DIPLOMARBEIT

Kettenbrüche im Körper der formalen Laurentreihen und Anwendungen

ausgeführt am Institut für Geometrie

der Technischen Universität Wien

unter der Anleitung von Ao.Univ.Prof. Dr. Michael Drmota

durch

Michael Fuchs

Schönburgstraße 7/3, 1040 Wien

3. April 2000 ....

Vorwort

Die Kettenbruchentwicklung einer reellen Zahl ist eines der Grundwerkzeuge in der klassischen Zahlentheorie und besitzt auch in vielen anderen Teilgebieten der Mathematik eine große Bedeutung. Der Grund liegt darin, dass in der Kettenbruchentwicklung einer reellen Zahl, die gesamte Information über die Approximierbarkeit der Zahl durch rationale Zahlen enthalten ist.

Man kann sich auch vom Körper der reellen Zahlen lösen und Kettenbrüche in anderen Körpern betrachten. Eine spezielle Klasse solcher Körper, in denen für Kettenbrüche viele Resultate der klassischen Theorie erhalten bleiben, geht auf E. Artin zurück.

In der berühmten Dissertation von Artin "Quadratische Zahlenkörper im Gebiete der höheren Kongruenzen, Algebraischer Teil" ([1]) überträgt dieser die Ergebnisse der Algebraischen Zahlentheorie über $\mathbb{Q}$ auf den Körper der formalen Laurentreihen über den Restklassenkörper $\mathbb{Z}_p$. Darunter versteht man die Menge aller formalen Summen der Form

$$\sum_{i=n}^{\infty} a_i x^{-i} \quad n \in \mathbb{Z}, \quad a_i \in \mathbb{Z}_p,$$

wobei Addition und Multiplikation wie im Potenzreihenring erklärt sind.

Um im sogenannten reell-quadratischen Fall zu zeigen, dass die Klassenzahl endlich ist, betrachtet Artin in diesem Körper Kettenbrüche, die er in völliger Analogie zur klassischen Theorie erklärt. Für den Beweis der Endlichkeit der Klassenzahl zeigt er, dass eines der schönsten Resultate der klassischen Theorie der Kettenbrüche, nämlich der Satz von Lagrange (siehe [6]), auch in diesem Körper gültig bleibt.

Das erste Kapitel dieser Arbeit beschäftigt sich mit den Grundlagen der Theorie dieser Kettenbrüche, wobei der Körper der Laurentreihen nicht nur über dem Restklassenkörper, sondern über jedem beliebigen Körper betrachtet wird. Insbesondere soll auch die starke Analogie zur klassischen Theorie aufgezeigt werden. Für die klassische Theorie sei auf das Standardwerk von

Khintchine [6] und auf das Buch von Rockett und Szüsz [18] verwiesen, sowie auf jedes Buch über elementare Zahlentheorie (siehe etwa [4],[16],[21]).

Die ersten 4 Unterabschnitte dieses Kapitels beinhalten die grundlegenden Definitionen und einfache Eigenschaften der Kettenbrüche über dem Körper der Laurentreihen. Viele Begriffe und Eigenschaften wurden dabei unmittelbar der klassischen Theorie entnommen ([4],[16],[21]) oder stellen Verallgemeinerungen der Artinschen Resultate dar. Insbesondere war es mir ein Anliegen, zunächst zwischen endlichen und unendlichen Kettenbrüchen genau zu unterscheiden und diese erst später zu einem Ganzen zusammenzufügen. Dabei sieht man, dass der Kettenbruchalgorithmus für endliche Kettenbrüche im engen Zusammenhang mit einem anderen wichtigen Algorithmus der Mathematik, nämlich dem euklidischen Algorithmus, steht und dass endliche Kettenbrüche in jedem Quotientenkörper über einem euklidischen Ring betrachtet werden können.

Der 4. Unterabschnitt endet mit dem Resultat, dass jede Laurentreihe genau eine Kettenbruchentwicklung besitzt, und dass diese für rationale Laurentreihen und nur für solche endlich ist. Dies zeigt zum ersten Mal die starke Analogie zur klassischen Theorie.

Im Unterabschnitt 5 wird ein weiteres wichtiges Resultat der klassischen Theorie im Körper der formalen Laurentreihen wiedergefunden, nämlich die Bestapproximationseigenschaft der Näherungsbrüche. Begriffsbildungen und Beweis sind dabei dem Buch von deMathan [10] entnommen.

In den verbleibenden 3 Unterabschnitten wird der Satz von Lagrange aus der klassischen Theorie auf den Körper der formalen Laurentreihen übertragen. Dabei muss allerdings die Endlichkeit des Grundkörpers vorausgesetzt werden. Die Beweisidee stammt wieder aus dem Buch von deMathan. Diese geht aber im wesentlichen auf den klassischen Beweis von Artin zurück.

Das zweite Kapitel beschäftig sich mit der Anwendung der Theorie der Kettenbrüche auf die Komplexität von Folgen.

In kryptologischen Anwendungen werden Folgen benötigt, die zufällig und unvorhersehbar sind. Das lineare Komplexitätsprofil hat sich dabei als gutes Maß zur Bewertung von Folgen bezüglich dieser Eigenschaften herausgestellt.

Zwischen dem linearen Komplexitätsprofil von Folgen und der Kettenbruchentwicklung im Körper der formalen Laurentreihen besteht ein enger Zusammenhang. Dieser Zusammenhang wird in den ersten drei Unterabschnitten behandelt. Das Hauptresultat ist dabei der erste Satz im Unterabschnitt 3 der auf Niederreiter [12] zurückgeht. Bei der Herleitung wurde der Weg über das rationale Approximationsproblem eingeschlagen (siehe [5]), aus dem das Resultat am natürlichsten folgt. Der Beweis basiert auf der Beweisidee aus [23].

Unterabschnitt 4 behandelt die Konstruktion von Folgen mit vorgegebenen Komplexitätsprofil. Der dabei betrachtete Algorithmus stammt von Niederreiter [12].

Im Unterabschnitt 5 wird das rationale Approximationsproblem vollständig gelöst. Der Beweis ist eine Mischung aus den Beweisen von [12] und [23].

Im Unterabschnitt 6 wird schließlich gezeigt, dass der berühmte Synthese Algorithmus von Berlekamp und Massey (siehe [8]), sehr natürlich aus dieser Betrachtung des linearen Komplexitätsprofils folgt.

Die verbleibenden Unterabschnitte widmen sich der Frage, welche Forderungen an das Komplexitätsprofil zu geeigneten Folgen führen, also Folgen die unabängig und unvorhersehbar sind. Dazu benötigt man insbesondere eine Reihe von wahrscheinlichkeitstheoretischen Aussagen, die in den Unterabschnitten 10 und 11 hergeleitet werden. All diese Resultate sind im wesentlichen aus den Arbeiten von Niederreiter [12],[13],[14] entnommen.

Abschließend möchte ich mich noch bei Prof. Niederreiter bedanken, der dieses interessante Thema vorgeschlagen hat und mir bei der Literaturauswahl behilflich war, sowie bei meinem Betreuer Prof. Drmota. Weiters bei Clemens und Anna für das fleißige Korrekturlesen, bei Fernande für die Übersetzung des französischen Buches von deMathan ins Deutsche und bei allen anderen, die direkt oder indirekt an der Entstehung dieser Arbeit beteiligt waren.

Wien, April 2000 Michael Fuchs

Inhaltsverzeichnis

Kapitel 1

Kettenbrüche

1.1 Der Körper der formalen Laurentreihen

Sei K ein Körper. Wir betrachten die Menge der folgenden formalen Summen

$$\sum_{i=n}^{\infty} a_i x^{-i} \quad n \in \mathbb{Z}, \quad a_i \in K.$$

Dabei wollen wir alle Summen identifizieren, die bis auf führende Nullen übereinstimmen. Weiters versehen wir diese Menge mit einer Addition und einer Multiplikation, die wie im Potenzreihenring über K erklärt sein sollen. Die so entstehende algebraische Struktur soll mit $K((x^{-1}))$ bezeichnet werden. Wir wollen zeigen, dass $K((x^{-1}))$ ein Körper ist.

Vorbereitend benötigen wir ein einfaches Ergebnis aus der Theorie der formalen Potenzreihen über einem Körper. Wie üblich bezeichnen wir den Potenzreihenring über einem Körper K mit $K[[x]]$.

Hilfssatz 1.1.1 *Sei $A \in K[[x]]$. Dann gilt*

$$A = \sum_{i=0}^{\infty} a_i x^i \quad \textit{ist Einheit} \quad \Longleftrightarrow \quad a_0 \neq 0.$$

Damit gilt wie schon erwähnt

Satz 1.1.2 *$K((x^{-1}))$ ist ein Körper, der sogenannte Körper der formalen Laurentreihen über K.*

Beweis. Betrachtet man zu festem $n_0 \in \mathbb{Z}$ alle $S \in K((x^{-1}))$ mit

$$S = \sum_{i=n_0}^{\infty} a_i x^{-i} \quad a_i \in K,$$

dann erhält man, aufgrund der Definition von Addition und Multiplikation in $K((x^{-1}))$, einen Ring der isomorph zum Potenzreihenring ist.

Damit sind die Ringaxiome in $K((x^{-1}))$ klar.

Bleibt also noch die Existenz von multiplikativen Inversen zu zeigen.
Dazu sei $S \in K((x^{-1})), S \neq 0$ gegeben, also

$$S = \sum_{i=n}^{\infty} a_i x^{-i} \quad a_i \in K, \quad a_n \neq 0.$$

Es gilt

$$S = \sum_{i=n}^{\infty} a_i x^{-i} = x^{-n} \sum_{i=0}^{\infty} a_{n+i} x^{-i} = x^{-n} A.$$

Aufgrund des Hilfssatzes 1.1.1 und der vorher erwähnten Isomorphie ist A eine Einheit. Also gibt es ein B mit $AB = 1$ und damit ist $S^{-1} = x^n B$. ■

Im Körper $K((x^{-1}))$ ist insbesondere der Polynomring $K[x]$ und damit auch der Körper der rationalen Funkionen $K(x)$ über K enthalten.
$K((x^{-1}))$ hat also eine ähnliche Struktur wie der Körper der reellen Zahlen und dadurch sind auch die Bezeichnungen *rationale Elemente* für die Elemente von $K(x)$ und *irrationale Elemente* für alle anderen motiviert.

Als nächstes wollen wir die Gradfunktion vom Polynomring auf $K((x^{-1}))$ fortsetzen.

Definition 1.1.3 Die Abbildung $v : K((x^{-1})) \longrightarrow \mathbb{Z} \cup \{-\infty\}$, die für $S \in K((x^{-1})), S \neq 0$ mit

$$S = \sum_{i=n}^{\infty} a_i x^{-i} \quad a_n \neq 0$$

durch $v(S) = -n$ und für $S = 0$ durch $v(S) = -\infty$ erklärt ist, heißt *Bewertung* von $K((x^{-1}))$.

Sie hat die folgenden, unmittelbar klaren Eigenschaften

Satz 1.1.4 *Für $S, T \in K((x^{-1}))$ und $A, B \in K[x], B \neq 0$ gilt*

1. $v(ST) = v(S) + v(T)$,
2. $v(S+T) \leq \max(v(S), v(T))$,
3. $v(S+T) = \max(v(S), v(T)) \quad$ *wenn* $\quad S \neq T$,

4. $v(A) = \deg(A)$,
5. $v(\frac{A}{B}) = \deg(A) - \deg(B)$.

