www.journal.asbsociety.com

ALUMNI SCIENTIAE BOHEMICAE
JASB
JOURNAL OF THE ASB SOCIETY

A Pseudorandom Sequence Generated over a Finite Field Using The Möbius Function

Zvoníček, Václav[1,2*]

1 *Gymnázium Brno, třída Kapitána Jaroše, příspěvková organizace*
2 *Charles University, Faculty of Mathematics and Physics, Ke Karlovu 2027/3, 12116 Praha 2*

About the author

Václav Zvoníček is currently in the second year of his Computer Science studies at the Faculty of Mathematics and Physics at the Charles University, Prague. Václav is also a former student of Gymnázium Brno, třídy Kapitána Jaroše in Brno, where he was a student of a mathematical class which encouraged him to focuse on mathematics and physics. During the high school studies, Václav was mainly interested in mathematics, physics and computer science. His interest thus results into the participation in several STEM-based competitions, such as Mathematics and Physics Olympiads or Students' Professional Activities (SPA). He achieved a nomination to European Physics Olympiad in Riga, Learned Society Award (for his first SPA contribution), and 2nd place in the national round of SPA in 2020 (Mathematics and Statistics). Apart from his academic interests, he also likes to play the piano and do as many sport activities as possible. In the future, he would like to take part in a research in Austria, Germany or Switzerland, mainly aiming at data processing problems or quantum computing.

Explanation for general audience

Randomness from a mathematical point of view is a tricky and challenging term to define, though each of us has a slight intuition of what it should be. In fact, it is still a question of whether there even exists a source of true randomness. Hence, we rather use the term pseudorandomness, which captures something difficult, but not impossible, to predict. For scientific purposes we are mostly interested in pseudorandom sequences of numbers since these can be used in computer science for randomized algorithms, which are often faster than normal ones, or, most importantly, in cryptography.

In this article, we focus on generating a pseudorandom sequence by using an algebraic structure, called finite field, and the Möbius function. The approach used for generating pseudorandom sequences was published quite recently, namely in 2016, and is therefore worth examining further. I decided to study the behaviour of the sequences by applying simple statistical tests: the frequency test and autocorrelation, which reflects the independence of the members of the sequence on one another.

After obtaining results from the aforementioned tests, two intriguing properties of the sequences were discovered. Namely, if we choose the finite fields of characteristic 3, the halves of the sequences are the same except for a sign, thus showing us a kind of strong dependence not acceptable in, for instance, cryptography. In addition, when fields of different characteristic are used, the produced sequences' members will not be completely uniformly distributed, which is usually an important requirement for the sequence to resemble random behaviour.