3.3 Der Berlekamp-Massey-Algorithmus

Der Beweis von Satz 1 ist konstruktiv: Er enthält einen Algorithmus, mit dem sukzessive ein linearer Rekurrenzgenerator aufgebaut wird. Beim Schritt von der Folgenlänge n zur Folgenlänge $n+1$ gibt es drei mögliche Fälle (1, 2a, 2b):

1. Fall $d_n = 0$, d. h. der Generator zum Rückkopplungspolynom φ erzeugt auch u_n: Dann bleiben φ und l ungeändert und ebenso ψ, t, r, d_r.

2. Fall $d_n \neq 0$, d. h. der Generator zum Rückkopplungspolynom φ erzeugt u_n nicht: Dann wird ein neues Rückkopplungspolynom η gebildet, dessen zugehöriger Generator $(u_0, \ldots, u_n)$ erzeugt. Es wird weiter unterschieden:

a) $l > \frac{n}{2}$: Dann ist $\lambda_{n+1} = \lambda_n$; es wird φ durch η ersetzt, l bleibt, und ebenso bleiben ψ, t, r, d_r.

b) $l \leq \frac{n}{2}$: Dann ist $\lambda_{n+1} = n + 1 - \lambda_n$; es wird φ durch η und l durch $n + 1 - l$ ersetzt, ferner ψ durch φ, t durch l, r durch n und d_r durch d_n.

Damit ist der Berlekamp-Massey-Algorithmus semiformal beschreibbar:

Input: Eine Folge $u = (u_0, \ldots, u_{N-1}) \in K^N$.

Output: Die lineare Komplexität $\lambda_N(u)$,

das Rückkopplungspolynom φ eines linearen Rekurrenzgenerators der Länge $\lambda_N(u)$, der u erzeugt.

Hilfsvariablen: n: aktueller Index, initialisiert mit $n := 0$,

l: aktuelle lineare Komplexität, initialisiert mit $l := 0$,

φ: aktuelles Rückkopplungspolynom $= 1 - a_1 T - \cdots - a_l T^l$, initialisiert mit $\varphi := 1$,

Invarianzbedingung: $u_i = a_1 u_{i-1} + \cdots + a_l u_{i-l}$ für $l \leq i < n$,

d: aktuelle Diskrepanz $= u_n - a_1 u_{n-1} - \cdots - a_l u_{n-l}$,

r: voriger Index, initialisiert mit $r := -1$,

t: vorige lineare Komplexität,

ψ: voriges Rückkopplungspolynom $= 1 - b_1 T - \cdots - b_t T^t$, initialisiert mit $\psi := 1$,

Invarianzbedingung: $u_i = b_1 u_{i-1} + \cdots + b_t u_{i-t}$ für $t \leq i < r$,

d': vorige Diskrepanz $= u_r - b_1 u_{r-1} - \cdots - b_t u_{r-t}$, initialisiert mit $d' := 1$,

η: neues Rückkopplungspolynom,

m: neue lineare Komplexität.

Iterationsschritte: Für $n = 0, \ldots, N-1$:

$d := u_n - a_1 u_{n-1} - \cdots - a_l u_{n-l}$
Falls $d \neq 0$
  $\eta := \varphi - \frac{d}{d'} \cdot T^{n-r} \cdot \psi$
  Falls $l \leq \frac{n}{2}$ [lineare Komplexität wächst]
    $m := n + 1 - l$
    $t := l$
    $l := m$
    $\psi := \varphi$
    $r := n$
    $d' := d$
  $\varphi := \eta$

Natürlich kann man sich auch gleich die ganze Folge (λ_n) ausgeben lassen.

Dieser Algorithmus wird jetzt auf das **Beispiel** der Folge 001101110 angewendet. Der Fall $d \neq 0$, $l \leq \frac{n}{2}$ wird durch „[!]“ bezeichnet.