Bei dieser Bewertung handelt es sich nicht um eine klassische Bewertung im Sinne der Bewertungstheorie. Aber man kann damit sehr leicht eine klassische Bewertung definieren.

Dazu sei $b \in \mathbb{N}, b \geq 2$ und wir definieren

$$|\,.\,| : \left\{ \begin{array}{ccc} K((x^{-1})) & \longrightarrow & \mathbb{R}_0^+ \\ S & \longmapsto & b^{v(S)} \end{array} \right.$$

wobei $b^{-\infty} = 0$ ist.

Aus den Eigenschaften von v und der Definition von $|.|$ folgt sofort

Satz 1.1.5 *$|\,.\,|$ ist eine nicht-archimedische Bewertung von $K((x^{-1}))$.*

Wie üblich erhalten wir deshalb durch

$$d : \left\{ \begin{array}{ccc} K((x^{-1})) \times K((x^{-1})) & \longrightarrow & \mathbb{R}_0^+ \\ (S,T) & \longmapsto & |S-T| \end{array} \right.$$

eine Metrik auf $K((x^{-1}))$.

Damit haben wir auf $K((x^{-1}))$ eine topologische Struktur und können insbesondere Konvergenz betrachten.

Der metrische Raum $(K((x^{-1})), d)$ hat eine Reihe von interessanten Eigenschaften, die wir zwar im folgenden nicht benötigen werden, die aber trotzdem der Vollständigkeit halber angegeben werden sollen. Die Beweise dieser Eigenschaften sind einfach und sollen deshalb entfallen.

Satz 1.1.6

1. *$(K((x^{-1})), d)$ ist ein vollständiger metrischer Raum.*
2. (a) *Sei $(A_n)_{n\geq 1}, A_n \in K((x^{-1})) \forall n$. Dann gilt*

   $$\sum_{n=1}^{\infty} A_n \quad \textit{konvergiert} \quad \Longleftrightarrow \quad A_n \longrightarrow 0.$$

   (b) *Jede konvergente Reihe konvergiert auch unbedingt, d.h. jede Umordnung konvergiert ebenfalls und zwar gegen den gleichen Wert.*

   (c) *Für das Produkt von konvergenten Reihen gilt die Cauchysche Produktregel.*
3. *$(K((x^{-1})), d)$ ist die Vervollständigung von $(K(x), d|_{K(x)\times K(x)})$.*

1.2 Endliche Kettenbrüche

Wir übertragen nun die klassische Kettenbruchtheorie auf den Körper der formalen Laurentreihen. Analogien zu den klassischen Resultaten werden dabei sehr schnell sichtbar.

In den Bezeichnungen schließen wir an den vorhergehenden Abschnitt an und beginnen mit der fundamentalen Definition

Definition 1.2.1 Ein Ausdruck der Form

$$A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \ldots + \cfrac{1}{A_{n-1} + \cfrac{1}{A_n}}}}$$

mit $A_i \in K((x^{-1})), 0 \leq i \leq n$ und $|A_i| > 1, 1 \leq i \leq n$ heißt ein *endlicher Kettenbruch*. Wir schreiben den Kettenbruch oft auch kurz als $[A_0; A_1, A_2, \ldots A_n]$.

Weiters heißt n die *Länge* des endlichen Kettenbruchs und die A_i die *Teilnenner* des Kettenbruchs.

Wie in der klassischen Theorie verwenden wir die folgenden Bezeichnungen

Definition 1.2.2 $S = [A_0; A_1, A_2, \ldots, A_n]$ sei ein gegebener Kettenbruch. Dann heißt

$$S_i = [A_0; A_1, \ldots A_i] \quad 0 \leq i \leq n$$

der *i-te Anfangsabschnitt* von S und

$$R_i = [A_i; A_{i+1}, \ldots A_n] \quad 0 \leq i \leq n$$

der *i-te Endabschnitt* von S.

Sei $S = [A_0; A_1, A_2, \ldots, A_n]$ mit $n \geq 2$. Dann ist nach Definition $|A_n| > 1$ und damit auch $|A_{n-1} + \frac{1}{A_n}| > 1$.

Induktiv sieht man also, daß jedem endlichen Kettenbruch ein Wert zugeordnet werden kann. Wir wollen ihm insbesondere den Wert in einer kanonischen Bruchdarstellung zuordnen.

Definition 1.2.3 $S = [A_0; A_1, A_2, \ldots, A_n]$. Wir definieren die *kanonische Bruchdarstellung* des Wertes von S induktiv nach der Länge

$n = 0: \ S = [A_0] = \frac{A_0}{1}$,

$n \geq 1:$ Die kanonische Darstellung für $[A_1; A_2 \dots A_n]$ ist bereits definiert und sei $\frac{P}{Q}$. Dann definieren wir für Kettenbrüche der Länge n

$$S = [A_0; A_1, A_2, \dots, A_n] = [A_0; \frac{P}{Q}] = A_0 + \frac{Q}{P} = \frac{A_0 P + Q}{P}.$$

Schlussendlich definieren wir noch

Definition 1.2.4 Sei $S = [A_0; A_1, A_2, \dots, A_n]$. Dann heißt die kanonische Bruchdarstellung des i-ten Abschnittes von S

$$S_i = [A_0; A_1, \dots, A_i] =: \frac{P_i}{Q_i} \quad 0 \leq i \leq n,$$

der *i-te Näherungsbruch* von S.

Für die Zähler und Nenner der Näherungsbrüche gelten wie in der klassischen Theorie die folgenden Rekursionen

Satz 1.2.5 *Sei* $S = [A_0; A_1, A_2, \dots, A_n]$. *Für die* P_i *und* Q_i *gilt*

$$\begin{aligned} P_i &= A_i P_{i-1} + P_{i-2} \quad 2 \leq i \leq n, \\ Q_i &= A_i Q_{i-1} + Q_{i-2} \quad 2 \leq i \leq n. \end{aligned}$$

Beweis. Wir beweisen die Behauptung mittels Induktion nach der Länge des Kettenbruchs.

Die Richtigkeit für Kettenbrüche der Länge 2 ist eine einfache Rechnung.

Die Behauptung sei nun gezeigt für alle Kettenbrüche der Länge i, mit $i \geq 2$. Wir betrachten $S_{i+1} = [A_0; A_1, \dots, A_{i+1}]$. Die Näherungsbrüche für $[A_1; A_2, \dots, A_{i+1}]$ bezeichnen wir mit $\frac{P'_j}{Q'_j}, 0 \leq j \leq i$. Für diese gilt die angegebene Rekursion und es gilt weiters

$$[A_0; A_1, \dots A_{j+1}] = [A_0, \frac{P'_j}{Q'_j}] = \frac{A_0 Q'_j + P'_j}{Q'_j} \quad 0 \leq j \leq i$$

und damit

$$\begin{aligned} P_{j+1} &= A_0 Q'_j + P'_j \\ Q_{j+1} &= Q'_j \end{aligned}$$

für $0 \leq j \leq i$. Schlussendlich erhalten wir

$$\begin{aligned}
P_{i+1} &= A_0 P'_i + Q'_i = \\
&= A_0(A_{i+1}P'_{i-1} + P'_{i-2}) + A_{i+1}Q'_{i-1} + Q'_{i-2} = \\
&= A_{i+1}(A_0 P'_{i-1} + Q'_{i-1}) + A_0 P'_{i-2} + Q'_{i-2} = \\
&= A_{i+1}P_i + P_{i-1},
\end{aligned}$$

sowie

$$Q_{i+1} = Q'_i = A_{i+1}Q'_{i-1} + Q'_{i-2} = A_{i+1}Q_i + Q_{i-1},$$

womit die Rekursion auch für $i+1$ gezeigt ist. ■

Definiert man noch zusätzlich $P_{-1} := 1$ und $Q_{-1} := 0$ so bleibt die Rekursion auch für $i = 1$ richtig.

Aus diesen Rekursionsbeziehungen können wir sofort folgern

Folgerung 1.2.6 *Sei $S = [A_0; A_1, \ldots, A_n]$. Für die P_i und Q_i gilt*

$$P_i Q_{i-1} - P_{i-1}Q_i = (-1)^{i-1} \quad 0 \leq i \leq n.$$

Beweis. Zunächst für $i = 0$

$$P_0 Q_{-1} - P_{-1}Q_0 = A_0 \cdot 0 - 1 \cdot 1 = -1.$$

Für $i \geq 1$ gelten die Rekursionen für P_i und Q_i. Wenn wir diese einsetzen erhalten wir

$$P_i Q_{i-1} - P_{i-1}Q_{i-2} = -(P_{i-1}Q_{i-2} - P_{i-2}Q_{i-1})$$

und damit induktiv die Behauptung. ■

Im nächsten Satz stellen wir eine Reihe von nützlichen Beziehungen zusammen.

Satz 1.2.7 *Sei $S = [A_0; A_1, \ldots, A_n]$. Dann gilt*

1. $|Q_0| < |Q_1| < \ldots < |Q_n|$,
2. $|Q_i| = |A_i Q_{i-1}| \quad 1 \leq i \leq n$,
3. $|Q_i| = \prod_{j=1}^{i} |A_j| \geq b^i \quad 0 \leq i \leq n$,
4. $|R_i| = |A_i| \quad 1 \leq i \leq n$,
5. $S = \frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}} \quad 0 \leq i < n$.

Beweis.

Zu (1) und (2): Wir zeigen die Behauptungen induktiv.
Zunächst für $i = 1$

$$|Q_1| = |A_1 Q_0 + Q_{-1}| = |A_1 Q_0| > |Q_0|.$$

Die Behauptung sei richtig für $i \geq 1$. Dann bekommen wir für $i+1$

$$|Q_{i+1}| = |A_{i+1} Q_i + Q_{i-1}|$$

und aufgrund der Gültigkeit für i

$$|A_{i+1} Q_i| > |Q_i| > |Q_{i-1}|$$

und damit

$$|Q_{i+1}| = |A_{i+1} Q_i| > |Q_i|.$$

Zu (3): Die Gleichheit ist eine unmittelbare Folge von (2) und die Ungleichung folgt aus der Tatsache, dass $|A_i| \geq b \quad \forall i \geq 1$. Weiters ist für $i = 0$ die Aussage trivial.

Zu (4): Wieder induktiv. Für $i = n$ ist die Aussage trivial.
Die Aussage sei bis $i + 1$ bewiesen. Dann gilt für i

$$|R_i| = \left| A_i + \frac{1}{R_{i+1}} \right|$$

und wegen

$$|R_{i+1}| = |A_{i+1}| > 1$$

folgt die Behauptung.

Zu (5): Die Behauptung folgt sofort aus der folgenden Umformung

$$S = [A_0; A_1, \ldots, A_n] = [A_0; \ldots, A_i, R_{i+1}]$$

und der Berechnung des $i+1$-ten Näherungsbruches für den rechten Kettenbruch, der mit S übereinstimmt. ■

Abschließend folgen noch einige Abschätzungen des Abstandes zwischen Näherungsbrüchen und dem Wert eines Kettenbruchs.

Satz 1.2.8 *Sei $S = [A_0; A_1, A_2, \ldots, A_n]$. Dann gilt*

1. $\left| S - \frac{P_i}{Q_i} \right| = \frac{1}{|Q_i Q_{i+1}|} \quad 0 \leq i < n,$

2. $\left| S - \frac{P_i}{Q_i} \right| < \frac{1}{|Q_i|^2} \quad 0 \leq i \leq n.$

Beweis.

