1.7 Allgemeine lineare Generatoren

Die gemeinsame Verallgemeinerung von linearen Kongruenzgeneratoren und linearen Schieberegister-Generatoren sind die **mehrstufigen linearen Rekurrenzgeneratoren**. Sie lassen sich bequem im Rahmen eines endlichen Rings R (kommutativ mit 1) behandeln; damit sind nicht nur die Ringe $\mathbb{Z}/m\mathbb{Z}$ erfaßt, sondern auch die endlichen Körper zusätzlich zu den Primkörpern $\mathbb{F}_p$, die ebenfalls zur Zufallserzeugung benützt werden können. Bei einem r-stufigen linearen Rekurrenzgenerator wird eine Folge (x_n) in R nach der Vorschrift

$$x_n = a_1 x_{n-1} + \cdots + a_r x_{n-r} + b$$

erzeugt. Als Parameter braucht man

- die **Rekursionstiefe** r (o. B. d. A. $a_r \neq 0$),
- die **Koeffizientenfolge** $a = (a_1, \ldots, a_r) \in R^r$,
- das **Inkrement** $b \in R$,
- einen **Startvektor** $(x_0, \ldots, x_{r-1}) \in R^r$.

Der lineare Rekurrenzgenerator heißt **homogen** oder **inhomogen**, je nachdem, ob $b = 0$ ist oder nicht.

Die Funktionsweise eines linearen Rekurrenzgenerators kann man ähnlich einem Schieberegister veranschaulichen, siehe Abbildung 3.

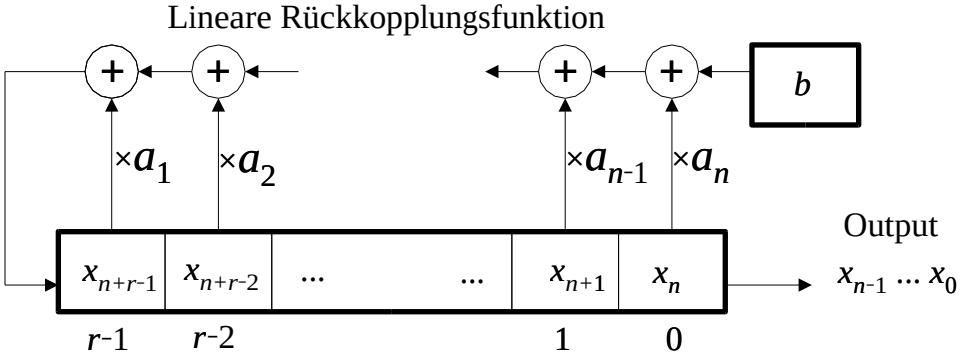

Abbildung 3: Ein linearer Rekurrenzgenerator

Inhomogene lineare Rekurrenzgeneratoren kann man leicht auf homogene reduzieren, wobei man allerdings eine Rekursionsstufe zusätzlich in Kauf nehmen muss: Aus den beiden Gleichungen

$$\begin{aligned} x_{n+1} &= a_1 x_n + \cdots + a_r x_{n-r+1} + b, \\ x_n &= a_1 x_{n-1} + \cdots + a_r x_{n-r} + b, \end{aligned}$$

folgt nämlich durch Subtraktion

$$x_{n+1} = (a_1 + 1)x_n + (a_2 - a_1)x_{n-1} \cdots + (-a_r)x_{n-r}.$$

Im Falle $r = 1$, $x_n = ax_{n-1} + b$, wird diese Formel zu

$$x_n = (a + 1)x_{n-1} - ax_{n-2}.$$

Daher wird der inhomogene Fall im folgenden vernachlässigt.