Eingangsbedingungen				Aktionen
$n = 0$	$u_0 = 0$	$l = 0$	$\varphi = 1$	$d := u_0 = 0$
$r = -1$	$d' = 1$	$t =$	$\psi = 1$	
$n = 1$	$u_1 = 0$	$l = 0$	$\varphi = 1$	$d := u_1 = 0$
$r = -1$	$d' = 1$	$t =$	$\psi = 1$	
$n = 2$	$u_2 = 1$	$l = 0$	$\varphi = 1$	$d := u_2 = 1$ [!]
$r = -1$	$d' = 1$	$t =$	$\psi = 1$	$\eta := 1 - T^3$
				$m := 3$
$n = 3$	$u_3 = 1$	$l = 3$	$\varphi = 1 - T^3$	$d := u_3 - u_0 = 1$
$r = 2$	$d' = 1$	$t = 0$	$\psi = 1$	$\eta := 1 - T - T^3$
$n = 4$	$u_4 = 0$	$l = 3$	$\varphi = 1 - T - T^3$	$d := u_4 - u_3 - u_1 = -1$
$r = 2$	$d' = 1$	$t = 0$	$\psi = 1$	$\eta := 1 - T + T^2 - T^3$
$n = 5$	$u_5 = 1$	$l = 3$	$\varphi = 1 - T + T^2 - T^3$	$d := u_5 - u_4 + u_3 - u_2 = 1$
$r = 2$	$d' = 1$	$t = 0$	$\psi = 1$	$\eta := 1 - T + T^2 - 2T^3$

Von jetzt an unterscheiden sich die Ergebnisse je nach Charakteristik des Grundkörpers K. Sei zuerst $\operatorname{char} K \neq 2$. Dann geht es so weiter:

Eingangsbedingungen	Aktionen
$n = 6 \quad u_6 = 1 \quad l = 3$ $\varphi = 1 - T + T^2 - 2T^3$ $r = 2 \quad d' = 1 \quad t = 0 \quad \psi = 1$	$d := u_6 - u_5 + u_4 - 2u_3 = -2$ [!] $\eta = 1 - T + T^2 - 2T^3 + 2T^4$ $m := 4$
$n = 7 \quad u_7 = 1 \quad l = 4$ $\varphi = 1 - T + T^2 - 2T^3 + 2T^4$ $r = 6 \quad d' = -2 \quad t = 3$ $\psi = 1 - T + T^2 - 2T^3$	$d := u_7 - u_6 + u_5 - 2u_4 + 2u_3 = 3$ $\eta = 1 + \frac{1}{2}T - \frac{1}{2}T^2 - \frac{1}{2}T^3 - T^4$
$n = 8 \quad u_8 = 0 \quad l = 4$ $\varphi = 1 + \frac{1}{2}T - \frac{1}{2}T^2 - \frac{1}{2}T^3 - T^4$ $r = 6 \quad d' = -2 \quad t = 3$ $\psi = 1 - T + T^2 - 2T^3$	$d := u_8 + \frac{1}{2}u_7 - \frac{1}{2}u_6 - \frac{1}{2}u_5 - u_4 = -\frac{1}{2}$ [!] $\eta := 1 + \frac{1}{2}T - \frac{3}{4}T^2 - \frac{1}{4}T^3 - \frac{5}{4}T^4 + \frac{1}{2}T^5$ $m := 5$

Als Ergebnis erhalten wir die Folge der linearen Komplexitäten

$$\lambda_0 = 0, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 3, \lambda_4 = 3, \lambda_5 = 3, \lambda_6 = 3, \lambda_7 = 4, \lambda_8 = 4, \lambda_9 = 5$$

und die Rekursionsvorschrift

$$u_i = -\frac{1}{2}u_{i-1} + \frac{3}{4}u_{i-2} + \frac{1}{4}u_{i-3} + \frac{5}{4}u_{i-4} - \frac{1}{2}u_{i-5} \quad \text{für } i = 5, \ldots, 8.$$

