3.2 Synthese linearer Schieberegister

In diesem Abschnitt geht es darum, zu einer gegebenen endlichen Bitfolge ein lineares Schieberegister kürzester Länge zu finden. Der Ansatz aus Abschnitt 2 zur Vorhersage von Zufallsgeneratoren lieferte ein lineares Schieberegister unter der Annahme, dass man schon ein evtl. nichtlineares hat, lässt aber kaum erkennen, ob es vielleicht ein kürzeres gäbe. Mit einem etwas anderen Ansatz ist die gestellte Aufgabe aber überraschend einfach zu lösen: mit einem Algorithmus von Massey (1969), der in einem anderen Kontext vorher schon von Berlekamp (1968) angegeben worden war.

Da keine speziellen Eigenschaften des Körpers $\mathbb{F}_2$ benützt werden, wird hier ein beliebiger Körper K zu Grunde gelegt. Gesucht wird ein homogener Kongruenzgenerator möglichst geringer Rekursionstiefe l, der eine gegebene endliche Folge $u \in K^N$ erzeugt.

Für einen solchen Kongruenzgenerator mit Bildungsgestz

$$u_k = a_1 u_{k-1} + \cdots + a_l u_{k-l} \quad \text{für } k = l, \ldots, N-1$$

ist $(a_1, \ldots, a_l) \in K^l$ der Koeffizientenvektor; das Polynom

$$\varphi = 1 - a_1 T - \cdots - a_l T^l \in K[T]$$

heißt **Rückkopplungspolynom**. Es ist das reziproke Polynom zum charakteristischen Polynom der Begleitmatrix A: Ist dieses $\chi = \mathrm{Det}(T \cdot 1 - A)$, so ist

$$\chi = T^l - a_1 T^{l-1} - \cdots - a_l, \quad \text{also} \quad \varphi = T^l \cdot \chi(\frac{1}{T}).$$

Hilfssatz 2 *Der homogene lineare Kongruenzgenerator mit Koeffizienten $(a_1, \ldots, a_l)$ erzeuge die Folge $u = (u_0, \ldots, u_{n-1}) \in K^n$, aber nicht die Folge $\hat{u} = (u_0, \ldots, u_n) \in K^{n+1}$. Dann hat jeder homogene lineare Kongruenzgenerator, der $\hat{u}$ erzeugt, eine Länge $m \geq n + 1 - l$.*

Beweis. **Fall 1:** $l \geq n$. Dann ist $l + m \geq n + 1$, außer wenn $l = n$, $m = 0$. In diesem Fall müsste aber wegen $m = 0$ notwendig $u_0 = \ldots = u_n$ sein, und der Generator würde auch $\hat{u}$ erzeugen, Widerspruch.

Fall 2: $l \leq n - 1$. *Annahme*: $m \leq n - l$. Es ist

$$u_j = a_1 u_{j-1} + \cdots + a_l u_{j-l} \quad \text{für } l \leq j \leq n-1.$$

Sei $(b_1, \ldots, b_m)$ der Koeffizientenvektor eines homogenen linearen Kongruenzgenerators, der $\hat{u}$ erzeugt; dann ist

$$u_j = b_1 u_{j-1} + \cdots + b_m u_{j-m} \quad \text{für } m \leq j \leq n.$$

Insgesamt folgt

$$\begin{aligned} u_n &\neq a_1 u_{n-1} + \cdots + a_l u_{n-l} \\ &= \sum_{i=1}^{l} a_i \cdot \underbrace{\sum_{k=1}^{m} b_k u_{n-i-k}}_{u_{n-i}} \quad [\text{da } n-l \geq m] \\ &= \sum_{k=1}^{m} b_k \cdot \underbrace{\sum_{i=1}^{l} a_i u_{n-k-i}}_{u_{n-k}} = u_n, \end{aligned}$$

Widerspruch. $\diamond$

Sei nun $u \in K^N$ eine Folge. Für $0 \leq n \leq N$ sei $\lambda_n(u) = \lambda_n$ die kleinste Rekursionstiefe eines Generators, der $(u_0, \ldots, u_{n-1})$ erzeugt.

Hilfssatz 3 *Für jede Folge $u \in K^N$ gilt:*

(i) $\lambda_{n+1} \geq \lambda_n$.
(ii) *Genau dann, wenn es einen Generator der Rekursionstiefe λ_n gibt, der $(u_0, \ldots, u_n)$ erzeugt, gilt $\lambda_{n+1} = \lambda_n$.*
(iii) *Gibt es einen solchen nicht, ist*

$$\lambda_{n+1} \geq n + 1 - \lambda_n.$$

Beweis. (i) Jeder Generator, der $(u_0, \ldots, u_n)$ erzeugt, erzeugt erst recht $(u_0, \ldots, u_{n-1})$.

(ii) folgt aus (i).

(iii) Die Voraussetzung von Hilfssatz 2 gilt für jeden Generator von $(u_0, \ldots, u_{n-1})$. $\diamond$

Satz 1 [Massey] *Sei $u \in K^N$ und $0 \leq n \leq N-1$. Sei ferner $\lambda_{n+1}(u) \neq \lambda_n(u)$. Dann ist*

$$\lambda_n(u) \leq \frac{n}{2} \quad \textit{und} \quad \lambda_{n+1}(u) = n + 1 - \lambda_n(u).$$

Beweis. Der Fall $\lambda_n = 0$ ist besonders leicht: Es ist $u_0 = \ldots = u_{n-1} = 0$. Falls $u_n = 0$, ist $\lambda_{n+1} = \lambda_n = 0$, also nichts zu beweisen. Falls $u_n \neq 0$, ist $\lambda_{n+1} = n + 1 = n + 1 - \lambda_n$ nach Bemerkung 5 in 3.1.

