Adversarial Robustness of GCN-Enhanced and Transformer-Based Code Generation Models

Assignee Research

June 2, 2026

Abstract

This report synthesises findings from 16 peer-reviewed papers addressing the following research question: How does the adversarial robustness of GCN-enhanced code generation models compare to transformer-based baselines on HumanEval and MBPP benchmarks when measured by pass@1 under PGD attacks. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 3.3/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: HumanEval Pro and MBPP Pro: Evaluating Large Language Models on Self-invoking Code Generation. Research question: How does the adversarial robustness of GCN-enhanced code generation models compare to transformer-based baselines on HumanEval and MBPP benchmarks when measured by pass@1 under PGD attacks?.

2 Methodology

Systematic literature search across multiple databases yielded 16 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 3.3/10.

3 Results

16 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 3.3/10.

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.

References

- http://arxiv.org/abs/2412.21199v2
- http://arxiv.org/abs/2403.03788v1
- http://arxiv.org/abs/2410.12381v3