Im Falle $\operatorname{char} K = 2$ sehen die letzten drei Iterationen so aus:

Eingangsbedingungen	Aktionen
$n = 6 \quad u_6 = 1 \quad l = 3$ $\varphi = 1 - T - T^2$ $r = 2 \quad d' = 1 \quad t = 0 \quad \psi = 1$	$d := u_6 - u_5 - u_4 = 0$
$n = 7 \quad u_7 = 1 \quad l = 3$ $\varphi = 1 - T - T^2$ $r = 2 \quad d' = 1 \quad t = 0 \quad \psi = 1$	$d := u_7 - u_6 - u_5 = 1$ [!] $\eta = 1 - T - T^2 - T^5$ $m := 5$
$n = 8 \quad u_8 = 0 \quad l = 5$ $\varphi = 1 - T - T^2 - T^5$ $r = 7 \quad d' = 1 \quad t = 3 \quad \psi = 1 - T - T^2$	$d := u_8 - u_7 - u_6 - u_3 = 1$ $\eta := 1 - T^3 - T^5$

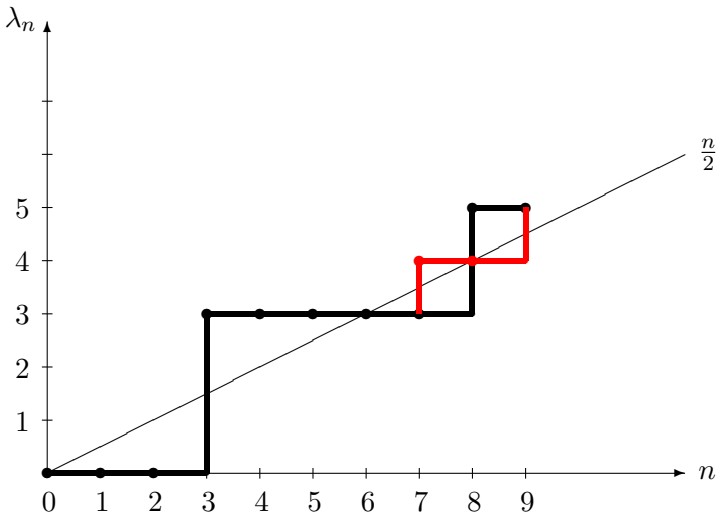
Die Folge der linearen Komplexitäten ist hier

$$\lambda_0 = 0, \lambda_1 = 0, \lambda_2 = 0, \lambda_3 = 3, \lambda_4 = 3, \lambda_5 = 3, \lambda_6 = 3, \lambda_7 = 3, \lambda_8 = 5, \lambda_9 = 5$$

und die Rekursionsvorschrift

$$u_i = u_{i-3} + u_{i-5} \quad \text{für } i = 5, \ldots, 8.$$

Die Entwicklung der linearen Komplexität wird auch noch grafisch dargestellt; die rote Linie kennzeichnet den Fall $\operatorname{char} K \neq 2$:



Der Aufwand für den Berlekamp-Massey-Algorithmus ist $O(N^2 \log N)$.

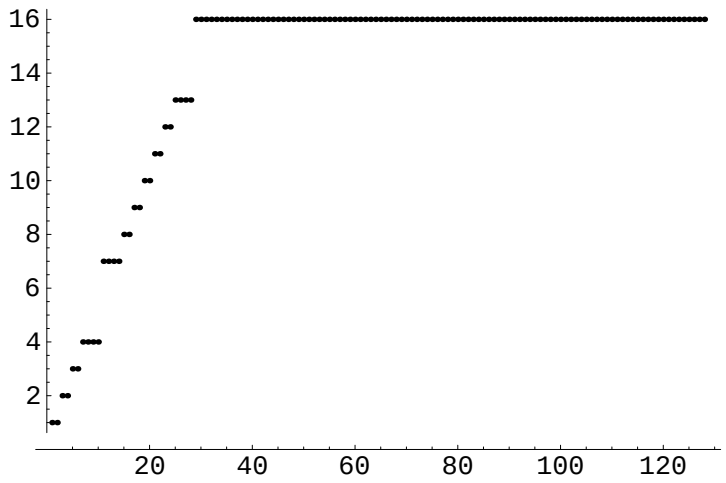
Die Folge $(\lambda_n)_{n\in\mathbb{N}}$ bzw. (für endliche Bitfolgen) $(\lambda_n)_{0\le n\le N}$ heißt das **Linearitätsprofil** der Bitfolge u.

