HAMFU
HISTORY

KRIEG IM AETHER

Vorlesungen an der Eidgenössischen Technischen Hochschule in Zürich
im Wintersemester 1978/1979
Leitung: Abteilung für Übermittlungstruppen, Divisionär A. Guisolan

Kryptologie: Analyse und Synthese rekursiver Folgen

Referent: Dr. P. Nyffeler

Diese Vorlesung wurde durch die Stiftung HAMFU digitalisiert und als
PDF Dokument für www.hamfu.ch aufbereitet.

KRYPTOLOGIE : ANALYSE UND SYNTHESE REKURSIVER FOLGEN

Dr. P. Nyffeler

Inhalt

1. Einleitung und Uebersicht
2. Die **D**- Transformation
2.1. Die **Z**- Transformation als "diskrete" **L**- Transformation
2.2. Die **D**- Transformation als spezielle **Z**- Transformation
2.3. Eigenschaften der **D**- Transformation
2.4. Die Rücktransformation $\mathbf{D}^{-1}$
3. Anwendungen der **D**- Transformation
3.1. Die Taktsteuerung
3.2. Die Produktschaltung
3.3. Die Binomialfaltung
4. Zusammenfassung
5. Literaturhinweise

1. Einleitung und Uebersicht

In diesem Vortrag geht es darum, Folgen durch eine günstige Transformation so zu beschreiben, dass die Eigenschaften dieser Folgen leicht untersucht werden können.

Adresse des Autors:

Peter Nyffeler, Dr. phil. nat.,
c/o Bundesamt für Uebermittlungstruppen
3000 Bern 25

Um den Zusammenhang mit kryptologischen Problemstellungen anzudeuten, zeigt Fig. 1 das allgemeine Chiffrierprinzip:

Fig. 1: Allgemeines Chiffrierprinzip

Der Klartext **K** wird durch den Chiffriergenerator **ChG** mit Hilfe des geheimen Schlüssels **S** in den Chiffretext **C** umgewandelt:

$$C = f(K,S)$$

Die Abbildung **f** muss so geartet sein, dass **K** wieder zurückgewonnen werden kann:

$$K = f^{-1}(C,S)$$

K und **C** sind nichts anderes als Teilfolgen aus Elementen eines endlichen Alphabets.

Fig. 2 zeigt das spezielle Chiffrierprinzip, bei welchem der Chiffriergenerator in Anlehnung an den "one time pad" in den eigentlichen Chiffriergenerator und den Mischer **M** zerlegt ist:

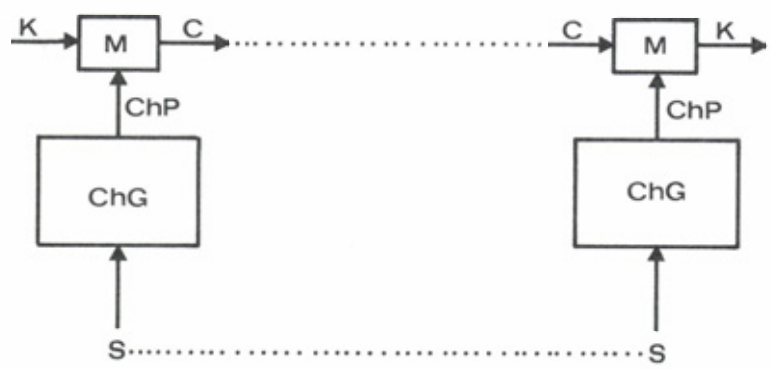


Fig. 2: Spezielles Chiffrierprinzip

Hier kommt als weitere Folge das Chiffrierprogramm **ChP** dazu, eine Folge, welche "möglichst zufällig" aufgebaut sein muss.