Zu (1): Wir verwenden 1.2.7 (5) sowie 1.2.6

$$\left| S - \frac{P_i}{Q_i} \right| = \left| \frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}} - \frac{P_i}{Q_i} \right| = \frac{1}{|(R_{i+1}Q_i + Q_{i-1})Q_i|}.$$

Nun gilt wegen 1.2.7 (2) und (4)

$$|R_{i+1}Q_i| = |R_{i+1}||Q_i| = |A_{i+1}||Q_i| = |Q_{i+1}| > |Q_{i-1}|,$$

also

$$|R_{i+1}Q_i + Q_{i-1}| = |Q_{i+1}|$$

und damit die Behauptung.

Zu (2): Für $0 \leq i < n$ folgt die Behauptung aus (1) und 1.2.7 (1) und für $i = n$ ist die Behautpung trivial. ■

1.3 Kettenbrüche und Euklidischer Algorithmus

Ausgangspunkt für unsere weiteren Betrachtungen ist die folgende Überlegung.

Seien $A, B \in K[x], B \neq 0$ zwei Polynome. Da $K[x]$ ein euklidischer Ring ist können wir den euklidischen Algorithmus anwenden und erhalten

$$R_i = A_{i+1}R_{i+1} + R_{i+2} \quad -1 \leq i \leq n-1,$$

wobei $R_{-1} = A$ und $R_0 = B$ gesetzt wurde. Für die Reste gilt

$$0 = |R_{n+1}| < |R_n| < \ldots < |R_1| < |R_0| = |B|.$$

Damit erhalten wir

$$\frac{A}{B} = \frac{R_{-1}}{R_0} = A_0 + \frac{R_1}{R_0} = A_0 + \frac{1}{\frac{R_0}{R_1}}$$

und wenn wir so fortfahren

$$\frac{A}{B} = [A_0; A_1, \ldots, A_n],$$

wobei, wegen der absteigenden Ungleichungskette für die Reste, $|A_i| > 1, \forall i \geq 1$ gilt.

Mit Hilfe des euklidischen Algorithmus erhalten wir also für jedes rationale Element in $K((x^{-1}))$ eine Kettenbruchentwicklung mit Polynome als Teilnenner. Diesen endlichen Kettenbrüchen wollen wir einen speziellen Namen geben.

Definition 1.3.1 Ein endlicher Kettenbruch $[A_0; A_1, \ldots, A_n]$ mit $A_i \in K[x], \forall i$ heißt *regulär.*

Reguläre Kettenbrüche besitzen natürlich rationale Elemente von $K((x^{-1}))$ als Werte. Weiters erfasst man mit den regulären Kettenbrüchen, wie wir schon gesehen haben, alle rationalen Elemente. Man erfasst sogar alle Elemente genau einmal. Bevor wir diesen Sachverhalt zeigen, wollen wir noch eine nützliche Bezeichnung einführen.

Definition 1.3.2 Sei $S \in K((x^{-1}))$ mit $S = \sum_{i=n}^{\infty} a_i x^{-i}$. Dann heißt

$$E(S) = \sum_{i=n}^{0} a_i x^{-i}$$

der *polynomiale Anteil* von S.

Klarerweise gilt die folgende Aussage

Hilfssatz 1.3.3 *Sei $S \in K((x^{-1}))$ und $A \in K[x]$. Dann gilt*

$$|S - A| < 1 \Longrightarrow A = E(S).$$

Nun zeigen wir das schon erwähnte Resultat.

Satz 1.3.4 *Jedes Element aus $K(x)$ besitzt genau eine reguläre Kettenbruchentwicklung.*

Beweis. Die Existenz einer regulären Kettenbruchentwicklung wurde schon gezeigt. Bleibt also noch der Beweis der Eindeutigkeit.

Sei $S \in K(x)$ und $S = [A_0; A_1, \ldots, A_n]$ eine reguläre Kettenbruchentwicklung.
Zunächst gilt

$$|S - A_0| = \frac{1}{|R_1|} = \frac{1}{|A_1|} < 1$$

und damit nach 1.3.3, dass $A_0 = E(S)$.
Wir bezeichnen mit $B_0 = S - E(S)$ und erhalten $R_1 = B_0^{-1}$. Da $R_1 = [A_1; A_2, \ldots, A_n]$ bekommen wir auf analoge Art und Weise $A_1 = E(R_1) = E(B_0^{-1})$.
Dann bezeichnen wir mit $B_1 = B_0^{-1} - E(B_0^{-1})$ und es gilt $R_2 = B_1^{-1}$ usw.

Zusammenfassend erhalten wir

$$\begin{array}{lll} A_0 = E(S) & B_0 = S - E(S), & \\ A_i = E(B_{i-1}^{-1}) & B_i = B_{i-1}^{-1} - E(B_{i-1}^{-1}) & 1 \leq i \leq n, \end{array}$$

und damit sind die Teilnenner durch S eindeutig bestimmt. ■

Dieser Beweis liefert noch ein zweites Verfahren für die Berechnung der regulären Kettenbruchentwicklung von $S \in K(x)$. Man berechnet solange die A_i und B_i nach dem im Beweis erwähnten Verfahren, bis man zu einem B_i kommt dessen Wert 0 ist. Dies passiert für rationale Elemente stets.

Im Gegensatz zum Verfahren mit dem Euklidischen Algorithmus kann dieses Verfahren auch für irrationale Elemente $S \in K((x^{-1}))$ angewendet werden. Dort bricht der Algorithmus natürlich nicht ab, weil man sonst für S eine reguläre Kettenbruchentwicklung hätte. Wir werden, um auch für irrationale S eine eindeutige Kettenbruchentwicklung zu erhalten, unendliche Kettenbrüche betrachen müssen.

Ab diesem Abschnitt meinen wir mit dem Wort Kettenbrüche, wenn nicht anders erwähnt, stets reguläre Kettenbrüche.

1.4 Unendliche Kettenbrüche

Wie in der klassischen Theorie definieren wir

Definition 1.4.1 Ein Ausdruck der Form

$$A_0 + \cfrac{1}{A_1 + \cfrac{1}{A_2 + \ldots + \cfrac{1}{A_i + \ldots}}}$$

mit $A_i \in K[x], \forall i$ und $|A_i| > 1, i \geq 1$ heißt ein *unendlicher (regulärer) Kettenbruch*. Wie bei den endlichen Kettenbrüchen schreiben wir ihn kurz in der Form $[A_0; A_1, A_2, \ldots]$.
Weiters bezeichnen wir auch hier die A_i als *Teilnenner* des Kettenbruchs.

Die Definitionen 1.2.2 und 1.2.4 können wir wörtlich auf die unendlichen Kettenbrüche übertragen.
Damit erhält man insbesondere für einen unendlichen Kettenbruch zwei Folgen, nämlich die Folgen der P_i und Q_i, die die Rekursionsbeziehungen aus Satz 1.2.5 sowie die Beziehung aus der Folgerung 1.2.6 erfüllen.
Weiters bleiben klarerweise auch die Punkte (1),(2) und (3) aus Satz 1.2.7, natürlich ohne die Einschränkung $i \leq n$, richtig.

Als nächsten Punkt wollen wir auch den unendlichen Kettenbrüchen einen Wert zuordnen.

Definition 1.4.2 Sei $[A_0; A_1, A_2, \ldots]$ ein unendlicher Kettenbruch. Wir nennen ihn *konvergent* und S seinen *Wert*, wenn gilt

$$\frac{P_i}{Q_i} \longrightarrow S \quad \text{für} \quad i \longrightarrow \infty.$$

Wie in der Theorie der Reihen schreiben wir kurz $S = [A_0; A_1, A_2, \ldots]$.

Die Frage, welche unendlichen Kettenbrüche konvergieren, beantwortet der nächste Satz.

Satz 1.4.3 *Jeder unendliche Kettenbruch ist konvergent.*

Beweis. Sei $[A_0; A_1, A_2, \ldots]$ ein unendlicher Kettenbruch. Wir betrachten die Konvergenz der folgenden Reihe

$$\sum_{k=1}^{\infty} \left(\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right).$$

Wegen Folgerung 1.2.6 und Satz 1.2.7 (3) gilt für alle $k \geq 1$

$$\left| \frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right| = \frac{1}{|Q_k||Q_{k-1}|} \leq b^{-(2k-1)} \longrightarrow 0 \quad \text{für} \quad i \longrightarrow \infty$$

und damit wegen Satz 1.1.6 die Konvergenz der betrachteten Reihe. Daher gilt

$$\sum_{k=1}^{i} \left(\frac{P_k}{Q_k} - \frac{P_{k-1}}{Q_{k-1}} \right) = \frac{P_i}{Q_i} - \frac{P_0}{Q_0} \quad \text{konvergiert für} \quad i \longrightarrow \infty$$

und damit konvergiert auch die Folge der Näherungsbrüche, also auch der unendliche Kettenbruch. ■

Insbesondere besitzen damit auch alle Endabschnitte eines unendlichen Kettenbruchs einen Wert. Wir können jetzt auch die restlichen Aussagen von Satz 1.2.7 auf unendliche Kettenbrüche übertragen.

Satz 1.4.4 *Sei $S = [A_0; A_1, A_2, \ldots]$. Dann gilt*

1. $|R_i| = |A_i| \quad i \geq 1,$
2. $S = \frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}} \quad i \geq 0,$
3. $S = [A_0; A_1, \ldots, A_{i-1}, R_i] \quad i \geq 0.$

Beweis.

Zu (1): Wir bezeichnen für $i \geq 1$ und $R_i = [A_i; A_{i+1}, \ldots]$ mit P'_j bzw. Q'_j den Zähler bzw. Nenner des j-ten Näherungsbruches. Es gilt für alle $j \geq 0$

$$\frac{P'_j}{Q'_j} \quad \text{ist Endabschnitt von} \quad [A_0; A_1, \ldots, A_i, \ldots, A_{i+j}]$$

und damit wegen 1.2.7 (4)

$$\left| \frac{P'_j}{Q'_j} \right| = |A_i| \quad j \geq 0.$$

Jetzt gilt aufgrund der Definition von R_i

$$\frac{P'_j}{Q'_j} \longrightarrow R_i \quad \Longrightarrow |A_i| = \left| \frac{P'_j}{Q'_j} \right| \longrightarrow |R_i|$$

und damit die Behauptung.

Zu (2): Wie oben bezeichnen wir für $i \geq 0$ und $R_{i+1} = [A_{i+1}; A_{i+2}, \ldots]$ mit P'_j bzw. Q'_j den Zähler bzw. Nenner des j-ten Näherungsbruches. Es gilt

$$\begin{aligned} \frac{P_{j+i}}{Q_{j+i}} &= [A_0; A_1, \ldots, A_i, A_{i+1}, \ldots, A_{i+j}] = \\ &= [A_0; A_1, \ldots, A_i, \frac{P'_{j-1}}{Q'_{j-1}}] = \\ &= \frac{P_i \frac{P'_{j-1}}{Q'_{j-1}} + P_{i-1}}{Q_i \frac{P'_{j-1}}{Q'_{j-1}} + Q_{i-1}} \end{aligned}$$

für alle $j \geq 1$. Wegen 1.2.7 (1) und (1) gilt

$$\frac{|Q_{i-1}|}{|Q_i|} < 1 \quad \text{und} \quad |R_{i+1}| = |A_{i+1}| > 1,$$

wobei der Fall $i = 0$ bei der ersten Aussage trivial ist. Deshalb konvergiert, wenn wir im obigen Bruch $j \longrightarrow \infty$ gehen lassen, der Nenner nicht gegen Null und damit bekommen wir im Grenzübergang die Behauptung.

