Acceleration of true orbit pseudorandom number generators using Newton's method

Asaki Saito
Future University Hakodate
saito@fun.ac.jp

Coauthor(s): Akihiro Yamaguchi

We developed pseudorandom number generators, termed true orbit generators, utilizing true orbits of the Bernoulli map on irrational algebraic integers [1,2]. These generators yield binary sequences that appear in the binary expansions of irrational algebraic integers, offering nonperiodic sequences, unlike existing generators. Supported by ergodic theory [3] and Borel's conjecture [4], these generators are expected to have high statistical quality, and extensive computer experiments have confirmed this [1,2]. However, their computational cost is significantly high, with a worst-case time complexity of $O(N^2)$ for generating a sequence of length N.

To address the issue of the high computational cost, we employ Newton's method, a technique for producing successively better approximations to the roots of a function, to accelerate the true orbit generators. This involves obtaining the exact binary expansion of a true root (i.e., an irrational algebraic integer) α from its approximation x, which includes an error. We establish a sufficient condition ensuring that the first N bits of the binary expansions of α and x match, thereby ensuring the generation of the same pseudorandom sequence as the true orbit generators. Furthermore, we demonstrate that the worst-case time complexity for generating a sequence of length N using the method proposed in this study is equivalent to that of multiplying two N-bit integers, showing its efficiency compared to the original generators with $O(N^2)$ time complexity.

[1] A. Saito and A. Yamaguchi, "Pseudorandom number generation using chaotic true orbits of the Bernoulli map," Chaos **26**, 063122 (2016).

[2] A. Saito and A. Yamaguchi, "Pseudorandom number generator based on the Bernoulli map on cubic algebraic integers," Chaos **28**, 103122 (2018).

[3] P. Billingsley, *Ergodic Theory and Information* (Wiley, New York, 1965).

[4] É. Borel, "Sur les chiffres décimaux de $\sqrt{2}$ et divers problèmes de probabilités en chaîne," C. R. Acad. Sci. Paris **230**, 591–593 (1950).