Allgemein folgt die erste Aussage aus der zweiten, denn wegen $\lambda_n < \lambda_{n+1}$ ist $2\lambda_n < n + 1$.

Die zweite Aussage wird nun durch Induktion über n bewiesen. Im Fall $n = 0$ ist $\lambda_0 = 0$ – dieser Fall ist schon erledigt.

Sei jetzt $n \geq 1$. Sei o. B. d. A. $l := \lambda_n \geq 1$. Sei

$$u_j = a_1 u_{j-1} + \cdots + a_l u_{j-l} \quad \text{für } j = l, \ldots, n-1;$$

das zugehörige Rückkopplungspolynom ist also

$$\varphi := 1 - a_1 T - \cdots - a_l T^l \in K[T].$$

Die „n-te Diskrepanz“ sei

$$d_n := u_n - a_1 u_{n-1} - \cdots - a_l u_{n-l}.$$

Ist $d_n = 0$, so erzeugt der Generator auch u_n, und es ist nichts zu beweisen. Sei also $d_n \neq 0$. Sei r die Länge der Folge vor der letzten Zunahme der linearen Komplexität, also

$$t := \lambda_r < l, \quad \lambda_{r+1} = l.$$

Wegen der Induktionsannahme ist $l = r + 1 - t$. Ist

$$u_j = b_1 u_{j-1} + \cdots + b_t u_{j-t} \quad \text{für } j = t, \ldots, r-1,$$

so ist das zugehörige Rückkopplungspolynom

$$\psi := 1 - b_1 T - \cdots - b_t T^t \in K[T],$$

und für die analog gebildete r-te Diskrepanz gilt

$$d_r := u_r - b_1 u_{r-1} - \cdots - b_t u_{r-t} \neq 0,$$

Ist $t = 0$, so $\psi = 1$ und $d_r = u_r$. Nun wird das Polynom

$$\eta := \varphi - \frac{d_n}{d_r} \cdot T^{n-r} \cdot \psi = 1 - c_1 T - \cdots - c_m T^m \in K[T]$$

gebildet mit $m = \operatorname{Grad} \eta$. Was macht der zugehörige homogene lineare Kongruenzgenerator? Es ist

$$\begin{aligned} u_j - \sum_{i=1}^{m} c_i u_{j-i} &= u_j - \sum_{i=1}^{l} a_i u_{j-i} - \frac{d_n}{d_r} \cdot \left[u_{j-n+r} - \sum_{i=1}^{t} b_i u_{j-n+r-i} \right] \\ &= 0 \quad \text{für } j = m, \ldots, n; \end{aligned}$$

für $j = 0, \ldots, n-1$ folgt das direkt, für $j = n$ kommt zunächst $d_n - [d_n/d_r] \cdot d_r$ heraus. Er erzeugt also $(u_0, \ldots, u_n)$. Nun ist

$$\lambda_{n+1} \leq m \leq \max\{l, n - r + t\} = \max\{l, n + 1 - l\}.$$

Wegen der Monotonie der linearen Komplexität ist $m > l$, nach Hilfssatz 2 ist $m \geq n + 1 - l$. Also folgt $m = n + 1 - l$ und $\lambda_{n+1} = m$. Damit ist die Behauptung bewiesen. $\diamond$

Korollar 1 *Ist $d_n \neq 0$ und $\lambda_n \leq \frac{n}{2}$, so ist*

$$\lambda_{n+1} = n + 1 - \lambda_n > \lambda_n.$$

Beweis. Nach Hilfssatz 2 ist $\lambda_{n+1} \geq n + 1 - \lambda_n$, also $\lambda_{n+1} \geq \frac{n}{2} + 1 > \lambda_n$. Nach Satz 1 folgt daraus $\lambda_{n+1} = n + 1 - \lambda_n$. $\diamond$

Bei dem sukzessiven Aufbau eines linearen Rekurrenzgenerators im Beweis des Satzes tritt also in jedem Iterationsschritt einer der folgenden Fälle ein:

- $d_n = 0$: Dann ist $\lambda_{n+1} = \lambda_n$.
- $d_n \neq 0$: Dann ist
  - $\lambda_{n+1} = \lambda_n$, falls $\lambda_n > \frac{n}{2}$,
  - $\lambda_{n+1} = n + 1 - \lambda_n$, falls $\lambda_n \leq \frac{n}{2}$.

  Insbesondere gilt stets:

- Ist $\lambda_n > \frac{n}{2}$, so $\lambda_{n+1} = \lambda_n$.
- Ist $\lambda_n \leq \frac{n}{2}$, so $\lambda_{n+1} = \lambda_n$ oder $\lambda_{n+1} = n + 1 - \lambda_n$.

Nebenbei haben wir eine alternative Möglichkeit gefunden, lineare Schieberegister vorherzusagen:

Korollar 2 *Wird $u \in \mathbb{F}_2^n$ von einem linearen Schieberegister der Länge $\leq l$ erzeugt, so lässt sich ein solches aus $u_0, \ldots, u_{2l-1}$ bestimmen.*

Beweis. Wäre erstmals $d_n \neq 0$ für $n \geq 2l$, so $\lambda_n \leq l \leq \frac{n}{2}$, also $\lambda_{n+1} = n + 1 - \lambda_n \geq l + 1$, Widerspruch. $\diamond$