Zu (3): Für $i = 0$ ist die Aussage trivial. Für $i > 0$ ist sie eine unmittelbare Folgerung von (2). ∎

Damit können wir auch den Satz 1.2.8, natürlich ohne Einschränkung von i nach oben, für unendliche Kettenbrüche wortwörtlich übernehmen.

Jetzt kommen wir zum Hauptergebnis dieses Abschnittes.

Satz 1.4.5. *Der Wert eines unendlichen Kettenbruchs ist stets irrational. Umgekehrt tritt jedes irrationale Element als Wert genau eines unendlichen Kettenbruchs auf.*

Beweis. Es sei $S = [A_0; A_1, A_2, \ldots]$. Zunächst können wir wie im Beweis von Satz 1.3.4 folgern, dass $A_0 = E(S)$ ist. Von der dortigen Vorgehensweise motiviert definieren wir

$$B_0 = S - E(S) \quad \text{und} \quad B_i = B_{i-1}^{-1} - E(B_{i-1}^{-1})$$

für alle $i \geq 1$, für die das möglich ist. Wir zeigen induktiv, dass diese Definition für alle i funktioniert, wobei wir uns im i-ten Schritt der Induktion davon überzeugen, dass $B_{i-1} \neq 0$ ist und dass für R_i und A_i gilt

$$R_i = B_{i-1}^{-1} \quad \text{und} \quad A_i = E(B_{i-1}^{-1}) \quad i \geq 1.$$

Der erste Schritt der Induktion folgt wie im Beweis von Satz 1.3.4. Sei also der i-te Schritt gezeigt, dann gilt nach Satz 1.4.4 (3)

$$R_i = [A_i; R_{i+1}] = A_i + \frac{1}{R_{i+1}}$$

und damit nach Induktionsvoraussetzung

$$\frac{1}{R_{i+1}} = R_i - A_i = B_{i-1}^{-1} - E(B_{i-1}^{-1}) = B_i \neq 0.$$

Weiters folgt draus $R_{i+1} = B_i^{-1}$ und weiters wie üblich

$$|R_{i+1} - A_{i+1}| < \frac{1}{|R_{i+2}|} = \frac{1}{|A_{i+2}|} < 1$$

und mit Hilfssatz 1.3.3

$$A_{i+1} = E(R_{i+1}) = E(B_i^{-1}),$$

wie es behauptet war.

Diese Methode aus S auf die A_i zu schließen ist genau die zweite Methode zur Gewinnung der Kettenbruchentwicklung eines rationalen S. Da hier die Methode nicht abbricht, kann S nicht rational sein. Damit ist der Wert eines unendlichen Kettenbruchs irrational.

Weiters erkennen wir aus dem obigen Beweis, dass ein irrationales Element nur Wert von höchstens einem unendlichen Kettenbruch sein kann. Bleibt also noch die Existenz für ein beliebiges irrationales Element S zu zeigen.

Dazu definieren wir die A_i mit dem obigen Algorithmus. Wie schon früher erwähnt kann er klarerweise nicht abbrechen. Wie üblich bezeichnen wir Zähler bzw. Nenner der Näherungsbrüche von $[A_0; A_1, A_2, \ldots]$ mit P_i bzw Q_i. Aufgrund der Definition der A_i gilt

$$S = [A_0; A_1, \ldots, A_i, B_i^{-1}] \quad i \geq 0$$

und damit wegen Satz 1.2.7 (5) und Folgerung 1.2.6

$$\left| S - \frac{P_i}{Q_i} \right| = \left| \frac{B_i^{-1} P_i + P_{i-1}}{B_i^{-1} Q_i + Q_{i-1}} - \frac{P_i}{Q_i} \right| = \frac{1}{|B_i^{-1} Q_i + Q_{i-1}||Q_i|}$$

für alle $i \geq 0$. Da aber $|B_i^{-1}| > 1$ folgt aus Satz 1.2.7 (1)

$$|B_i^{-1} Q_i| > |Q_i| > |Q_{i-}|$$

und damit mit Satz 1.2.7 (2)

$$|B_i^{-1} Q_i + Q_{i-1}| = |B_i^{-1} Q_i| = |A_{i+1} Q_i| = |Q_{i+1}| > |Q_i|.$$

Damit können wir in obiger Ungleichung weiter abschätzen und erhalten

$$\left| S - \frac{P_i}{Q_i} \right| < \frac{1}{|Q_i|^2}$$

und damit mit $|Q_i| \longrightarrow \infty$ wegen Satz 1.2.7 (1), dass tatsächlich $S = [A_0; A_1, A_2, \ldots]$ gilt. ■

Wenn wir unter Kettenbrüchen die regulären endlichen Kettenbrüche aus dem vorigen Abschnitt und die unendlichen Kettenbrüche aus diesem Abschnitt verstehen, dann lassen sich die Ergebnisse folgendermaßen zusammenfassen. Man beachte insbesondere dabei die starke Analogie zum klassischen Resultat (siehe etwa [6] Satz 14).

Satz 1.4.6 *Jedes S aus $K((x^{-1}))$ tritt als Wert von genau einem Kettenbruch auf (die sogenannte Kettenbruchentwicklung von S). Diesen Kettenbruch erhält man durch das folgende Verfahren*

$$\begin{array}{ll} A_0 = E(S) & B_0 = S - E(S) \\ A_i = E(B_{i-1}^{-1}) & B_i = B_{i-1}^{-1} - E(B_{i-1}^{-1}) \end{array}$$

wobei man es solange ausfürt bis $B_i = 0$ ist. Weiters besitzen genau die rationalen Elemente eine endliche Kettenbruchentwicklung.

Wie in der klassischen Theorie wird der obige Algorithmus *Kettenbruchalgorithmus* genannt.

1.5 Näherungsbrüche als Bestapproximierende

Ein wichtiger Punkt in der klassischen Theorie der Kettenbrüche war, dass sich die Näherungsbrüche als Bestapproximierende, in einem bestimmten Sinn, interpretieren liessen (siehe [6] §6). Dieses Ergebnis können wir auch hier wiederfinden.

Wir beginnen mit der folgenden Definition

Definition 1.5.1 Sei $S \in K((x^{-1}))$ und $P, Q \in K[x], Q \neq 0$. Dann heißt $\frac{P}{Q}$ *Bestapproximierende* von S wenn für alle $P', Q' \in K[x]$ mit $1 \leq |Q'| \leq |Q|$ gilt

$$|Q'S - P'| \geq |QS - P|.$$

Man beachte, dass es bei dieser Definition nicht nur auf das rationale Element, sondern auch auf die entsprechende Bruchdarstellung ankommt.

Als unmittelbare Folgerung aus der Definition erhalten wir

Hilfssatz 1.5.2 *Sei $S \in K((x^{-1}))$ und $\frac{P}{Q}$ Bestapproximierende von S, dann gilt*

1. *P und Q sind relativ prim, also $(P, Q) = 1$.*
2. *$\frac{aP}{aQ}$ mit $a \in K \backslash \{0\}$ ist ebenfalls Bestapproximierende von S.*

Wir benötigen noch ein einfaches Hilfsergebnis.

Hilfssatz 1.5.3 *Sei $S \in K((x^{-1}))$ sowie $P, Q \in K[x], Q \neq 0$ und $(P, Q) = 1$. Gilt nun*

$$\left| S - \frac{P}{Q} \right| < \frac{1}{|Q|^2},$$

dann ist $\frac{P}{Q}$ Bestapproximierende von S.

Insbesondere gilt für alle $P', Q' \in K[x]$ mit $1 \leq |Q'| \leq |Q|$ und $\frac{P}{Q} \neq \frac{P'}{Q'}$

$$|Q'S - P'| > |QS - P|.$$

Beweis. Sei $P', Q' \in K[x]$ und $1 \leq |Q'| \leq |Q|$. Wir unterscheiden zwei Fälle

$\frac{P'}{Q'} = \frac{P}{Q}$: Da der zweite Bruch gekürzt vorliegt und Q' der obigen Bedingung unterworfen ist folgt, dass $P' = aP$ und $Q' = aQ$ mit $a \in K \backslash \{0\}$. Damit gilt

$$|Q'S - P'| = |a||QS - P| = |QS - P|.$$

$\frac{P'}{Q'} \neq \frac{P}{Q}$: Zunächst gilt

$$\left|\frac{P}{Q} - \frac{P'}{Q'}\right| \geq \frac{1}{|QQ'|} \geq \frac{1}{|Q|^2}$$

und damit mit der vorausgesetzten Ungleichung

$$\left|S - \frac{P'}{Q'}\right| = \left|S - \frac{P}{Q} + \frac{P}{Q} - \frac{P'}{Q'}\right| = \left|\frac{P}{Q} - \frac{P'}{Q'}\right| \geq \frac{1}{|Q||Q'|}.$$

Multiplikation mit $|Q'|$ ergibt schließlich

$$|Q'S - P'| \geq \frac{1}{|Q|} > |QS - P|.$$

Insbesondere folgt der Zusatz aus dem zweiten Teil. ■

Damit können wir nun das Hauptergebnis dieses Abschnittes zeigen. Dieses geht auf deMathan [10] zurück.

Satz 1.5.4 *Sei $S \in K((x^{-1}))$. Dann sind alle Bestapproximierenden von S gegeben durch*

$$\frac{aP_i}{aQ_i} \quad a \in K\backslash\{0\}, i \geq 0,$$

wobei P_i und Q_i die Zähler und Nenner der Näherungsbrüche bezeichnen.

Beweis. Da es sich bei den P_i und Q_i um Polynome handelt, die die Beziehung in Folgerung 1.2.7 erfüllen, folgt, dass $(P_i, Q_i) = 1$ ist. Aus dem Satz 1.2.8 (2) und dem entsprechenden Resultat für unendliche Kettenbrüche, sowie dem Hilfssatz 1.5.3 folgt, dass $\frac{P_i}{Q_i}$ Bestapproximierende von S ist. Damit sind nach Satz 1.5.2 alle oben angegebenen Brüche tatsächlich Bestapproximierende.

Bleibt also nur mehr zu zeigen, dass es keine weiteren gibt. Angenommen es gibt also einen bestapproximierenden Bruch $\frac{P}{Q}$ von S, der nicht in der obigen Menge enthalten ist. Da $(P, Q) = 1$ ist, muss $\frac{P}{Q} \neq \frac{P_i}{Q_i}, \forall i$ sein. Damit kann es nach dem Zusatz von Hilfssatz 1.5.3 kein i geben, sodass $|Q_i| = |Q|$ ist. Wir unterscheiden zwei Fälle

Fall 1: $\exists i: \quad |Q_i| < |Q| < |Q_{i+1}|$. Es existieren $C, D \in K[x], C \neq 0, D \neq 0$ und $(C, D) = 1$ mit

$$\frac{P}{Q} = \frac{CP_i + DP_{i-1}}{CQ_i + DQ_{i-1}},$$

wobei die Bedingungen $C \neq 0, D \neq 0$ sowie $(C, D) = 1$ trival erreichbar sind, falls die Existenz einer solchen Darstellung gezeigt ist. Von der Existenz überzeugt man sich dadurch, dass zunächst für $i = 1$ eine solche Darstellung in trivialer Weise erreichbar ist. Dann muss man nur mehr die entsprechenden Rekursionsbeziehungen für die Q_i und P_i aus Satz 1.2.5 verwenden.

