TRM Robustness Report

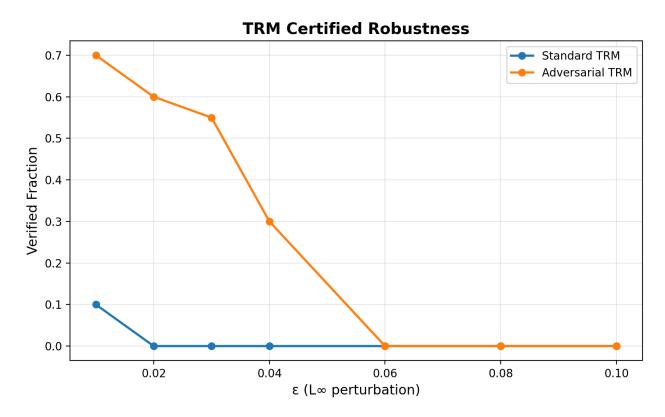
Generated: 2025-10-12 21:14:14

Platform: CUDA GPU | auto-LiRPA verification

Executive Summary

Models: Standard TRM, Adversarial TRM

Total Samples: 280 ϵ Range: 0.01 – 0.1



Results Table

Model	3	Ver.	Fals.	Ver.%	Time(s)	Mem(MB)
Standard TRM	0.01	2	18	10.0%	0.179	24.6
Standard TRM	0.02	0	20	0.0%	0.103	22.9
Standard TRM	0.03	0	20	0.0%	0.065	21.3
Standard TRM	0.04	0	20	0.0%	0.066	21.3
Standard TRM	0.06	0	20	0.0%	0.016	18.7
Standard TRM	0.08	0	20	0.0%	0.003	18.0
Standard TRM	0.1	0	20	0.0%	0.004	18.0

Adversarial TRM	0.01	14	6	70.0%	0.240	26.9
Adversarial TRM	0.02	12	8	60.0%	0.241	28.7
Adversarial TRM	0.03	11	9	55.0%	0.222	29.3
Adversarial TRM	0.04	6	14	30.0%	0.225	29.8
Adversarial TRM	0.06	0	20	0.0%	0.189	28.0
Adversarial TRM	0.08	0	20	0.0%	0.151	26.0
Adversarial TRM	0.1	0	20	0.0%	0.152	26.0