DATE: 2025/12/1

Department of Electrical and Electronic Information Engineering		ID	M223233
Name	Tenyu Kudo		

Supervisor	Shuichi Ichikawa

Abstract

Title	A Random Number Generation Method Using Generative Adversarial Networks and Linear Feedback Shift Registers

Random number generation is critically important, particularly in fields such as security, cryptography, and simulation. There are two main types of random numbers: True Random Numbers (TRN), which leverage physical phenomena and thus offer high unpredictability using specialized hardware, and Pseudo Random Numbers (PRN), which are generated by deterministic algorithms, enabling fast generation but becoming predictable if the algorithm and internal state is inferred.

In addition to these, a new type of random number called Unpredictable Random Number (URN), has been proposed. URN operates internally using a deterministic algorithm but incorporates an external entropy source to generate a practically unpredictable sequence of numbers. Chiba and Ichikawa (2023) generated an URN by introducing fluctuations in the LFSR sampling interval using wind direction data. However, since wind direction data is only available once per hour, this approach had limitations in generation speed.

This study examines an URN using temperature data as the entropy source to introduce fluctuations in the LFSR sampling interval. The target data was hourly temperature observation data for Kanazawa City published by the Japan Meteorological Agency, collected over the past three years. Since this data consists of date, time and temperature (in 0.1 deg Celsius), preprocessing and discretization were performed considering its characteristics. This data was then used as entropy to vary the LFSR's sampling interval.

In the DIEHARD test, when using a 32-bit LFSR, good results were obtained under the condition that the basic LFSR sampling interval was 32 or higher for both the method utilizing the fractional part of the temperature data (Method2) and the method utilizing the temperature difference (Method3). However, the more stringent NIST tests failed with the 32-bit LFSR. When using 48-bit and 64-bit LFSRs, the method applying mod4 operations to temperature differences (Method3-Pattern1-mod4) consistently passed the tests even when initial values or tap settings were altered.

Since temperature data are sampled at one hour intervals, constraints on entropy generation rate still exist. Therefore, this study investigated Generative Adversarial Networks (GAN) to generate data sequences with properties similar to meteorological data. GANs are models that generate high-quality data through competitive learning between a generator and a discriminator. We constructed and compared multiple models, including the RNN-CGAN (Recurrent Neural Networks Conditional GAN) model, which achieved the highest generation accuracy. We trained it on 12 years of past temperature data and utilized the generated 3 years of pseudo-meteorological data as sampling fluctuations for the LFSR.

The results showed that in the DIEHARD test, good results were obtained using Method2 and Method3, similar to the actual temperature data. The NIST test also showed a similar overall trend. Specifically, using Method2, stable passing was confirmed for both 48-bit and 64-bit LFSRs.