Mit dieser Darstellung gilt

$$\begin{aligned}
Q_i(CP_i + DP_{i-1}) - P_i(CQ_i + DQ_{i-1}) &= (-1)^i D \\
Q_{i-1}(CP_i + DP_{i-1}) - P_{i-1}(CQ_i + DQ_{i-1}) &= (-1)^{i-1} C
\end{aligned}$$

und damit $(CP_i + DP_{i-1}, CQ_i + DQ_{i-1}) = 1$. Multipliziert man C und D mit einem geeigneten $a \in K\backslash\{0\}$ dann erhält man also

$$\begin{aligned}
P &= CP_i + DP_{i-1}, \\
Q &= CQ_i + DQ_{i-1}.
\end{aligned}$$

Aus Satz 1.2.7 (5) bzw. Satz 1.4.4 (2) folgt

$$S = \frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}},$$

und damit

$$\begin{aligned}
|QS - P| &= \left| Q\frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}} - S \right| = \\
&= \frac{|R_{i+1}(QP_i - PQ_i) - (PQ_{i-1} - QP_{i-1})|}{|R_{i+1}Q_i + Q_{i-1}|}.
\end{aligned}$$

Unter Verwendung der obigen Formeln für P und Q erhält man

$$|QS - P| = \frac{|DR_{i+1} - C|}{|Q_{i+1}|}.$$

Wegen Satz 1.2.8 (1) gilt

$$|Q_iS - P_i| = \frac{1}{|Q_{i+1}|}$$

und wegen der Voraussetzung, dass $\frac{P}{Q}$ Bestapproximierende ist

$$|QS - P| \leq |Q_iS - P_i|.$$

Durch Einsetzen in das obige Ergebnis bekommt man

$$|DR_{i+1} - C| \leq 1$$

woraus wegen

$$|R_{i+1}| > 1 \quad \text{und} \quad |D| \geq 1, |C| \geq 1$$

folgt

$$|C| = |D||R_{i+1}|$$

und damit

$$|C| > |D| \quad \text{und} \quad |C| \geq |R_{i+1}| = |A_{i+1}|.$$

Weiters können wir folgern

$$|CQ_i| > |DQ_i| > |DQ_{i-1}|$$

und abschließend

$$|Q| = |CQ_i + DQ_{i-1}| = |CQ_i| \geq |A_{i+1}Q_i| = |Q_{i+1}|,$$

was ein Widerspruch ist.

Fall 2: Die Kettenbruchentwicklung ist endlich mit der Länge n und $|Q| > |Q_n|$. Dann ist aber $S = \frac{P_n}{Q_n}$ und daher

$$0 = |Q_n S - P_n| \geq |QS - P|$$

also $|QS - P| = 0$. Daraus folgt

$$S = \frac{P}{Q} = \frac{P_n}{Q_n},$$

was wieder ein Widerspruch ist. ■

1.6 Äquivalente Kettenbruchentwicklungen

In Analogie zur klassischen Theorie definieren wir (siehe etwa [18])

Definition 1.6.1 Seien $S, S' \in K((x^{-1}))$ zwei irrationale Elemente mit Kettenbruchentwicklung $S = [A_0; A_1, A_2, \ldots]$ bzw. $S' = [A'_0; A'_1, A'_2, \ldots]$. Wie üblich bezeichnen wir den Wert des i-ten Endabschnittes von S bzw. S' mit R_i bzw. R'_i. Dann sagen wir S und S' besitzen *äquivalente Kettenbruchentwicklungen*, wenn es $i, j \in \mathbb{N} \cup \{0\}$ und $a \in K \backslash \{0\}$ gibt, mit $R_i = aR'_j$.

Bei der so erhaltenen Relation auf der Menge der irrationalen Elemente von $K((x^{-1}))$ handelt es sich, wie man sofort feststellt, um eine Äquivalenzrelation.

Wir wollen noch eine weiter Äquivalenzrelation auf der Menge der irrationalen Elemente definieren.

Definition 1.6.2 Seien $S, S' \in K((x^{-1}))$ zwei irrationale Elemente. Wir nennen S und S' *äquivalent* - in Zeichen $S \sim S'$ - wenn es $A, B, C, D \in K[x]$ gibt mit $AD - BC \in K \backslash \{0\}$, sodass gilt

$$S = \frac{AS' + B}{CS' + D}.$$

Wie man auch hier leicht sieht, handelt es sich wirklich um eine Äquivalenzrelation.

Ziel ist es nun zu zeigen, dass diese beiden Äuqivalenzrelationen identisch sind.

Satz 1.6.3 *Seien $S, S' \in K((x^{-1}))$ zwei irrationale Elemente. Dann gilt*

$$S und S' besitzen\ äquivalente\ Kettenbruchentwicklungen \iff S \sim S'.$$

Beweis. Wir wollen mit R_i bzw R'_i die Werte der i-ten Restabschnitte, sowie mit P_i, Q_i bzw P'_i, Q'_i die Nenner und Zähler der Näherungsbrüche von S bzw S' bezeichnen.

$\Longrightarrow$: Wegen Satz 1.4.4 (2) sowie Folgerung 1.2.7 gilt $S \sim R_i$ und $S' \sim R'_i$ für alle $i \geq 0$. Nach Voraussetzung gibt es ein $i, j \in \mathbb{N} \cup \{0\}$ mit $R_i \sim R'_j$ woraus $S \sim S'$ aufgrund der Symmetrie und Transitivität von $\sim$ folgt.

$\Longleftarrow$: Nach Definition von $S \sim S'$ gibt es $A, B, C, D \in K[x]$ mit $AD - BC \in K \backslash \{0\}$ und

$$S' = \frac{AS + B}{CS + D}.$$

Zunächst setzen wir voraus, dass $|S| > 1$ und $|C| > |D| > 0$ ist. Dann gilt

$$\begin{aligned} \left| S' - \frac{A}{C} \right| &= \left| \frac{AS + B}{CS + D} - \frac{A}{C} \right| = \\ &= \frac{|BC - AD|}{|C||CS + D|} = \\ &= \frac{1}{|C||CS + D|} \end{aligned}$$

und mit

$$|CS| > |C| > |D|$$

erhalten wir

$$\left| S' - \frac{A}{C} \right| = \frac{1}{|C||CS + D|} = \frac{1}{|C||CS|} < \frac{1}{|C|^2}.$$

Eine analoge Rechung ergibt

$$\left| S' - \frac{B}{D} \right| = \frac{|S|}{|D||CS + D|} = \frac{1}{|C||D|} < \frac{1}{|D|^2}.$$

Wegen $AD - BC \in K\backslash\{0\}$ gilt $(A,C) = 1$ und $(B,D) = 1$. Damit folgt aus Hilfssatz 1.5.3, dass sowohl $\frac{A}{C}$ als auch $\frac{B}{D}$ Bestapproximierende von S' sind.

Aus Satz 1.5.4 erhalten wir also, dass es ein $i \geq 0$ mit $\frac{B}{D} = \frac{P_i'}{Q_i'}$ gibt. Auch $\frac{A}{C}$ muss mit einer der Näherungsbrüche von S' übereinstimmen.

Es gilt nun, nach der Verallgemeinerung von Satz 1.2.8 (2) auf den Fall unendlicher Kettenbrüche,

$$|DS' - B| = \frac{1}{|Q_{i+1}'|}$$

und nach der vorigen Berechnung

$$|DS' - B| = \frac{1}{|C|},$$

was $|C| = |Q_{i+1}'|$ zur Folge hat. Damit ist $\frac{A}{C} = \frac{P_{i+1}'}{Q_{i+1}'}$.

Also stimmt $\frac{B}{D}$ mit dem i-ten und $\frac{A}{C}$ mit dem $i+1$-ten Näherungsbruch von S' überein. Weil beide Brüche gekürzt sind gibt es $a, b \in K\backslash\{0\}$ mit

$$\begin{array}{ll} B = aP_i' & D = aQ_i' \\ A = bP_{i+1}' & C = bQ_{i+1}'. \end{array}$$

Aufgrund von Satz 1.4.4 (2) sowie der Beziehnung zwischen S' und S gilt

$$S' = \frac{R_{i+2}'P_{i+1}' + P_i'}{R_{i+2}'Q_{i+1}' + Q_i'} = \frac{\frac{b}{a}SP_{i+1}' + P_i'}{\frac{b}{a}SQ_{i+1}' + Q_i'}$$

und nach einfacher Rechnung $R_{i+2}' = \frac{b}{a}S$. Also besitzen S und S' äquivalente Kettenbruchentwicklungen und damit ist die Behauptung für diesen Fall bewiesen.

Jede andere Situation wollen wir auf den vorigen Fall zurückführen. Dazu betrachten wir nach Satz 1.4.4 (2)

$$S = \frac{R_{i+1}P_i + P_{i-1}}{R_{i+1}Q_i + Q_{i-1}}$$

und setzen in die Beziehung zwischen S und S' ein. Nach einfacher Rechnung erhalten wir

$$S' = \frac{(AP_i + PQ_i)R_{i+1} + AP_{i-1} + BQ_{i-1}}{(CP_i + DQ_i)R_{i+1} + CP_{i-1} + DQ_{i-1}},$$

wobei wir folgende Bezeichnungen einführen

$$\begin{array}{ll} A' = AP_i + PQ_i & B' = AP_{i-1} + BQ_{i-1}, \\ C' = CP_i + DQ_i & D' = CP_{i-1} + DQ_{i-1}. \end{array}$$

Eine leichte Rechnung zeigt $A'D' - B'C' \in K\backslash\{0\}$ und damit $S' \sim R_{i+1}$. Für ausreichend großes i gilt

$$\begin{aligned} |C'| &= |CP_i + DQ_i| = |Q_i||CS + D| > 0, \\ |D'| &= |CP_{i-1} + DQ_{i-1}| = |Q_{i-1}||CS + D| > 0, \\ |C'| &> |D'| > 0 \end{aligned}$$

und aus Satz 1.4.4 (1) folgt $|R_{i+1}| > 1$. Damit können wir den ersten Teil anwenden und erhalten, dass S' und R_{i+1} äquivalente Kettenbruchentwicklungen besitzen, womit auch die Behauptung für S und S' folgt. ■

1.7 Quadratische Irrationalitäten

Eines der schönsten Ergebnisse der klassischen Theorie der Kettenbrüche ist der Satz von Lagrange, der besagt, dass quadratische Irrationalitäten und nur diese eine periodische Kettenbruchentwicklung besitzen (siehe etwa [6] Satz 28). Dieses Ergebnis kann auch im Körper der formalen Laurentreihen wiedergefunden werden, wenn man voraussetzt, dass der Grundkörper K ein endlicher Körper ist.

Wir machen also bis zum Ende des Kapitels die Voraussetzung

$$K = \mathbb{F}_q \quad mit \quad q = p^n, p \in \mathbb{P}, n \in \mathbb{N}.$$

Bevor wir den Satz von Lagrange formulieren und beweisen können, benötigen wir eine Reihe von Begriffsbildungen, die in diesem Abschnitt bereitgestellt werden sollen.

