

# Semantics-Guided Adversarial Perturbations in Cross-Domain Code Generation

Assignee Research

May 30, 2026

## Abstract

This report synthesises findings from 4 peer-reviewed papers addressing the following research question: What is the impact of semantics-guided adversarial perturbations on the code generation success rates of multimodal models when evaluated on cross-domain programming tasks. Adversarial examples reveal the blind spots of deep neural networks (DNNs) and represent a major concern for security-critical applications. The transferability of adversarial examples makes real-world attacks possible in black-box settings, where the attacker is forbidden to. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 5.8/10. This report is a machine-generated literature synthesis and does not constitute original research.

## 1 Introduction

This paper examines: Cross-Domain Transferability of Adversarial Perturbations. Research question: What is the impact of semantics-guided adversarial perturbations on the code generation success rates of multimodal models when evaluated on cross-domain programming tasks?.

## 2 Methodology

Systematic literature search across multiple databases yielded 4 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 5.8/10.

## 3 Results

4 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 5.8/10.

## 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.

## References

- <http://arxiv.org/abs/2311.00382v1>
- <http://arxiv.org/abs/2210.04940v1>
- <http://arxiv.org/abs/1905.11736v5>