1.7 Mehrstufige 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.

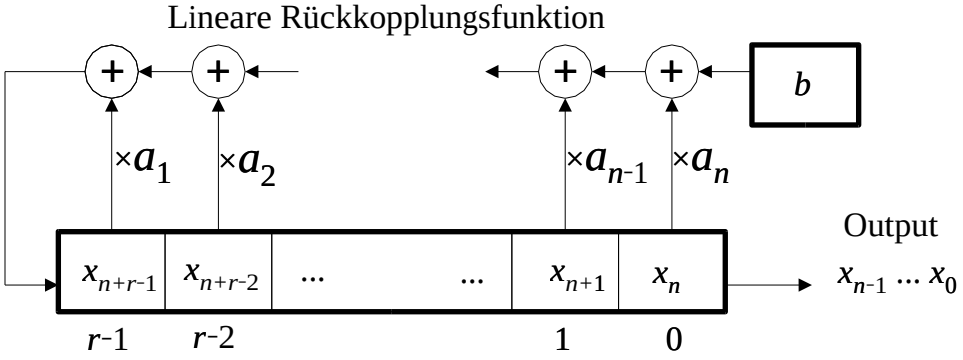

Abbildung 3: Ein linearer Rekurrenzgenerator

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** $x_{(n)} = (x_n, \ldots, x_{n+r-1})^t$ 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

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