Damit ist das Bedürfnis zur Behandlung von Folgen aufgezeigt. Dabei beschränken wir uns, im Hinblick auf die Beispiele, auf Folgen aus Elementen des (einfachsten) Alphabets $Z_2=\{0,1\}$

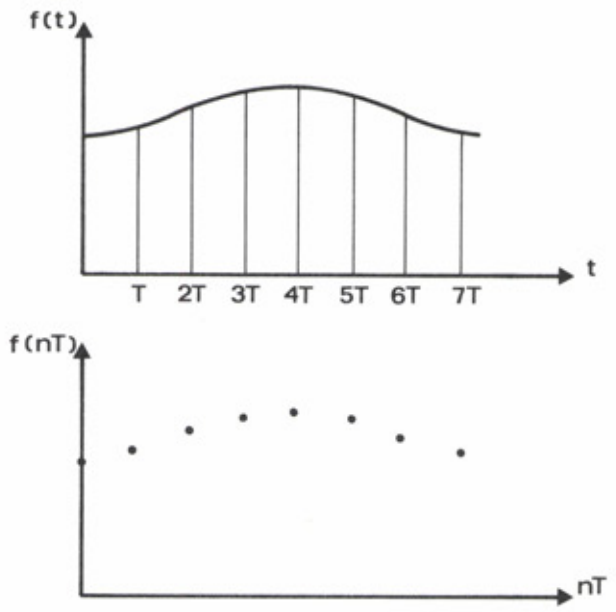
Im nächsten Kapitel wird eine hier günstige Transformation, die **D**- Transformation, beschrieben und gezeigt, wie sich eine Folge als Superposition von einfacheren Teilfolgen darstellen lässt. Dies wird auch im ersten Beispiel des dritten Kapitels illustriert.

Anhand von zwei weiteren, ausgewählten Beispielen wird im dritten Kapitel das umgekehrte Vorgehen, die Zusammensetzung einfacher Folgen zu einer "komplizierteren" Folge, gezeigt.

2. Die D- Transformation

2.1. Die Z- Transformation als "diskrete" L- Transformation

Die Z- Transformation entsteht durch diskrete Abtastung aus der L- Transformation (Laplace-Transformation), wie Fig. 3 veranschaulicht:



$$f(nT) \curvearrowright Z[f] = F[z] = \sum_{n=0}^{\infty} f(nT)\, z^{-n}$$

Fig. 3: Die Z- Transformation

Dabei geht das bei der L- Transformation auftretende Integral in eine unendliche Summe über; der ursprünglichen Funktion wird also bei der Z- Transformation eine Potenzreihe in der komplexen Variablen z zugeordnet.

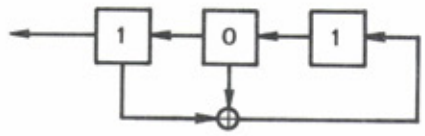
2.2. Die D- Transformation als spezielle Z- Transformation

Betrachtet man nur Funktionen (Folgen) mit diskreten Funktionswerten, so geht die Z- Transformation in die D- Transformation über:

L- Transformation, diskrete Argumente $\Longrightarrow$ Z- Transformation

Z- Transformation, diskrete Funktionswerte $\Longrightarrow$ D- Transformation

Die D- Transformation soll nun zuerst an einem einfachen Beispiel, einer SR- Folge, nachvollzogen werden. Fig. 4 zeigt, wie die binäre SR- Folge als formale Potenzreihe in D dargestellt werden kann:



$$a(n) = \{1\ 0\ 1\ 1\ 1\ 0\ 0 \mid 1\ 0\ 1 \ldots\}$$

$$A(D) = (1+D^{-2}+D^{-3}+D^{-4})+(D^{-7}+D^{-9}+D^{-10}+D^{-11}) + \ldots$$

$$A(D) = (\cancel{1}+\cancel{D^{-2}}+\cancel{D^{-3}}+\cancel{D^{-4}})+(\cancel{D^{-7}}+\cancel{D^{-9}}+\cancel{D^{-10}}+\cancel{D^{-11}}) + \ldots$$

