

2.1 Der allgemeine lineare Generator

Erinnern wir uns an die Beschreibung des allgemeinen linearen Generators: Gegeben sind

- als externe Parameter ein Ring R und ein R -Modul M ,
- als interner Parameter eine lineare Abbildung $A: M \rightarrow M$,
- als Zustand der Vektor $x_n \in M$,
- als Startwert der Vektor $x_0 \in M$,
- als Zustandsänderung die Rekursion $x_n = Ax_{n-1}$ für $n \geq 1$.

Bemerkung (Trivialfall): Falls A bekannt ist, ist aus jedem Folgeglied x_k die weitere Folge $(x_n)_{n \geq k}$ komplett vorhersagbar. Dieser Fall ist also kryptologisch völlig uninteressant. Die Rückwärtsberechnung von x_n mit $0 \leq n < k$ ist allerdings im allgemeinen nur möglich, wenn A injektiv ist. Das reicht natürlich nicht, um kryptologische Brauchbarkeit zu erreichen. Daher wird im folgenden meist nur das Problem der Vorwärtsberechnung behandelt und angenommen, dass ein Anfangsstück der Folge x_0, \dots, x_k bekannt ist. Trotzdem sollte man das Problem der Rückwärtsberechnung auch immer im Auge behalten.

Annahme also jetzt: R und M sind bekannt, A ist unbekannt, ein Anfangsstück x_0, \dots, x_k ist bekannt (o. B. d. A. $x_0 \neq 0$). Das *Vorhersageproblem* ist: Kann man daraus x_{k+1}, x_{k+2}, \dots bestimmen?

Man kann, wenn es einem gelingt, eine Linearkombination

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

zu bestimmen – also mit bekannten Koeffizienten c_1, \dots, c_k . Dann ist nämlich

$$\begin{aligned} x_{k+1} &= Ax_k = c_1 Ax_{k-1} + \dots + c_k Ax_0 \\ &= c_1 x_k + \dots + c_k x_1 \\ &\vdots \\ x_n &= c_1 x_{n-1} + \dots + c_k x_{n-k} \quad \text{für alle } n \geq k, \end{aligned}$$

die weitere Folge also komplett bestimmt – ohne dass man A kennt(!). Wie findet man eine solche Linearkombination?

Die Antwort liegt – natürlich – in der linearen Algebra. Im gegenwärtigen abstrakten Rahmen setzt man voraus, dass M noethersch ist (das ist die „richtige“ Verallgemeinerung von endlich-dimensionalen Vektorräumen); dann ist die aufsteigende Folge von Untermoduln

$$Rx_0 \subseteq Rx_0 + Rx_1 \subseteq \dots \subseteq M$$

stationär, d. h., es gibt ein k mit $x_k \in Rx_0 + \dots + Rx_{k-1}$: das ist die gesuchte lineare Relation. – Falls M endlich ist, wie wir es bei der Zufallserzeugung ja meist einrichten, ist die noethersche Eigenschaft selbstverständlich trivial. – Das erste solche k reicht, alle übrigen x_n , $n \geq k$, liegen dann auch in diesem Untermodul.

Wir haben also gezeigt:

Satz 1 (Noethersches Prinzip für lineare Generatoren) *Sei R ein Ring, M ein noetherscher R -Modul, $A: M \rightarrow M$ linear und $(x_n)_{n \in \mathbb{N}}$ eine Folge in M mit $x_n = Ax_{n-1}$ für $n \geq 1$. Dann gibt es ein $k \geq 1$ und $c_1, \dots, c_k \in R$ mit*

$$x_n = c_1 x_{n-1} + \dots + c_k x_{n-k} \quad \text{für alle } n \geq k.$$

Jedes k mit $x_k \in Rx_0 + \dots + Rx_{k-1}$ ist geeignet.

Wie bestimmt man aber den Index k und die Koeffizienten c_1, \dots, c_k praktisch? Dazu muss man natürlich in R und M rechnen können. Wir betrachten im folgenden zwei Beispiele: $R = K$ ein Körper oder $R = \mathbb{Z}/m\mathbb{Z}$ ein Restklassenring von ganzen Zahlen.

In beiden Fällen kann man von vornherein etwas darüber sagen, wie oft eine echte Zunahme in der Kette der Untermoduln vorkommen kann. Ist z. B. R ein Körper, so ist die Anzahl der echten Schritte durch die Vektorraum-Dimension $\dim M$ beschränkt. Allgemein gilt:

Satz 2 (KRAWCZYK) *Sei M ein R -Modul und $0 \subset M_1 \subset \dots \subset M_l \subseteq M$ eine echt aufsteigende Kette von Untermoduln. Dann ist $2^l \leq \#M$.*

Dieser Satz ist natürlich nur dann nützlich, wenn M endlich ist. Aber das ist ja derjenige Fall, der für die Vorhersage von Kongruenzgeneratoren am meisten interessiert. Man kann dann auch $l \leq {}^2\log(\#M)$ schreiben. Das ist nicht so viel schlechter als die Abschätzung im Fall Körper/Vektorraum, beides endlich: $l \leq \dim(M) \leq {}^2\log(\#M)/{}^2\log(\#R)$.

Beweis. Sei $b_i \in M_i - M_{i-1}$ für $i = 1, \dots, l$ (mit $M_0 = 0$). Dann besteht die Menge

$$U = \{c_1 b_1 + \dots + c_l b_l \mid \text{alle } c_i = 0 \text{ oder } 1\} \subseteq M$$

aus 2^l verschiedenen Elementen. Wären nämlich zwei davon gleich, so wäre ihre Differenz (für ein t mit $1 \leq t \leq l$) von der Form

$$e_1 b_1 + \dots + e_t b_t = 0 \text{ mit } e_i \in \{0, \pm 1\}, e_t \neq 0.$$

Da $e_t = \pm 1 \in R^\times$, folgte $b_t = -e_t^{-1}(e_1 b_1 + \dots + e_{t-1} b_{t-1}) \in M_{t-1}$, Widerspruch. Also ist $\#M \geq \#U = 2^l$. \diamond