Für die ersten 128 Bits der Folge, die in 1.10 von einem linearen Schieberegister erzeugt wurde, ist das Linearitätsprofil:

$$(0, 1, 1, 2, 2, 3, 3, 4, 4, 4, 4, 7, 7, 7, 7, 8, 8, 9, 9, 10, 10, 11, 11, 12,$$

$$12, 13, 13, 13, 13, 16, 16, 16, 16, \ldots),$$

und graphisch dargestellt sieht das so aus:

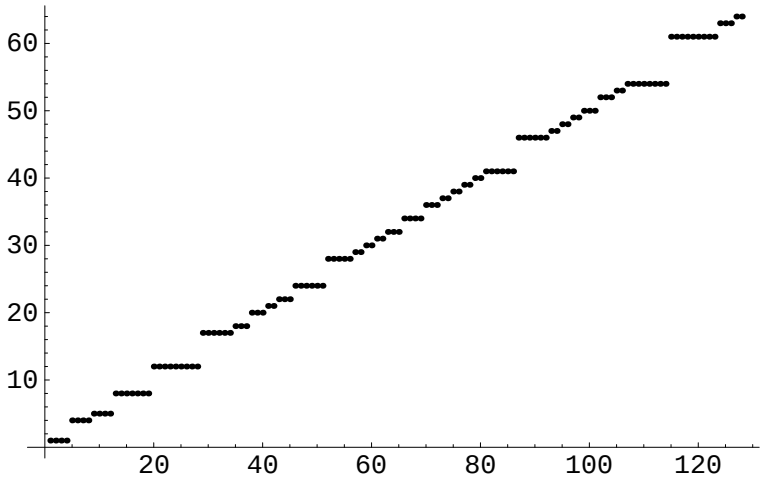


Für die ersten 128 Bits der Folge, die in 4.1 von einem „perfekten“ Zufallsgenerator erzeugt werden wird, ist das Linearitätsprofil:

$$(0, 1, 1, 1, 1, 4, 4, 4, 4, 5, 5, 5, 5, 8, 8, 8, 8, 8, 8, 8, 8, 12, 12, 12, 12,$$

$$12, 12, 12, 12, 12, 17, 17, 17, 17, 17, 17, 18, 18, 18, 20, 20, 20, 21, 21,$$
$$22, 22, 22, 24, 24, 24, 24, 24, 24, 28, 28, 28, 28, 28, 29, 29, 30, 30, 31,$$
$$31, 32, 32, 32, 34, 34, 34, 34, 36, 36, 36, 37, 37, 38, 38, 39, 39, 40, 40,$$
$$41, 41, 41, 41, 41, 41, 46, 46, 46, 46, 46, 46, 47, 47, 48, 48, 49, 49, 50,$$
$$50, 50, 52, 52, 52, 53, 53, 54, 54, 54, 54, 54, 54, 54, 54, 61, 61, 61, 61,$$
$$61, 61, 61, 61, 61, 63, 63, 63, 64, 64),$$

und das graphisch dargestellt sieht so aus:



Man sieht im zweiten Fall die unregelmäßige Schwankung um die Diagonale, wie es sich für eine „gute“ Zufallsfolge gehört. Im ersten Fall ist dieser Effekt auch vorhanden, aber nur, bis die lineare Komplexität der Folge erreicht ist.