$$D \cdot A(D) = (\cancel{D}+\cancel{D^{-1}}+\cancel{D^{-2}}+\cancel{D^{-3}})+(\cancel{D^{-6}}+\cancel{D^{-8}}+\cancel{D^{-9}}+\cancel{D^{-10}}) + \ldots$$

$$D^3 \cdot A(D) = (\cancel{D^3}+\cancel{D}+\cancel{1}+\cancel{D^{-1}})+(\cancel{D^{-4}}+\cancel{D^{-6}}+\cancel{D^{-7}}+\cancel{D^{-8}}) + \ldots$$

$$\Longrightarrow \boxed{A(D) = D \cdot \frac{D^2}{1+D+D^3}}$$

Fig. 4: **D**- Transformation einer **SR**- Folge

Weil die **SR**- Folge rekursiv ist, lässt sich dabei die formale Potenzreihe weiterverarbeiten und als Quotient zweier Polynome schreiben. Es gelten die folgenden anschaulichen Korrespondenzen:

D	$\longleftrightarrow$	Verzögerungsglied
$1+D+D^3$	$\longleftrightarrow$	Rekursion
D^2	$\longleftrightarrow$	Anfangsstellung

2.3. Eigenschaften der **D**-Transformation

Das im letzten Abschnitt anhand eines Beispiels durchgeführte Vorgehen kann nun allgemein formuliert werden. Jeder binären Folge wird vorerst eine formale Potenzreihe über Z_2 zugeordnet:

$$a(n) = \{a_n\} \in Z_2^{N_0} \xrightarrow{D} A(D) \in Z_2[[D]]$$

Dabei entsprechen sich die folgenden Operationen der beiden Ringe:

$$\{a_n\}+\{b_n\} = \{a_n+b_n\} \longleftrightarrow A(D)+B(D)$$

$$\{a_n\}*\{b_n\} = \{\sum_{i=0}^{n} a_i b_{n-i}\} \longleftrightarrow A(D)\cdot B(D)$$

Für rekursive Folgen lässt sich die entsprechende formale Potenzreihe als Quotient zweier Polynome darstellen:

$$A(D) = D \cdot \frac{p(D)}{r(D)}$$

Dabei entspricht der Zähler $p(D)$ der Anfangsstellung $(a_0,\ldots,a_{k-1})$ und der Nenner $r(D)$ dem Rekursionspolynom $r(x)$ der Folge.

Damit diese Polynomdivision überhaupt durchführbar ist, wird der Ring der formalen Potenzreihen (analog dem Uebergang von den ganzen zu den rationalen Zahlen) in den Körper der formalen Laurentreihen eingebettet. Die Elemente dieses Körpers nennt man auch etwa Operatoren; **D** kann als eine Art Verschiebungsoperator aufgefasst werden:

$$D(\{a_{n+\varrho}\}) = D^{-\varrho}A(D) + \sum_{i=0}^{\varrho-1} a_i D^{i-\varrho}$$

2.4. Die Rücktransformation D^{-1}

Schon bei der **Z**- Transformation lässt sich die Rücktransformation dann besonders einfach beschreiben, wenn man die Pole (Nullstellen des Nennerpolynoms) kennt.

Dies soll hier am Beispiel aus Abschnitt 2.2. illustriert werden. Dazu muss der Erweiterungskörper von Z_2 bezüglich der Wurzeln von $1+x+x^3$, das Galoisfeld $GF(2^3)$, gebildet werden. Fig. 5 zeigt das Vorgehen anhand dieses Beispiels:

$$\{a_n\} \xrightarrow{D} A(D) = D \cdot \frac{D^2}{1+D+D^3}$$

Partialbruchzerlegung

$$A(D) = D \cdot \left[\frac{A_0}{D+\alpha_0} + \frac{A_1}{D+\alpha_1} + \frac{A_2}{D+\alpha_2}\right]$$

$$A(D) = D \cdot \left[\frac{\alpha^3}{D+\alpha} + \frac{\alpha^6}{D+\alpha^2} + \frac{\alpha^5}{D+\alpha^4}\right]$$

$$\{\alpha^n\} \xrightarrow{D^{-1}} \frac{D}{D+\alpha}$$

$$\{a_n\} = \left\{\sum_{i=0}^{2} A_i \alpha_i^n\right\} \xrightarrow{D^{-1}} A(D)$$

