Pseudorandom sequences derived from automatic sequences

Arne Winterhof (Austrian Academy of Sciences)

Many automatic sequences, such as the Thue-Morse sequence or the Rudin-Shapiro sequence, have some desirable features of pseudorandomness such as a large linear complexity and a small well-distribution measure. However, they also have some undesirable properties in view of certain applications. For example, the majority of possible binary patterns never appears in automatic sequences and their correlation measure of order 2 is extremely large.

Certain subsequences, such as automatic sequences along squares, may keep the good properties of the original sequence but avoid the bad ones.

In this survey talk we investigate properties of pseudorandomness and non-randomness of automatic sequences and their subsequences and present results on their behaviour under several measures of pseudorandomness including linear complexity, correlation measure of order k, expansion complexity and normality.

(This is joint work with László Mérai.)

References

[1] L. Mérai, A. Winterhof, Pseudorandom sequences derived from automatic sequences, Cryptogr. Commun. 14 (4), 783–815.
`https://arxiv.org/abs/2105.03086`
`https://link.springer.com/article/10.1007/s12095-022-00556-9`