Im homogenen Fall kann man unter Verwendung der **Zustandsvektoren** $x_{(n)} = (x_n, \ldots, x_{n+r-1})$ schreiben

$$x_{(n)} = Ax_{(n-1)} \quad \text{für } n \geq 1$$

mit der **Begleitmatrix**

$$A = \begin{pmatrix} 0 & 1 & \ldots & 0 \\ & \ddots & \ddots & \\ & & & 1 \\ a_r & a_{r-1} & \ldots & a_1 \end{pmatrix}.$$

Die nächste Stufe der Verallgemeinerung ist also ein **Matrixgenerator**. Parameter sind:

- eine $r \times r$-Matrix $A \in M_r(R)$,
- ein Startvektor $x_0 \in R^r$.

Die Folge wird gebildet nach der Formel

$$x_n = Ax_{n-1} \in R^r.$$

Noch allgemeiner (und begrifflich einfacher) ist die abstrakt-algebraische Version, der **allgemeine lineare Generator**. Gegeben sind:

- ein Ring R (kommutativ und mit Einselement),
- ein R-Modul M,
- eine R-lineare Abbildung $A : M \longrightarrow M$,
- ein Startwert $x_0 \in M$.

Daraus wird eine Folge $(x_n)_{n\in\mathbb{N}}$ gebildet nach der Formel

$$x_n = Ax_{n-1} \quad \text{für } n \geq 1.$$

Beispiele.

1. Für einen homogenen linearen Kongruenzgenerator ist
$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R \quad (r = 1), \quad A = (a).$$
2. Für einen inhomogenen linearen Kongruenzgenerator ist
$$R = \mathbb{Z}/m\mathbb{Z}, \quad M = R^2 \quad (r = 2), \quad A = \begin{pmatrix} 0 & 1 \\ -a & a+1 \end{pmatrix}.$$
3. Für einen lineares Schieberegister ist
$$R = \mathbb{F}_2, \quad M = \mathbb{F}_2^l \quad (r = l), \quad A = \text{die Begleitmatrix},$$
die nur aus Nullen und Einsen besteht.

Falls M endlich ist, kann die Rekursion nur endlich viele verschiedene Werte annehmen, muss also nach einer eventuellen Vorperiode periodisch werden.

Satz 2 *Sei M ein endlicher R-Modul und $A : M \longrightarrow M$ linear. Genau dann, wenn A bijektiv ist, sind alle vom zugehörigen allgemeinen linearen Generator erzeugten Folgen rein-periodisch.*

Beweis. Sei A bijektiv und x_0 ein Startvektor. Sei t der kleinste Index, so dass x_t einen bereits vorher durchlaufenen Wert annimmt, und sei s der kleinste Index mit $x_t = x_s$. Wäre $s \geq 1$, so $x_s = Ax_{s-1}$ und $x_t = Ax_{t-1}$, also
$$x_{t-1} = A^{-1}x_t = A^{-1}x_s = x_{s-1},$$
im Widerspruch zur Minimalität von t.

Sei umgekehrt A nicht bijektiv; da M endlich ist, ist A dann auch nicht surjektiv. Man kann also $x_0 \in M - A(M)$ wählen. Dann kann niemals $x_0 = Ax_t$ sein, die Folge ist also nicht reinperiodisch. $\diamond$

Dieses Ergebnis lässt sich über die Begleitmatrix auf homogene mehrstufige Kongruenzgeneratoren, insbesondere auf lineare Schieberegister anwenden:

Korollar 1 *Ein homogener linearer Kongruenzgerator der Rekursionstiefe r erzeugt stets rein-periodische Folgen, wenn der Koeffizient a_r in $\mathbb{Z}/m\mathbb{Z}$ invertierbar ist. Ein lineares Schieberegister der Länge l erzeugt rein-periodische Folgen, wenn der Rückkopplungskoeffizient $a_l \neq 0$ ist.*

Die erste Aussage gilt auch im nicht-homogenen Fall, da die Formel
$$x_{n-r} = a_r^{-1}(x_n - a_1x_{n-1} - \cdots - a_{r-1}x_{n-r+1} - b)$$
für die Rückwärtsberechnung der Folge sorgt.