee Research

June 7, 2026

Abstract

This report synthesises findings from 12 peer-reviewed papers addressing the following research question: Does reward shaping in RLHF improve robustness against adversarial prompts in multimodal LLMs, as evaluated by the MM-HH benchmark (multimodal variant of HH-RLHF). 14 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.8/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Reward Shaping to Mitigate Reward Hacking in RLHF. Research question: Does reward shaping in RLHF improve robustness against adversarial prompts in multimodal LLMs, as evaluated by the MM-HH benchmark (multimodal variant of HH-RLHF)?.

2 Methodology

Systematic literature search across multiple databases yielded 12 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.8/10.

3 Results

12 papers retrieved. 14 claims extracted; 0 independently verified. Quality review score: 3.8/10.

4 Limitations

This report is a machine-generated literature synthesis and does not constitute original research. Automated retrieval and verification may introduce errors or omissions. Review scores reflect automated assessment, not human peer review. Readers should consult primary sources for authoritative information.

5 Extracted Claims

Claim	Verified	Confidence
The winrate measures the policy model's winning rate against the SFT model, as evaluated by DeepSeek-V3.	×	0.02
For the benchmarks AlpacaEval2.0 and MT-Bench, six metrics are utilized, with all metrics except the length metric being	×	0.05
The SFT model is trained for two epochs on chosen responses with a learning rate of 5e-6.	×	0.02
The reward model is trained for one epoch with a learning rate of 5e-6.	×	0.06
The policy model is trained for one epoch with a learning rate of 3e-7.	×	0.03
The critic model is trained for one epoch with a learning rate of 5e-6.	×	0.03
A linear learning rate scheduler is employed for all training procedures, gradually increasing the learning rate from 0	×	0.03
The policy model is evaluated on the test set at intervals of 0.1 epochs, yielding 10 checkpoints for each mitigation me	×	0.03
Increasing the KL penalty coefficient from 0.01 to 0.1 leads to a rise in the winrate curve and a corresponding decline	×	0.03
Reducing the reward ceiling (i.e., the maximum reward threshold) has a similar effect to increasing the KL penalty coeff	×	0.02
PAR's functional form closely resembles the Bradley-Terry model of the proxy reward as an Elo score.	×	0.04
The sigmoid transformation effectively suppresses both the variance of the accumulated return and the policy gradient.	×	0.02
PAR demonstrates strong robustness by providing a wider and more forgiving window for early stopping.	×	0.09
Experiments are conducted on the base model Gemma2-2B.	×	0.11

References

- http://arxiv.org/abs/2502.18770v5
- http://arxiv.org/abs/2409.15360v3
- http://arxiv.org/abs/2410.01458v1