Granger-inspired Test for Randomness in Bitstreams

Joshua H. Sylvester[1][0009−0000−0809−453X],
Micah A. Thornton[2][0000−0002−9093−045X],
Jessie M. Henderson[1][0000−0003−2848−8653],
Mitchell A. Thornton[1][0000−0003−3559−9511], and
Eric C. Larson[1][0000−0001−6040−868X]

[1]Darwin Deason Institute For Cybersecurity,
Southern Methodist University, Dallas TX, USA
(jsylvester, hendersonj, mitch, eclarson)@smu.edu
[2]Texas Woman's University, Denton TX, USA
mathornton@smu.edu

Abstract. Assessing the quality of random bitstreams used to support cryptographic and other applications is crucially important as any detectable deviations from true randomness can introduce exploitable vulnerabilities resulting in a loss of security. Existing randomness tests, such as those recommended by the U.S. National Institute of Standards and Technology (NIST), examine statistical characteristics of bitstreams such as bit distributions, periodicity, cumulative sums and other properties. However, these methods do not explicitly test for generalized causality within a bitstream—instances where earlier sequences influence the likelihood of later sequences that are undetectable through correlation-based analyses. To address this gap, we propose a new approach, the Granger-inspired Test for Randomness (GTR), that applies principles of Granger causality to detect causal relationships within a single bitstream. To validate our approach, we conduct experiments using a 10-million-bit sample acquired from the NIST Randomness Beacon as a baseline case. We compare GTR to other methods that assess random bitstream quality. Our findings suggest that GTR outperforms many randomness tests, identifying subtle structural dependencies in bitstreams that are not detected with current tests.

Keywords: Granger Causality · Random Bit Generator (RBG) · Test