2.2 Lineare Generatoren über Körpern

Hier wird der Spezialfall betrachtet, dass $R = K$ ein Körper und M ein endlich-dimensionaler K-Vektorraum ist (also ein noetherscher K-Modul).

Dann muss man nur das minimale k finden mit

$$\mathrm{Dim}(Kx_0 + \cdots + Kx_k) = \mathrm{Dim}(Kx_0 + \cdots + Kx_{k-1})$$

– diese Zahl ist dann das gesuchte k – und dann die Linearkombination

$$x_k = c_1 x_{k-1} + \cdots + c_k x_0.$$

Das ist eine Standard-Aufgabe der linearen Algebra.

Zur konkreten Berechnung wählt man eine feste Basis $(e_1, \ldots, e_r)$ von M. Sei

$$x_n = \sum_{i=1}^{r} x_{in} e_i$$

die jeweilige Basis-Darstellung. Da $\mathrm{Rang}(x_0, \ldots, x_{k-1}) = k$, gibt es eine Indexmenge $I = \{i_1, \ldots, i_k\} \subseteq \{1, \ldots, r\}$ mit $\#I = k$, so dass die Matrix

$$X = (x_{ij})_{i \in I, 0 \leq j < k} = \begin{pmatrix} x_{i_1 0} & \ldots & x_{i_1 k-1} \\ \vdots & & \vdots \\ x_{i_k 0} & \ldots & x_{i_k k-1} \end{pmatrix}$$

invertierbar ist. Die bisher noch unbekannten c_j gewinnt man aus dem Ansatz

$$x_k = \sum_{j=0}^{k-1} c_j x_j,$$

also

$$\sum_{i=1}^{r} x_{ik} e_i = \sum_{j=0}^{k-1} \sum_{i=1}^{r} c_j x_{ij} e_i,$$

also

$$x_{ik} = \sum_{j=0}^{k-1} x_{ij} c_j \quad \text{für alle } i \in I,$$

oder in Matrixschreibweise:

$$\bar{x} = (x_{ik})_{i \in I} = X \cdot c.$$

Die Lösung ist

$$c = X^{-1} \cdot \bar{x}.$$

Damit sind auch schon die ersten beiden Aussagen des folgenden Zusatzes zu Satz 1 bewiesen:

Satz 3 *Zusätzlich zu den Voraussetzungen von Satz 1 sei $R = K$ ein Körper. Dann gilt:*

(i) *Das minimale geeignete k ist das kleinste mit* $\operatorname{Dim}(Kx_0+\cdots+Kx_k) = k$*; es ist $k \leq \operatorname{Dim} M =: r$.*

(ii) *Die Koeffizienten $c_1, \ldots, c_k$ werden durch Lösung eines linearen Gleichungsystems mit invertierbarer quadratischer Koeffizientenmatrix bestimmt, deren Einträge aus Basiskoeffizienten von $x_0, \ldots, x_{k-1}$ bestehen.*

(iii) *Ist $k = r$, so ist A eindeutig aus den Basiskoeffizienten von $x_0, \ldots, x_k$ bestimmbar.*

Beweis. (iii) Seien

$$X_1 = (x_r, \ldots, x_1),\ X_0 = (x_{r-1}, \ldots, x_0) \in M_r(K).$$

Dann ist $X_1 = AX_0$ in Matrix-Darstellung bezüglich der Basis $(e_1, \ldots, e_r)$ von M. Da $\operatorname{Rang} X_0 = r$, ist X_0 invertierbar und

$$A = X_1 X_0^{-1},$$

wie behauptet. $\diamond$

Ist A invertierbar, so kann man analog die Folge (x_n) auch rückwärts berechnen, sobald man ein Stück $x_t, \ldots, x_{t+r}$ der Länge $r+1$ mit $\operatorname{Rang}(x_t, \ldots, x_{t+r-1}) = r$ gefunden hat.

Beispiel.

Im Fall eines r-stufigen homogenen linearen Kongruenzgenerators $x_n = a_1 x_{n-1} + \cdots a_r x_{n-r}$ über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit p prim ist

$$A = \begin{pmatrix} 0 & 1 & & \\ & \ddots & \ddots & \\ & & 0 & 1 \\ a_r & \ldots & a_2 & a_1 \end{pmatrix}, \quad \operatorname{Det} A = (-1)^r a_r.$$

Hier ist A also genau dann invertierbar, wenn $a_r \neq 0$, und das kann man o. B. d. A. annehmen – sonst ist die Rekursionstiefe $< r$.

Für die Vorhersage der Folge benötigt man dann höchstens $r+1$ Zustandsvektoren, also $2r$ Folgenglieder:

Korollar 1 *Ein r-stufiger homogener linearer Kongruenzgenerator mit bekanntem Primzahlmodul ist aus den $2r$ Folgegliedern $x_0, \ldots, x_{2r-1}$ vorhersagbar.*

Korollar 2 *Ein lineares Schieberegister der Länge l ist aus den ersten $2l$ Bits vorhersagbar.*

Korollar 3 *Ein homogener linearer Kongruenzgenerator mit bekanntem Primzahlmodul ist aus* x_0, x_1*, ein inhomogener aus* x_0, x_1, x_2, x_3 *vorhersagbar.*

Im nächsten Abschnitt wird u. a. gezeigt, dass bereits x_0, x_1, x_2 genügen.

Damit sind lineare Schieberegister als Quelle von Schlüsselbits für eine Bitstrom-Chiffre ein- für allemal kryptologisch erledigt. – Sollte die Länge zusätzlich geheim sein, kann der Kryptoanalytiker sie durch sukzessives Probieren bestimmen; das erhöht die Schwierigkeit des Angriffs nur unwesentlich.

Bei linearen Kongruenzgeneratoren könnte allerdings noch der Fall interessant sein, dass der Modul m geheimgehalten wird (und eventuell nicht prim ist). Dieser Fall wird im folgenden ebenfalls erledigt.