Fig. 5: Die Rücktransformation D^{-1}

Damit hat man die ursprüngliche Folge als Superposition von Folgen mit Elementen aus dem endlichen Körper $GF(2^3)$ dargestellt, wie Fig. 6 verdeutlichen soll:

$A_0\alpha_0^n$:	α^3	α^4	α^5	α^6	1	α	α^2	α^3	...
$A_1\alpha_1^n$:	α^6	α	α^3	α^5	1	α^2	α^4	α^6	...
$A_2\alpha_2^n$:	α^5	α^2	α^6	α^3	1	α^4	α	α^5	...
	1	0	1	1	1	0	0	1	...

Fig. 6 : Superposition von $\{a_n\}$

Dabei lässt sich die Struktur der Folge $\{a_n\}$ schon aus der einen Folge:

$$\alpha^3\ \alpha^4\ \alpha^5\ \alpha^6\ 1\ \ \alpha\ \ \alpha^2\ \alpha^3\ \ldots$$

ablesen. Eine solche Folge wird in [4] als Galoisfolge bezeichnet. Da die obige Folge durch das Paar $(A_0, \alpha_0) = (\alpha^3, \alpha)$ bestimmt ist, ergibt sich gesamthaft:

$$\boxed{\{a_n\} \longleftrightarrow (A_0, \alpha_0) = (\alpha^3, \alpha)}$$

Dabei charakterisiert A_0 die Anfangsstellung und α_0 die Rekursion der ursprünglichen Folge.

Damit ist ein wirksames Instrumentarium zur Analyse und Synthese von Folgen bereitgestellt. Je nach Problemstellung wird man dabei im (diskreten) "Zeitbereich" bzw. im "D- Bereich" arbeiten, analog etwa zum Zeit- bzw. Frequenzbereich bei der Fouriertransformation.

Dies sollen die drei Beispiele im nächsten Kapitel veranschaulichen.

3. Anwendungen der D- Transformation

3.1. Die Taktsteuerung

Bei der Taktsteuerung wird, wie es der Name andeutet, aus einer Folge

$$\{a_t\} = \{a_0, \ldots, a_t, \ldots\}$$

die neue Folge

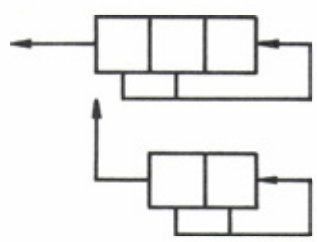
$$\{a_{n_t}\} = \{a_{n_0}, \ldots, a_{n_t}, \ldots\}$$

gebildet, wobei die neuen "Zeiten" n_t durch eine zweite Folge

$$\{b_t\} = \{b_0, \ldots, b_t, \ldots\}$$

bestimmt werden.

Fig. 7 zeigt ein Beispiel einer solchen Taktsteuerung. Dabei führt das Hauptschieberegister nur dann einen Takt aus, wenn der Ausgang des Steuerschieberegisters eine "1" ist, sonst bleibt es stehen (Ausgang eine "0").



$\{a_t\}$: 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 · · ·

$\{b_t\}$: 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 · · ·

$\{a_{n_t}\}$: $0_0\,1\,1_1\,1\,0_0\,1\,0_0\,0\,1_1\,1\,1_1\,0\,1_1\,0 \cdots$

Fig. 7: Taktgesteuertes Schieberegister

Die ursprüngliche Folge wird dabei so verändert, dass einzelne Glieder mehrfach auftreten (kleine Symbole)

