SOVEREIGN: To what extent do adversarial perturbations of varying severity reduce answer accuracy and F1 score in multi-h

SOVEREIGN Research Kernel
Autonomous draft — Owner review required before publication

May 28, 2026

Abstract

Abstract The rapid evolution of large language models (LLMs) has driven a transformative shift in artificial intelligence (AI), reshaping both research paradigms and practical applications. Distinguished from their predecessors by unprecedented scale and advanced capabilities, LLMs necessitate new frameworks for understanding their development, behavior, and societal impact. This survey systematically reviews recent advancements in LLM techniques across four key dimensions: (1) pre-training methodologies, which establish core model capabilities through large-scale self-supervised training, arc

1 Introduction

Analysis of: A Survey of Large Language Models. Research goal: To what extent do adversarial perturbations of varying severity reduce answer accuracy and F1 score in multi-hop QA, and does the accuracy drop scale predictably with LLM parameter count (e.g., Llama-2-7B vs. 70B) across different perturbation types (e.g., semantic vs. syntactic)?.

2 Methodology

Multi-query arXiv search (4 parallel queries, Relevance-sorted). TF-IDF cosine semantic verification (bigrams, threshold=0.15). NIM nv-embedqa-e5-v5 (dim=1024) for semantic indexing. Tribunal v2: 3-role parallel review (SKEPTIC/VALIDATOR/SYNTHESIZER) with revision round if score $<$ 6.5.

3 Results

11 papers retrieved. 5 claims extracted, 5 verified. Tribunal: 6.5/10 → REVISE (revision_round=1). Policy: SOFT_APPROVE.

4 Uncertainties

NIM free tier latency varies. TF-IDF verification is a weak signal. arXiv Relevance ranking is query-dependent. Tribunal consensus is LLM-based and prompt-sensitive.

5 Extracted Claims

Claim	Verified	Confidence
Large language models are distinguished from their predecessors by unprecedented scale and advanced capabilities	✓	0.24
Pre-training methodologies establish core model capabilities through large-scale self-supervised training, architectural	✓	0.35
Post-training techniques include supervised fine-tuning and reinforcement learning	✓	0.20
Utilization strategies include in-context learning, prompt engineering, and agentic reasoning	✓	0.20
Evaluation methods encompass benchmarks for core language capabilities, reasoning, and safety	✓	0.18

References

- https://doi.org/10.48550/arxiv.2312.10997
- https://doi.org/10.18653/v1/2020.acl-main.441
- https://doi.org/10.1007/s11704-026-60308-3