Wir beginnen mit der folgenden Definition

Definition 1.7.1 Sei $S \in K((x^{-1}))$ ein algebraisches Element 2.Ordnung über $K(x)$. Dann heißt S eine *quadratische Irrationalität.*

Betrachtet man das Minimalpolynom von einer quadratischen Irrationalität S, so besitzt es in $K((x^{-1}))$ noch eine weitere Nullstelle. Diese ist stets verschieden von S denn es gilt

Satz 1.7.2 *Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität. Dann ist S separabel über $K(x)$.*

Beweis. Die zweite Nullstelle des Minimalpolynoms von S in $K((x^{-1}))$ sei $\bar{S}$. Wir nehmen indirekt an $S = \bar{S}$ und unterscheiden zwei Fälle

Char $K \neq 2$: Das Minimalpolynom von S ist

$$(X - S)(X - \bar{S}) = X^2 - 2SX + S^2$$

und damit muss $-2S \in K(x)$ sein. Das bedeutet aber $S \in K(x)$ was ein Widerspruch ist.

Char $K = 2$: Nach Voraussetzung ist in diesem Fall $K = \mathbb{F}_q$ mit $q = 2^n$. Wir berechnen wieder das Minimalpolynom von S

$$(X - S)(X - \bar{S}) = X^2 + S^2.$$

Es gilt also $S^2 \in K(x)$ und damit auch S^{2^n} in $K(x)$. Mit

$$S = \sum_{i=l}^{\infty} a_i x^{-i} \quad a_l \neq 0,$$

und der Voraussetzung erhalten wir

$$S^{2^n} = \sum_{i=l}^{\infty} a_i^{2^n} x^{-2^n i} = \sum_{i=l}^{\infty} a_i x^{-2^n i} \in K(x),$$

was natürlich $S \in K(x)$ bedeutet und damit ebenfalls einen Widerspruch darstellt. ■

Wir führen folgende Bezeichnung ein

Definition 1.7.3 Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität. Die zweite Nullstelle des Minimalpolynoms von S bezeichnen wir mit $\bar{S}$. Dann heißt $\bar{S}$ das *konjugierte Element* zu S.

Damit erhalten wir eine Abbildung, die auf der Menge der quadratischen Irrationalitäten definiert ist und jeder das konjugierte Elemten zuordnet. Diese wollen wir als *konjugierter Abbildung* bezeichnen. Außerdem erweitern wir sie für die Elemente von $K(x)$ durch $\bar{A} = A, A \in K(x)$.

Aus einem allgemeineren Satz der Körpertheorie folgt

Satz 1.7.4 *Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität. Dann ist die Abbildung*

$$f : \begin{cases} (K(x))(S) & \longrightarrow & (K(x))(\bar{S}) \\ A + BS & \longmapsto & A + B\bar{S} \end{cases}$$

ein Körperisomorphismus. Dieser stimmt mit der konjugierten Abbildung eingeschränkt auf $(K(x))(S)$ überein.

Beweis. Wir wollen uns nur den Zusatz überlegen. Zunächst folgt aus der Körpertheorie, dass $A+BS$ mit $A, B \in K(x), B \neq 0$ eine quadratische Irrationalität ist. Da f ein Isomorphismus ist, muss $f(A+BS)$ eine Nullstelle des Minimalpolynoms von $A+BS$ sein. Nun ist $f(A+BS) \neq A+BS$ und daher $f(A+BS)$ die konjugierte Nullstelle zu $A+BS$. Im Fall $B=0$ ist die Aussage trivial. ■

Für den nächsten Satz wollen wir Char $K \neq 2$ voraussetzen.

Satz 1.7.5 *Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität. Dann läßt sich S darstellen in der Form*

$$S = \frac{E+\Delta}{F} \quad \text{mit} \quad E, F \in K[x], F \neq 0 \quad \text{und} \quad \Delta^2 \in K[x].$$

Ist zusätzlich S' ein irrationales Element von $K((x^{-1}))$ mit $S' \sim S$ dann erhält man für S' die Darstellung

$$S' = \frac{E'+\Delta}{F'} \quad \text{mit} \quad E', F' \in K[x], F' \neq 0$$

mit insbesondere demselben Δ.

Beweis. Wir betrachten das Minimalpolynom von S in der Form

$$X^2 + \frac{B}{A}X + \frac{C}{A} \quad A, B, C \in K[x], A \neq 0.$$

So eine Darstellung ist natürlich immer möglich, wobei allerdings A, B und C nicht eindeutig bestimmt sind. Wir definieren $\Delta := 2AS + B$ und erhalten

$$\Delta^2 = 4A^2S^2 + 4ABS + B^2.$$

Einsetzen von S in das Minimalpolynom und umformen ergibt

$$S^2 = -\frac{B}{A}S - \frac{C}{A}.$$

Dies können wir oben einsetzen und erhalten

$$\Delta^2 = B^2 - 4AC \in K[x]$$

und damit wegen der Voraussetzung Char $K \neq 2$ und der Definition von Δ

$$S = \frac{-B+\Delta}{2A}$$

also die behauptete Darstellung.

Bleibt noch der Beweis der zweiten Aussage. Augrund der Definition von $\sim$ gibt es $A', B', C', D' \in K[x]$ mit $A'D' - B'C' \in K\backslash\{0\}$, sodass gilt

$$S' = \frac{A'S + B'}{C'S + D'}$$

und nach Einsetzen der obigen Darstellung von S, sowie einer einfachen Rechnung erhält man die zweite Aussage. ■

Wenn S eine quadratische Irrationalität ist und $S' \sim S$ gilt, dann ist auch S' eine quadratische Irrationalität. Dies folgt sofort, indem man S durch S' darstellt und in das Minimalpolynom von S einsetzt.

Der letzte Satz besagt insbesondere, dass die Äquivalenzklasse von S bezüglich $\sim$ in $(K(x))(\Delta)$ mit geeigneten Δ enthalten ist. Da die zweite Nullstelle des Minimalpolynoms von Δ durch $-\Delta$ gegeben ist, erhält man die konjugierten Elemente einfach durch vertauschen von Δ mit $-\Delta$.

Abschließend führen wir noch die folgende Bezeichnung ein, die wir im nächsten Abschnitt benötigen werden

Definition 1.7.6 Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität. Wir bezeichnen S als *speziell* wenn gilt

$$|S| > 1 \quad \text{und} \quad |\bar{S}| < 1.$$

1.8 Periodische Kettenbrüche

Unser Ziel ist, wie schon erwähnt, die Verallgemeinerung des Satzes von Lagrange auf den Körper der formalen Potenzreihen. Dazu brauchen wir zunächst den Begriff des periodischen Kettenbruchs.

Definition 1.8.1 Sei $S \in K((x^{-1}))$ ein irrationales Element mit der Kettenbruchentwicklung $S = [A_0; A_1, A_2, \ldots]$. Wir sagen S besitzt eine *periodische Kettenbruchentwicklung*, wenn es ein $n_0 \in \mathbb{N} \cup \{0\}$ und ein $k \in \mathbb{N}$ gibt, sodass gilt

$$A_{n+k} = A_n \quad \forall n \geq n_0.$$

Weiters sprechen wir von einer *rein periodischen Kettenbruchentwicklung*, wenn $n_0 = 0$ ist und sonst von einer *gemischt periodischen Kettenbruchentwicklung.*

Um unser Hauptergebnis beweisen zu können, benötigen wir eine Reihe von

Hilfsergebnissen. Diese Beweisidee stammt aus deMathan [10] geht aber im wesentlichen auf den klassischen Beweis von Artin [1] zurück.

Hilfssatz 1.8.2 *Sei $S \in K((x^{-1}))$ eine quadratische Irrationalität mit Kettenbruchentwicklung $S = [A_0; A_1, A_2, \ldots]$. Dann gibt es ein $i \in \mathbb{N}$, sodass der Wert des i-ten Restabschnittes R_i speziell ist.*

Beweis. Zunächst sind wegen $R_i \sim S$ auch alle Restabschnitte von S quadratische Irrationalitäten. Weiters gilt wegen Satz 1.4.4 (1) $|R_i| = |A_i| > 1, i \geq 1$. Aus demselben Satz, allerdings Eigenschaft (2), folgt für alle $i \geq 1$

$$S = \frac{R_i P_{i-1} + P_{i-2}}{R_i Q_{i-1} + Q_{i-2}}$$

und nach einer einfachen Umformung

$$R_i = \frac{-Q_{i-2} S + P_{i-2}}{Q_{i-1} S - P_{i-1}}.$$

Wendet man den Isomorphismus aus Satz 1.7.4 an, so erhält man

$$\bar{R_i} = \frac{-Q_{i-2}\bar{S} + P_{i-2}}{Q_{i-1}\bar{S} - P_{i-1}} = -\frac{Q_{i-2}}{Q_{i-1}} \frac{\bar{S} - \frac{P_{i-2}}{Q_{i-2}}}{\bar{S} - \frac{P_{i-1}}{Q_{i-1}}}.$$

Nun konvergiert $\frac{P_i}{Q_i} \longrightarrow S$ und aus Satz 1.7.2 folgt, dass $S \neq \bar{S}$. Also gilt für ausreichend großes i

$$\left| \bar{S} - \frac{P_{i-2}}{Q_{i-2}} \right| = \left| \bar{S} - \frac{P_{i-1}}{Q_{i-1}} \right| = |S - \bar{S}|$$

und damit

$$|\bar{R_i}| = \left| \frac{Q_{i-2}}{Q_{i-1}} \right|,$$

was wegen Satz 1.2.8 (1) $|\bar{R_i}| < 1$ und damit die Behauptung impliziert. ■

Hilfssatz 1.8.3 *Sei $S \in K((x^{-1}))$ speziell mit der Kettenbruchentwicklung $S = [A_0; A_1, A_2, \ldots]$. Dann sind auch die Werte der i-ten Restabschnitte R_i speziell.*

Beweis. Es genügt die Behauptung für R_1 zu zeigen. Da $A_0 = E(S)$ und $S = [A_0; R_1]$ ist, erhalten wir

$$R_1 = \frac{1}{S - E(S)}$$

und nach Anwendung des Isomorphismus aus Satz 1.7.4

$$\left| \frac{1}{\bar{R_1}} \right| = |\bar{S} - E(S)|.$$

Nun ist nach Voraussetzung S speziell also $|\bar{S}| < 1$ sowie $|A_0| = |E(S)| > 1$. Damit gilt weiters

$$|\bar{S} - E(S)| = |E(S)| > 1.$$

Dies bedeutet also mit der obigen Beziehung $|\bar{R}_1| < 1$ und $|R_1| > 1$ ist trivial. ■

Wir erinnern noch einmal daran, dass wenn in einer Äquivalenzklasse von $\sim$ ein Element quadratische Irrationalität ist, dann sind alle Elemente quadratische Irrationalitäten. Solche Äuquivalenzklassen wollen wir nun näher betrachten.

Hilfssatz 1.8.4 *In jeder Äquivalenzklasse von $\sim$, deren Elemente quadratischen Irrationalitäten sind, gibt es nur endlich viele spezielle Elemente.*

Beweis. Wir unterscheiden zwei Fälle

Char $K \neq 2$: Wegen Satz 1.7.5 wissen wir in diesem Fall, dass sich jedes Element der Äquivalenzklasse darstellen läßt durch

$$\frac{E+\Delta}{F} \quad \text{mit} \quad E, F \in K[x], F \neq 0 \quad \text{und} \quad \Delta^2 \in K[x].$$

Insbesondere gilt also für ein spezielles Element

$$\left|\frac{E+\Delta}{F}\right| > 1 \quad \text{und} \quad \left|\frac{E-\Delta}{F}\right| < 1$$

oder anders geschrieben

$$|E - \Delta| < |F| < |E + \Delta|.$$

Daraus folgt, dass $|E| = |\Delta|$ ist, weil andernfalls $|E - \Delta| = |E + \Delta|$ gelten würde. Insbesondere gibt es aufgrund der Endlichkeit von K nur endlich viele E mit dieser Eigenschaft und dazu wegen

$$|F| < |E + \Delta|$$

auch nur endlich viele F. Also kann es nur endlich viele spezielle Elemente in der Äquivalenzklasse geben.

