1.10 Statistische Eigenschaften von linearen Schieberegistern

Die statistischen Eigenschaften von Schieberegisterfolgen der maximalen Periode $2^l - 1$, wobei l die Länge des Schieberegisters ist, wurden bereits von GOLOMB ausführlich untersucht.

Referenz:

> Solomon E. GOLOMB: **Shift Register Sequences.** Revised Edition, Aegean Park Press, Laguna Hills 1982. ISBN 0-89412-048-4

Hier einige Aussagen dazu:

Bemerkungen

1. In jeder vollen Periode kommen genau 2^{l-1} Einsen und $2^{l-1} - 1$ Nullen vor.

   Beweis. Es werden alle 2^l Zustandsvektoren $\in \mathbb{F}_2^l$ außer 0 jeweils genau einmal angenommen; das entspricht den ganzen Zahlen im Intervall $[1 \dots 2^l - 1]$. Davon sind 2^{l-1} ungerade, der Rest gerade, und ihre Paritäten bilden genau die Output-Folge des Schieberegisters.

2. Ein **Run** in einer Folge ist ein maximales konstantes Stück.

   Beispiel: $\dots 0111110 \dots$ ist ein Einser-Run der Länge 5.

   Bedenkt man, dass die Stücke der Länge l der Schieberegister-Folge genau die verschiedenen Zustandsvektoren $\neq 0$ sind, so ist klar, dass in der vollen Periode folgendes vorkommt:

   - Kein Run der Länge $> l$.
   - Genau ein Einser-Run und kein Nuller-Run der Länge l – denn sonst käme der Nuller-Zustand vor bzw. der Einser-Zustand öfter als einmal vor.
   - Jeweils genau ein Einser- und Nuller-Run der Länge $l - 1$.
   - Allgemein jeweils genau 2^{k-1} Einser- und Nuller-Runs der Länge $l - k$ für $1 \leq k \leq l - 1$.
   - Insbesondere genau 2^{l-1} Runs der Länge 1, davon jeweils genau die Hälfte Nullen und Einsen.

3. Für eine periodische Folge $x = (x_n)_{n \in \mathbb{N}}$ in $\mathbb{F}_2$ der Periode s ist die **Autokorrelation** zur Verschiebung um t definiert durch

$$\begin{aligned} \kappa_x(t) &= \frac{1}{s} \cdot [\#\{n \mid x_{n+t} = x_n\} - \#\{n \mid x_{n+t} \neq x_n\}] \\ &= \frac{1}{s} \cdot \sum_{n=0}^{s-1} (-1)^{x_{n+t} + x_n} \end{aligned}$$

(analog wie in Kapitel II für BOOLEsche Funktionen). Wird nun x von einem Schieberegister der Länge l erzeugt,

$$x_n = a_1 x_{n-1} + \cdots + a_l x_{n-l} \quad \text{für } n \geq l,$$

so kann man die Differenzenfolge $y_n = x_{n+t} - x_n$ bilden. Diese wird offensichtlich von dem gleichen Schieberegister erzeugt. Sind die Startwerte $y_0, \ldots, y_{l-1}$ sämtlich 0, so ist der Zustandsvektor $x_{(t)} = x_{(0)}$, also t ein Vielfaches der Periode und $\kappa_x(t) = 1$. Andernfalls – und falls x die maximal mögliche Periode $s = 2^l - 1$ hat – durchläuft y in einer Periode nach Bemerkung 1 genau 2^{l-1} Einsen und $2^{l-1} - 1$ Nullen. Daher ist

$$\kappa_x(t) = \begin{cases} 1, & \text{wenn } s|t, \\ -\frac{1}{s}, & \text{sonst.} \end{cases}$$

Die Autokorrelation ist also – außer bei Verschiebungen um Vielfache der Periode – *gleichmäßig klein.*

Diese Aussagen bedeuten, dass die Folge sehr gleichmäßig verteilt ist, und wurden von GOLOMB als die drei Zufälligkeits-Postulate bezeichnet. Wegen dieser Eigenschaften werden solche Folgen, also insbesondere Schieberegisterfolgen maximaler Periode, in der Elektrotechnik auch als „Rauschen“ bezeichnet (PN-sequences = Pseudo Noise Sequences).

