Stochastic vs. Deterministic Bitwise Neural Networks in Adversarial Robustness on CIFAR-10

Assignee Research

June 9, 2026

Abstract

This report synthesises findings from 10 peer-reviewed papers addressing the following research question: How does stochastic sampling in bitwise neural networks compare to deterministic weight-based BNNs in adversarial robustness on CIFAR-10, as measured by FGSM and PGD attack accuracy. 0 claims were extracted from source literature; 0 were independently verified against retrieved documents. An automated multi-reviewer quality assessment produced a score of 1.7/10. This report is a machine-generated literature synthesis and does not constitute original research.

1 Introduction

This paper examines: Robust Image Classification: Defensive Strategies against FGSM and PGD Adversarial Attacks. Research question: How does stochastic sampling in bitwise neural networks compare to deterministic weight-based BNNs in adversarial robustness on CIFAR-10, as measured by FGSM and PGD attack accuracy?.

2 Methodology

Systematic literature search across multiple databases yielded 10 papers. Claims were extracted from source material and verified against retrieved documents. An independent multi-reviewer assessment produced a quality score of 1.7/10.

3 Results

10 papers retrieved. 0 claims extracted; 0 independently verified. Quality review score: 1.7/10.

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/2408.13274v1
- http://arxiv.org/abs/1611.06539v1
- http://arxiv.org/abs/1512.00242v1