Char $K = 2$: Sei S ein Element der Äquivalenzklasse. Wir schreiben das Minimalpolynom von S in der Form

$$AX^2 + BX + C \quad \text{mit} \quad A, B, C \in K[x], A \neq 0$$

und es gilt mit dem konjugierten Element zu S

$$-(S + \bar{S}) = S + \bar{S} = S - \bar{S} = \frac{B}{A},$$

was wegen der Separabilität von S, $B \neq 0$ impliziert.

Sei S' ein weiteres Element der Äquivalenzklasse. Dann gilt aufgrund der Definition von $\sim$

$$S = \frac{A'S' + B'}{C'S' + D'} \quad \text{mit} \quad A', B', C', D' \in K[x] \quad \text{und} \quad A'D' - B'C' \in K\backslash\{0\}$$

und eingesetzt in das Minimalpolynom von S sowie vereinfacht

$$(AA'^2 + BA'C' + CC'^2)S'^2 + B(A'D' + B'C')S' + AB'^2 + BB'D' + CD'^2 = 0.$$

Weiters können wir wegen $A'D' + B'C' = A'D' - B'C' \in K\backslash\{0\}$ durch das inverse Element in K dividieren und erhalten

$$ES'^2 + BS' + F = 0 \quad E, F \in K[x]$$

mit den Definitionen

$$\begin{aligned} E &= \frac{AA'^2 + BA'C' + CC'^2}{A'D' + B'C'}, \\ F &= \frac{AB'^2 + BB'D' + CD'^2}{A'D' + B'C'}. \end{aligned}$$

Dieses Polynom ist, wenn man es durch E dividiert, das Minimalpolynom von S'. Wenn S' nun speziell ist, dann gilt aufgrund der Definition $|S' + \bar{S}'| = |S'| > 1$ und $|S'\bar{S}'| < |S'| = |S' + \bar{S}'|$. Also erhält man

$$\left| \frac{B}{E} \right| = |S' + \bar{S}'| > 1,$$

sowie

$$\left| \frac{F}{E} \right| = |S'\bar{S}'| < |S' + \bar{S}'| = \left| \frac{B}{E} \right|$$

und dadurch $|E| < |B|$ und $|F| < |B|$. Da $|B|$ fest ist, gibt es aufgrund der Endlichkeit von K wieder nur endlich viele E und F, also wieder nur endlich viele spezielle Elemente in der Äquivalenzklasse. ∎

Abschließend benötigen wir noch das folgende Hilfsergebnis

Hilfssatz 1.8.5 *Sei $S \in K((x^{-1}))$ reduziert mit der Eigenschaft, dass es ein $A \in K[x]$ gibt, sodass auch $A + \frac{1}{S}$ reduziert ist. Dann ist A eindeutig bestimmt.*

Beweis Wir bezeichnen

$$S' = A + \frac{1}{S}$$

und verwenden den Isomorphismus aus Satz 1.7.4 und erhalten

$$\left| A - \left(-\frac{1}{\bar{S}} \right) \right| = |\bar{S}'| < 1.$$

Daraus folgt wegen Hilfssatz 1.3.3

$$A = E\left(-\frac{1}{\bar{S}} \right),$$

was die Eindeutigkeit von A zeigt. ■

Nun können wir endlich den Satz von Lagrange formulieren und beweisen.

Satz 1.8.6 *Genau die quadratischen Irrationalitäten besitzen eine periodische Kettenbruchentwicklung. Diese ist für alle speziellen quadratischen Irrationalitäten rein periodisch und für alle anderen gemischt periodisch.*

Beweis. Sei $S \in K((x^{-1}))$.

Zuerst setzen wir voraus, dass S eine quadratische Irrationalität ist. Dann folgt aus Hilfssatz 1.8.2, dass es einen speziellen Rest gibt und aus Hilfssatz 1.8.3, dass auch alle weiteren Reste speziell sind. Diese liegen aber alle in derselben Äquivalenzklasse wie S und dort gibt es wegen Hilfssatz 1.8.4 nur endlich viele, was die Periodizität der Kettenbruchentwicklung bedeutet.

Besitzt nun umgekehrt S eine periodische Kettenbruchentwicklung, dann gibt es ein $n_0 \in \mathbb{N} \cup \{0\}$ und ein $k \in \mathbb{N}$ mit $R_{n+k} = R_n, \forall n \geq n_0$. Insbesondere gilt also $R_{n_0} = R_{n_0+k}$ und damit wegen Satz 1.4.4 (2)

$$R_{n_0} = \frac{AR_{n_0} + B}{CR_{n_0} + D} \quad \text{mit} \quad A, B, C, D \in K[x].$$

Umformen ergibt, dass R_{n_0} quadratische Irrationalität ist und wegen $S \sim R_{n_0}$ auch S.

Sei nun S speziell mit Kettenbruchentwicklung $S = [A_0; A_1, A_2, \ldots]$. Wir wissen schon, dass S eine periodische Kettenbruchentwicklung besitzt, also ein $n_0 \in \mathbb{N} \cup \{0\}$ und $k \in \mathbb{N}$ existiert mit $A_{n+k} = A_n, \forall n \geq n_0$. Es sei n_0 minimal gewählt und angenommen $n_0 \geq 1$. Dann gilt $R_{n_0} = R_{n_0+k}$ und wegen Hilfssatz 1.8.3, dass sowohl

$$A_{n_0-1} + \frac{1}{R_{n_0}} \quad \text{als auch} \quad A_{n_0-1+k} + \frac{1}{R_{n_0+k}}$$

speziell sind. Damit folgt aus Hilfssatz 1.8.5 $A_{n_0-1} = A_{n_0-1+k}$ was ein Widerspruch zur Minimalität von n_0 ist.

Wenn nun S eine rein periodische Kettenbruchentwicklung besitzt, dann folgt aus Hilfssatz 1.8.2 und Hilfssatz 1.8.3, dass S speziell ist. ■

Dieser Satz zeigt noch einmal die starke Analogie zur klassischen Theorie der Kettenbrüche.

Es stellt sich die Frage, ob dieser Satz auch für den Fall eines unendlichen Körpers richtig ist? Eine Richtung, und zwar dass der Wert eines periodischen Kettenbruchs stets eine quadratische Irrationalität ist, ist trivialerweise erfüllt. Die Umkehrung ist noch ein ungelöstes Problem.

Kapitel 2

Komplexität von Folgen

2.1 Das lineare Komplexitätsprofil

In kryptologischen Anwendungen, wie zum Beispiel beim *Vernam System* (siehe dazu [20]), benötigt man binäre Zufallszahlenfolgen. Diese können in der Praxis nur deterministisch erzeugt werden und damit sind sie nicht wirklich zufällig. Man muss also verlangen, dass das Verhalten dieser erzeugten Folgen, sehr gut das Verhalten von Zufallsfolgen widerspiegelt. Man spricht in diesem Zusammenhang von *Pseudozufallszahlen.*

Man benötigt also ein Maß für Folgen, dass diese bezüglich Zufälligkeit und Unvorhersehbarkeit bewertet. In der kryptologischen Anwendung hat sich herausgestellt, dass das *lineare Komplexitätsprofil* dafür sehr gut geeignet ist.

Wir wollen uns im Folgenden vom binären Fall lösen und Folgen über beliebigen Körpern betrachten. Bezeichne also K einen beliebigen Körper.

Wir beginnen mit der folgenden Definition

Definition 2.1.1 Sei $(s_i)_{i\geq 1}$ eine Folge von Elementen in K und $k \in \mathbb{N} \cup \{0\}$. Die Folge heißt *Schieberegisterfolge der Ordnung* k wenn es Elemente $a_0, a_1, \ldots, a_k$ mit $a_i \in K, 0 \leq i \leq k, a_k \neq 0$ gibt, sodass gilt

$$a_k s_{i+k} + a_{k-1} s_{i+k-1} + \ldots + a_0 s_i = 0 \quad \forall i \geq 1.$$

Weiters heißt das Polynom $f(x) = a_k x^k + a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ ein *charakteristisches Polynom* der Folge.

Damit führen wir den fundamentalen Begriff dieses Kapitels ein.

Definition 2.1.2 Sei $(s_i)_{i\geq 1}$ eine Folge in K und $n \in \mathbb{N}$. Dann heißt das

kleinste $k \in \mathbb{N} \cup \{0\}$, sodass $s_1, s_2, \ldots, s_n$ zu einer Schieberegisterfolge der Ordnung k fortgesetzt werden kann, die *n-te lineare Komplexität* der Folge, in Zeichen L_n.
Die Folge der linearen Komplexitäten $(L_n)_{n\geq 1}$ heißt das *lineare Komplexitätsprofil* von $(s_i)_{i\geq 1}$.

Unmittelbar aus der Definition der linearen Komplexität folgt, dass $0 \leq L_n \leq n$ und $L_n \leq L_{n+1}$ ist. Das Komplexitätsprofil einer Folge ist also eine nichtnegative, monoton wachsende Folge.

Unser erstes Ziel in diesem Kapitel wird sein, eine Verbindung zwischen der Komplexität von Folgen und der Kettenbruchentwicklung im Körper der formalen Laurentreihen herzuleiten. Dazu ordnen wir jeder Folge eine Laurentreihe zu.

Definition 2.1.3 Sei $(s_i)_{i\geq 1}$ eine Folge in K. Dann heißt die Laurentreihe

$$S = \sum_{i=1}^{\infty} s_i x^{-i}$$

die *erzeugende Funktion* der Folge.

Damit lassen sich die Schieberegisterfolgen über die erzeugenden Funktionen wie folgt charakterisieren

Satz 2.1.4 *Sei $f(x) \in K[x] \backslash \{0\}$ und $(s_i)_{i\geq 1}$ eine Folge in K. Genau dann ist die Folge Schieberegisterfolge mit charakteristischem Polynom $f(x)$, wenn die erzeugende Funktion S sich wie folgt darstellen läßt*

$$S = \frac{g(x)}{f(x)} \quad mit \quad g(x) \in K[x].$$

Beweis. Es sei $f(x) = a_k x^k + \ldots + a_1 x + a_0, a_k \neq 0$. Der Koeffizient bei der Potenz $x^{-i}, i \geq 1$ von $f(x)S$ lautet

$$a_0 s_i + a_1 s_{i+1} + \ldots + a_k s_{i+k}.$$

Damit ist der Beweis in beiden Richtungen trivial. ∎

Insbesondere folgt daraus, dass die Schieberegisterfolgen und nur diese eine rationale erzeugende Funktion besitzen. Verlangt man von der Bruchdarstellung zusätzlich, dass $(f(x), g(x)) = 1$ ist, dann heißt $f(x)$ ein *Minimalpolynom* der Schieberegisterfolge. Der Grad des Minimalpolynoms ist also die kleinste mögliche Ordnung der Schieberegisterfolge.

