

Zufallszahlen

NIST-Tests

Monobit $\rightarrow \Sigma f(\text{bit}), \text{erfc}()$

Frequency in Block

Runs

Matrix Rank 32×32

1 0 1 | 1 0 1 | 0 1 1 | ...

\hookrightarrow 3×3

$$\begin{pmatrix} 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \rightarrow \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix} \left. \vphantom{\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 0 \end{pmatrix}} \right\} \text{Rang } 2$$

Fourier-Transformation

Template Matching

1 0 1 1 1 0 0 1 0 0 0 1 0 0 1 0 1 1

... overlapping

... non-overlapping

Entropie-Test Ueli Maurer

testet Komprimierung (ZIP) nach Ziv

Lineare Komplexität (LFSR)

wie groß muss ein Schieberegister sein,

um die Zufallsfolge zu produzieren, blockweise