Man kann nun durch Behandlung im **D**- Bereich zeigen, dass sich die entstandene Folge als Superposition von "gespreizten" Folgen gleicher Rekursion darstellen lässt. Dies soll die folgende Fig. 8 veranschaulichen:

$$\{a_{n_t}\}: \quad \underline{0\,0\,1\,1\,1\,1\,0\,0\,1\,0\,0\,0\,1\,1\,1\,1\,1\,0\,1\,1\,0\cdots}$$

$$\begin{array}{ccccccc} 0 & 1 & 0 & 0 & 1 & 1 & 1\cdots \\ & 0 & 1 & 0 & 0 & 1 & 1 & 1\cdots \\ & & 1 & 1 & 1 & 0 & 1 & 0 & 0\cdots \end{array}$$

Fig. 8: Taktsteuerung als Superposition von "gespreizten" Folgen gleicher Rekursion

3.2. Die Produktschaltung

In den beiden nächsten Beispielen sollen zwei Folgen zu einer neuen, "komplizierteren" Folge zusammengesetzt werden. Wir gehen dabei von zwei **SR**- Folgen aus. Fig. 9 zeigt, wie diese beiden Folgen gemäss Kapitel 2 charakterisiert werden können.

Dabei ist α ein Element des Erweiterungskörpers $Z_2(\alpha)$, dem Galoisfeld $GF(2^2)$, und β ein Element des Erweiterungskörpers $Z_2(\beta)$, dem Galoisfeld $GF(2^3)$.

Wir wollen nun die Folgen $\{a_n\}$ und $\{b_n\}$ so zusammensetzen, dass sich die resultierende Rekursion durch das Produkt $\alpha\cdot\beta$ charakterisieren lässt. Diese Operation entspricht dem "Skalarprodukt" $\{a_n \cdot b_n\}$ der beiden Folgen. Wie die entstehende Galoisfolge wiederum eine **SR**- Folge bestimmt, zeigt Fig. 10.

$$\{a_n\} \quad A(D) = D \cdot \frac{1}{1+D+D^2}$$

$$(1,\alpha) \quad A(D) = D\left[\frac{1}{D+\alpha}+\frac{1}{D+\alpha^2}\right]$$

$$\{b_n\} \quad B(D) = D \cdot \frac{1+D}{1+D+D^3}$$

$$(\beta^4,\beta) \quad B(D) = D\left[\frac{\beta^4}{D+\beta}+\frac{\beta}{D+\beta^2}+\frac{\beta^2}{D+\beta^4}\right]$$

Fig. 9: **D**- Transformation von **SR**- Folgen

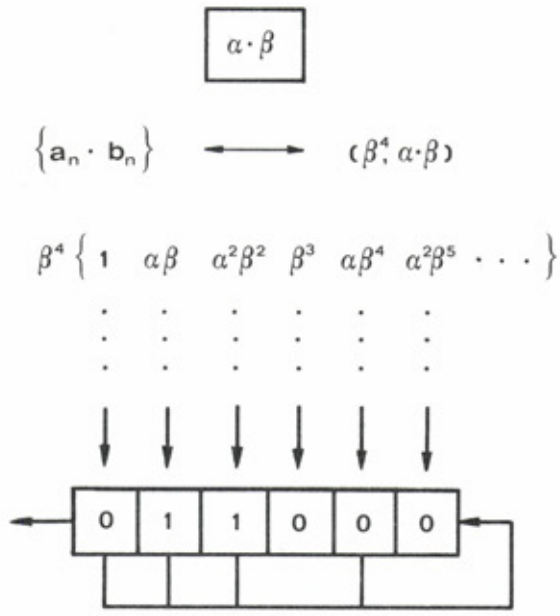


Fig. 10: Produktrekursion

Dieses Beispiel veranschaulicht den allgemein gültigen Satz:

Sind die Rekursionspolynome $\nu_\alpha(x)=1+x+x^2$ und $\nu_\beta(x)=1+x+x^3$ irreduzibel und ihre Grade teilerfremd $(ggT(2,3)=1)$, dann ist das Produktrekursionspolynom $\nu_{\alpha\cdot\beta}(x)=1+x+x^2+x^4+x^6$ auch irreduzibel vom Produktgrad $2\cdot 3=6$, aber nicht primitiv $(T_{\alpha\cdot\beta}=T_\alpha\cdot T_\beta = 3\cdot 7 = 21!)$.

