Über die Vorhersagbarkeit automatischer Folgen

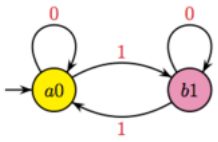
Arne Winterhof

Johann Radon Institut für angewandte und Computermathematik, Linz
Österreichische Akademie der Wissenschaften

Die *Thue-Morse Folge* $\mathcal{T} = (t_n)_{n=0}^{\infty} = (0110100110010110\ldots)$ ist definiert durch $t_0 = 0$ und

$$t_n = \begin{cases} t_{n/2}, & n \text{ gerade}, \\ 1 - t_{(n-1)/2}, & n \text{ ungerade}, \end{cases} \quad n = 1, 2, \ldots$$

und ist das wahrscheinlich berühmteste Beispiel einer *automatischen Folge*, d.h. einer Folge, die von einem endlichen Automaten erzeugt wird:



(Bei Eingabe der Bits von n wird t_n ausgegeben.)

Wir untersuchen verschiedene Vorhersagbarkeitsmaße für die Thue-Morse Folge und viele andere automatische Folgen: *lineare Komplexität, Expansionskomplexität und Autokorrelation.* Grob gesagt sind *nicht (schließlich) periodische* automatische Folgen vorhersagbar und daher kryptographisch schlecht.

Darüber hinaus studieren wir periodische Folgen über endlichen Körpern und vergleichen obige Vorhersagbarkeitsmaße. Z.B. zeigen wir, dass für p-periodische Folgen über $\mathbb{F}_p$ die Expansionskomplexität ein feineres Maß als die lineare Komplexität ist.

Für eine Primzahl $p > 2$ ist die p-periodische *Legendre-Folge* $\mathcal{L} = (\ell_n)_{n=0}^{\infty}$ definiert durch

$$\ell_n = \begin{cases} 1, & n \text{ quadratischer Rest modulo } p, \\ 0, & \text{sonst}, \end{cases} \quad n = 0, 1, \ldots$$

Sie besitzt große lineare Komplexität und kleine Autokorrelation sowie kleine Korrelation höherer Ordnung. Eine große Expansionskomplexität wäre eine weitere wünschenswerte Eigenschaft. Auch wenn viele Beispiele darauf hindeuten, ist ein Beweis dieser Eigenschaft anscheinend nicht in Reichweite. Stattdessen definieren wir ein weiteres Vorhersagbarkeitsmaß, das zwischen Expansionskomplexität und linearer Komplexität liegt und zeigen, dass dieses Maß für die Legendre-Folge groß ist.

References

[1] R. Hofer, A. Winterhof: Linear complexity and expansion complexity of some number theoretic sequences, erscheint in Workshop on Arithmetics in Finite Fields WAIFI 2016, Lecture Notes in Computer Sciences.

[2] L. Mérai, H. Niederreiter, A. Winterhof: Expansion complexity and linear complexity of sequences over finite fields, erscheint in Cryptography and Communications.