Hier eine Implementation von Schieberegistern in der leicht verständlichen Sprache von Mathematica – für eine Anwendung mit hohem Effizienzbedarf würde man natürlich eine Implementation in C vorziehen.

```
linShRep[n_Integer] :=
  Module[{y, outlist = {}},
    For[i = 0, i < n, i++,
      outlist = Append[outlist, Last[x]];
      y = Mod[a.x, 2];
      x = RotateRight[x];
      x[[1]] = y
      ];
    Return[outlist]
    ]
linShRep::usage =
"Generate a linear feedback shift register sequence.\n
1. Set up the coefficient array a consisting of 0s and 1s.\n
2. Set up the initial state of the shift register as an array
   x of the same length consisting of 0s and 1s.\n
3. Call linShRep with the desired number n of output Bits."
```

Ein exemplarischer Aufruf dieser Funktion mit einem Schieberegister der Länge 16, aus dem 1024 Bits erzeugt werden sollen, sieht so aus:

```
a = {0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1}
x = {0, 1, 1, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 1, 1}
z = linShRep[1024]
```

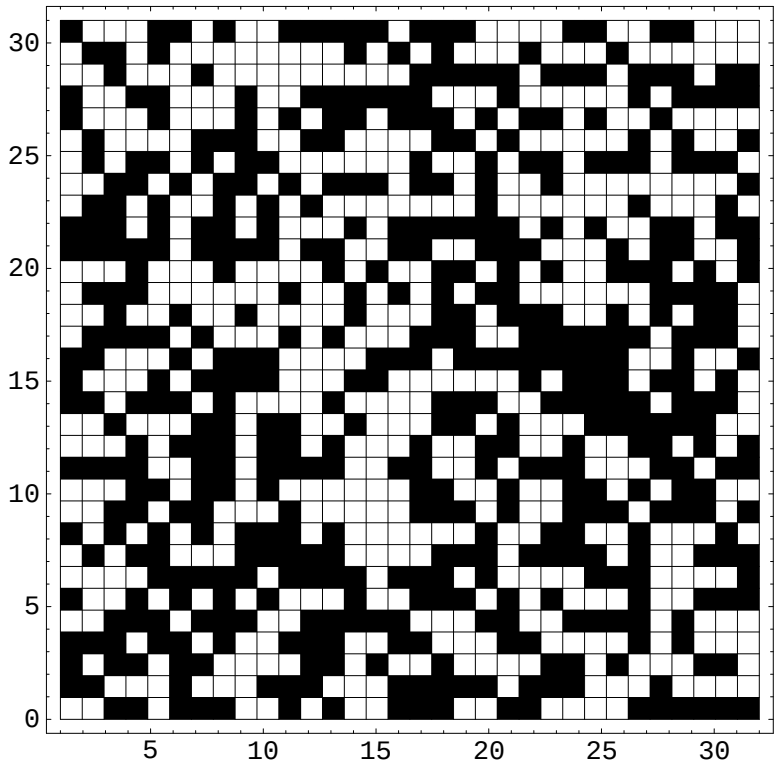
und ergibt den Output (ohne Klammern und Kommata wiedergegeben):

```
11001000110101100011001111000000
00111011100011100000100011101111
01001001111001011011110010111001
00010010110001100111001111010111
11000100011000001110011000010111
01101010101110110001010111011000
11110000010000100010111100011110
10100111000001111000100001011000
01010101000101111110110011011101
11001001110111110001011000100010
11100100101111110011011001010011
00001100100001100110100011100100
11101000100101110110011011001010
11011100100110111001011100000011
00100010111101111000110000010001
01110100001110011111101000100101
00111010001111000100000000110110
10000101110101110001100000010001
11011011011110111001000110101001
10001111110110101010011111100001
11101110111101011001010110001010
00000100001001100110001110100110
00010100101110100000010101100100
10010110101011111110111111011101
11001010010100010010110111111110
10100101001111110110100100010001
10111100011001111001011111010110
01110111010100100010100101101111
01100111011000000111011111010000
11011101111111110000010001000100
10010111111110101011101110111111
01110010110000010001111001100111
```

Eine Visualiserung, die mit dem Mathematica-Kommando

```
DensityPlot[z[[32*i + j]], {j, 1, 32}, {i, 0, 31},
   PlotPoints -> 32]
```

erzeugt wurde, zeigt, dass zumindest der äußere Eindruck der einer ziemlich zufälligen Bitfolge ist:



Das im Beispiel verwendete Schieberegister erzeugt übrigens eine Folge der maximalen Periode $2^{16} - 1 = 65535$, da sein charakteristisches Polynom

$$T^{16} + T^{14} + T^{13} + T^{11} + 1 \in \mathbb{F}_2$$

primitiv ist.