3.3. Die Binomialfaltung

Wie im letzten Abschnitt, gehen wir auch hier von den beiden Folgen

$$\{a_n\} \longleftrightarrow (1, \alpha) \quad \text{und}$$

$$\{b_n\} \longleftrightarrow (\beta^4, \beta)$$

aus. Die resultierende Rekursion soll sich nun aber durch die Summe $\alpha+\beta$ charakterisieren lassen. Dies entspricht der Binomialfaltung

$$\left\{ \sum_{i=0}^{n} \binom{n}{i}_{\text{mod } 2} a_i \cdot b_{n-i} \right\}$$

der beiden Folgen.

Die resultierende Folge ist in Fig. 11 dargestellt:

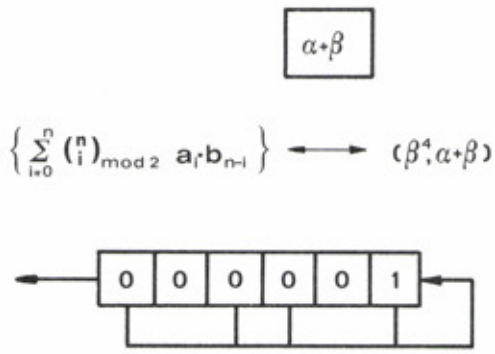


Fig. 11: Die Binomialfaltung
(Summenrekursion)

Hier gilt der allgemein gültige Satz:

Sind die Rekursionspolynome $\nu_\alpha(x)=1+x+x^2$ und $\nu_\beta(x)=1+x+x^3$ irreduzibel und ihre Grade teilerfremd (ggT(2,3)=1), dann ist das Summenrekursionspolynom $\nu_{\alpha+\beta}(x) = 1+x^2+x^3+x^5+x^6$ auch irreduzibel vom Produktgrad $2\cdot 3=6$.

In diesem Beispiel ist das Summenrekursionspolynom primitiv. Dies gilt aber nur, weil $\nu_\beta(\alpha)= 1+\alpha+\alpha^3=\alpha$ und $\nu_\alpha(\beta)=1+\beta+\beta^2=\beta^5$ primitiv sind:

$\nu_{\alpha+\beta}(x)$ ist nur dann primitiv, wenn $\nu_\beta(\alpha)$ in $Z_2(\alpha)$ und $\nu_\alpha(\beta)$ in $Z_2(\beta)$ primitiv sind.

Damit ist gleichzeitig eine Teillösung zur Bestimmung primitiver Polynome beliebigen Grades aufgezeigt.

4. Zusammenfassung

Zur Analyse und Synthese von rekursiven (periodischen) Folgen steht in der **D**- Transformation ein wirksames Hilfsmittel zur Verfügung.

Dabei lässt sich jede solche Folge als Superposition von Galoisfolgen darstellen. Umgekehrt wurde am Beispiel der Produktrekursion und Summenrekursion gezeigt, wie sich irreduzible und sogar primitive Rekursionspolynome höheren Grades konstruieren lassen.

5. Literaturhinweise

[1] W.H. Kautz (Herausgeber): Linear Sequential Switching Circuits, Holden-Day, 1965

[2] E.I. Jury: Theory and Application of the Z-Transform Method, John Wiley, 1964

[3] N. Zierler: Linear Recurring Sequences, J. Soc. Indust. Appl. Math. 7 (1959), S. 31 - 48

[4] F. Surböck, Struktur periodischer Binärfolgen, Dissertation an der Technischen Universität Wien, 1977

[5] P. Nyffeler: Binäre Automaten und ihre linearen Rekursionen, Dissertation an der Universität Bern, 1975