Analysis of pseudorandom sequences

Viktória Tóth

Department of Computer Algebra , ELTE

viktoria@inf.elte.hu

The notion of pseudorandomness is crucial in computational applications. This notion is used in the numerical analysis and also in pure mathematics. The most important ones are the cryptographycal applications, so I analyse certain families of sequences, presented by Mauduit and Sárközy, from this point of view.

I study collision and avalanche effect in families of finite pseudorandom binary and k-ary sequences. Both mentioned pseudorandom properties have practical importance.

Mauduit and Sárközy proved that the measures of pseudorandomness are small for some very important binary families, so I analyse these "good" constructions, whether they possess other strong pseudorandom properties as well. It turned out that some of them behave properly.

I extended the study of the pseudorandom properties mentioned above (collision and avalanche effect) to k-ary sequences, and found that the large family constructed is also collision free and it possesses the strict avalanche property.

References

[1] L. Goubin, C. Mauduit, A. Sárközy, *Construction of large families of pseudorandom binary sequences*, J. Number Theory 106 (2004), 56-69.

[2] C. Mauduit, J. Rivat, A. Sárközy, *Construction of pseudorandom binary sequences using additive characters*, Monatshefte Math. 141 (2004), 197-208.

[3] C. Mauduit, A. Sárközy, *On finite pseudorandom binary sequences I: The measures of pseudorandomness*, the Legendre symbol, Acta Arith. 82 (1997) 365-377.

[4] V. Tóth, *Collision and avalanche effect in families of pseudorandom binary sequences*, Periodica Math. Hungar. 55 (2007)2, 185-196.

[5] V. Tóth, *The study of collision and avalanche effect in a family of pseudorandom binary sequences*, Periodica Math. Hungar. 59 (2009)1, 1-8.

[6] V. Tóth, *Extension of the notion of collision and avalanche effect to sequences of k symbols*, Periodica Math. Hungar. 65. (2012) 2, 229–238.

[7] V. Tóth, *Collision and avalanche effect in pseudorandom sequences*, Annales Univ. Sci. Budapest., Sect. Comp. 41. (2013), 347–354.

[8] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Act. Sci. Ind. 1041, Hermann, Paris, 1948.