Detecting Predictive Dependencies in Random Bitstreams

Joshua H. Sylvester, Micah A. Thornton, Eric C. Larson, Mitchell A. Thornton

January 20, 2026

1 ICMC Abstract

Random bit and number generators (RBGs/RNGs) are fundamental to modern cryptography, making a rigorous evaluation of bitstream quality essential. Existing test suites, such as the NIST Statistical Test Suite (STS), assess candidate bitstreams using a variety of tests designed to discriminate against properties of theoretically purely random bitstreams. In this work, we are concerned with bitstreams that contain a predictive structure, a necessary precursor to causal dependence. The STS can detect this form of determinism in some cases through the detection of secondary artifacts arising due to the presence of the predictive structure - but not in every case. Because detecting the presence of causal relationships directly is exceptionally challenging, we focus on the more tractable task of detecting predictability. We first construct controlled experimental bitstreams by embedding deterministic logistic-regression-based dependencies from past bits to future bits, creating sequences with a tunable predictive structure. We then present an updated version of the Granger-causality-inspired Test for Randomness (GTR), originally introduced at ICMC 2023. Our results show that GTR is more sensitive than NIST-STS to these injected dependencies since GTR detects the predictive structures even in cases where STS fails due to the absence of the secondary artifacts, demonstrating that GTR provides a supplementary approach to STS for randomness evaluation by performing direct detection of predictive structures rather than relying on secondary artifacts that may, or may not, be present in the candidate bitstream. In particular, GTR serves as a valuable follow-up diagnostic applied after STS to probe the temporal or predictive structure beyond the secondary effects that STS is designed to detect.