Damit definieren wir weiter

Definition 2.1.5 Sei $(s_i)_{i\geq 1}$ eine Folge in K und $n \in \mathbb{N}$. Weiters betrachten wir eine Schieberegisterfolge, die mit $s_1, s_2, \ldots, s_n$ beginnt und minimale Ordnung besitzt. Dann heißt ein Minimalpolynom dieser Folge *n-tes Minimalpolynom* von $(s_i)_{i\geq 1}$.

Aus der Definition des n-ten Minimalpolynoms folgt sofort, dass der Grad mit dem n-ten Komplexitätsprofil übereinstimmt.

Wir wollen nun die folgenden Probleme lösen

- Gegeben sei eine Folge und ein $n \in \mathbb{N}$. Wie kann man ein n-tes Minimalpolynom der Folge berechnen?
- Kann man aus der Kenntnis der ersten $n-1$ Minimalpolynome einer Folge das n-te Minimalpolynom berechnen?

Wir werden uns nun überlegen, dass das erste Problem in ein äquivalentes Problem für die erzeugende Funktion umformuliert werden kann, und dass die Lösung des äquivalenten Problems in enger Verbindung mit der Kettenbruchentwicklung der erzeugenden Funktion steht. Diese Vorgehensweise ist [5] entnommen.

2.2 Das rationale Approximationsproblem

Wir beginnen mit der folgenden Definition

Definition 2.2.1 Sei $S \in K((x^{-1}))$ und $n \in \mathbb{N}$. Das Problem $P, Q \in K[x], Q \neq 0$, $\mathrm{grad}(Q)$ minimal mit der Eigenschaft

$$v\left(S - \frac{P}{Q}\right) < -n$$

zu finden, heißt das *rationale Approximationsproblem.*
Weiters heißt jedes $\frac{P}{Q}$ mit der obigen Eigenschaft eine *Lösung des rationalen Approximationsproblems.*

Die Existenz einer Lösung des rationalen Approximationsproblems ist trivial. Weiters ist zu vermuten, dass man durch die Näherungsbrüche von S eine Lösung bekommt, da diese die im Kapitel 1.5 angesprochene Bestapproximationseigenschaft erfüllen.

Wir verwenden ab jetzt die Konvention, dass $\mathrm{grad}(Q_i)$ und $\mathrm{grad}(A_i)$ gleich ∞ sind, wenn diese für S nicht existieren. Dabei bezeichnet wie üblich Q_i

den Nenner des i-ten Näherungsbruches und A_i den i-ten Teilnenner in der Kettenbruchentwicklung von S.

Wir verschärfen jetzt die schon angesprochene Bestapproximationseigenschaft der Näherungsbrüche aus Kapitel 1.5.

Hilfssatz 2.2.2 *Sei $S \in K((x^{-1}))$ und $\frac{P_i}{Q_i}$ der i-te Näherungsbruch von S. Dann gilt für alle $P, Q \in K[x]$ mit $1 \leq |Q| < |Q_{i+1}|$*

$$\left| S - \frac{P}{Q} \right| \geq \left| S - \frac{P_i}{Q_i} \right| .$$

Beweis. Die Aussage ist trivial wenn $S = \frac{P_i}{Q_i}$ und wenn $\frac{P}{Q} = \frac{P_i}{Q_i}$ ist. Also können wir beides ausschließen. Dann gilt

$$\left| S - \frac{P_i}{Q_i} \right| = \frac{1}{|Q_i||Q_{i+1}|}$$

und weiters

$$\left| \frac{P}{Q} - \frac{P_i}{Q_i} \right| = \frac{|PQ_i - P_iQ|}{|QQ_i|} > \frac{1}{|Q_iQ_{i+1}|}$$

und daraus folgt

$$\left| S - \frac{P}{Q} \right| = \left| \frac{P}{Q} - \frac{P_i}{Q_i} \right| > \frac{1}{|Q_iQ_{i+1}|} = \left| S - \frac{P_i}{Q_i} \right| ,$$

wie es behauptet war. ■

Damit bestätigt sich unsere Vermutung, dass man mit den Näherungsbrüchen von S eine Lösung des rationalen Approximationsproblems erhält.

Hilfssatz 2.2.3 *Sei $S \in K((x^{-1}))$ und $n \in \mathbb{N}$. Weiters sei $i \geq 0$ jener Index für den gilt*

$$\mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) \leq n < \mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}).$$

Dann ist $\frac{P_i}{Q_i}$ eine Lösung des rationalen Approximationsproblems.

Beweis. Zunächst gilt

$$v\left(S - \frac{P_i}{Q_i}\right) = -\mathrm{grad}(Q_i) - \mathrm{grad}(Q_{i+1}) < -n.$$

Im Fall $i = 0$ ist wegen $Q_0 = 1$ die Behauptung schon bewiesen. Sei also $i > 0$ vorausgesetzt. Dann gilt

$$v\left(S - \frac{P_{i-1}}{Q_{i-1}}\right) = -\mathrm{grad}(Q_{i-1}) - \mathrm{grad}(Q_i) \geq -n$$

und wegen Hilfssatz 2.2.2 für $P, Q \in K[x], Q \neq 0, \mathrm{grad}(Q) < \mathrm{grad}(Q_i)$

$$v\left(S - \frac{P}{Q}\right) \geq v\left(S - \frac{P_{i-1}}{Q_{i-1}}\right) \geq -n,$$

was die Minimalität von Q_i zeigt. ∎

Nun können wir die erste der beiden Fragen, die wir am Ende des Abschnitt 1 gestellt haben, lösen.

Hilfssatz 2.2.4 *Sei $(s_i)_{i\geq 1}$ eine Folge in K und $n \in \mathbb{N}$. Weiters sei S die erzeugende Funktion der Folge. Genau dann ist $f(x) \in K[x]\backslash\{0\}$ n-tes Minimalpolynom der Folge, wenn es ein $g(x) \in K[x]$ gibt, sodass $\frac{g(x)}{f(x)}$ Lösung des rationalen Approximationsproblems für S ist.*

Beweis.

$\Longrightarrow$: Sei $f(x)$ n-tes Minimalpolynom der Folge. Dann gibt es nach Definition eine Schieberegisterfolge, die mit $s_1, s_2, \ldots, s_n$ beginnt und $f(x)$ als Minimalpolynom besitzt. Sei $\frac{g(x)}{f(x)}$ die erzeugende Funktion dieser Folge. Aufgrund der Defintion des Minimalpolynoms einer Folge ist sofort klar, dass $\frac{g(x)}{f(x)}$ das rationale Approximationsproblem löst.

$\Longleftarrow$: Sei nun umgekehrt $\frac{g(x)}{f(x)}$ Lösung des rationalen Approximationsproblems. Es gilt klarerweise, dass $(g(x), f(x)) = 1$ ist und damit erzeugt diese Lösung eine Schieberegisterfolge mit Minimalpolynom $f(x)$. Diese beginnt mit $s_1, s_2, \ldots, s_n$ und hat unter allen Folgen, die ebenfalls mit $s_1, s_2, \ldots, s_n$ beginnen minimale Ordnung und damit ist $f(x)$ n-tes Minimalpolynom. ∎

Damit ist der Zusammenhang zwischen der linearen Komplexität von Folgen und Kettenbruchentwicklungen im Körper der formalen Laurentreihe hergestellt.

2.3 Folgen mit vorgegebenem Komplexitätsprofil

Aus den Hilfssätzen 2.2.3 und 2.2.4 des letzten Unterabschnittes erhalten wir sofort ein zentrales Ergebnis über das lineare Komplexitätsprofil von Folgen. Dieses geht auf Niederreiter [12] zurück.

Satz 2.3.1 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S und $n \in \mathbb{N}$. Weiters sei $i \geq 0$ jener Index für den gilt*

$$\mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) \leq n < \mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}).$$

Dann ist $L_n = \mathrm{grad}(Q_i)$.

Als unmittelbare Folgerung erhalten wir folgende Aussage über die Form des linearen Komplexitätsprofils.

Folgerung 2.3.2 *Sei* $(s_i)_{i\geq 1}$ *eine Folge in* K *mit erzeugenden Funktion* S. *Weiters sei* $q_i = \mathrm{grad}(Q_i), i \geq 0$. *Dann hat das lineare Komplexitätsprofil der Folge die Form*

$$q_0, q_0, \ldots, q_0, q_1, q_1, \ldots, q_1, \ldots, q_i, q_i, \ldots, q_i, \ldots,$$

wobei $q_1 - 1$ *oft* q_0 *wiederholt wird und* $q_{i+1} - q_{i-1}$ *oft* $q_i, i \geq 1$.

Die Q_i sind für die Konstruktion von Folgen mit vorgegebenem Komplexitätsprofil weniger geeignet. Deshalb betrachtet man

Definition 2.3.3 Sei $(s_i)_{i\geq 1}$ eine Folge in K mit Komplexitätsprofil wie in der Folgerung 2.3.2. Dann heißt die Folge $(q_{i+1} - q_i)_{i\geq 0}$ *Sprungkomplexitätsprofil* der Folge s_i.

Man beachte, dass das Sprungkomplexitätsprofil nur im Fall, dass keine Schieberegisterfolge vorliegt eine unendliche Folge ist. Weiters ist es eine Folge von positiven Zahlen.

Wichtig für die Konstruktion ist nun die folgende, einfache Erkenntnis

Hilfssatz 2.3.4 *Durch Angabe des Sprungkomplexitätsprofils einer Folge ist auch das lineare Komplexitätsprofil eindeutig bestimmt.*

Beweis. Man braucht nur die Folge der q_i aus dem Sprungkomplexitätsprofil zu ermitteln, denn dann erhält man das lineare Komplexitätsprofil mit Folgerung 2.3.2. Diese zu ermitteln ist aber trivial. ■

Damit ist es für die Konstruktion egal, ob man vom linearen Komplexitätsprofil oder vom Sprungkomplexitätsprofil ausgeht.

Für das Sprungkomplexitätsprofil einer Folge gilt

Satz 2.3.5 *Sei* $(s_i)_{i\geq 1}$ *eine Folge in* K *mit erzeugenden Funktion* S. *Dann ist* $(\mathrm{grad}(A_i))_{i\geq 1}$ *das Sprungkomplexitätsprofil der Folge.*

Beweis. Folgt aus Satz 1.2.7 (3) und Folgerung 2.3.2. ■

Damit erhält man eine Folge mit vorgegebenem Sprungkomplexitätsprofil, indem man einfach einen Kettenbruch betrachtet, dessen i-ter Teilnenner ein beliebiges Polynom vom Grad des i-ten Sprungkomplexitätsprofils ist und die von diesem Kettenbruch erzeugte Folge berechnet.

Wir sollten uns also einen Algorithmus überlegen, der bei gegebener Kettenbruchentwicklung, die erzeugte Folge berechnet.

2.4 Berechnung der erzeugten Folge

Es sei $A_1, A_2, \ldots$ eine gegebene endliche oder unendliche Folge von Polynomen in $K[x]$ mit Grad größer als 0. Wir betrachten $S = [0; A_1, A_2, \ldots]$ und $(s_i)_{i\geq 1}$ bezeichne die von S erzeugte Folge. Wir suchen einen Algorithmus zur Berechnung der s_i.

Zunächst betrachten wir nur die ersten i Polynome $A_1, \ldots, A_i$. Dazu berechnen wir rekursiv P_i und Q_i mit $A_0 = 0$. Wegen

$$v\left(S - \frac{P_i}{Q_i}\right) = -\mathrm{grad}(Q_i) - \mathrm{grad}(Q_{i+1})$$

erzeugt der i-te Näherungsbruch eine Folge, von der die ersten $\mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}) - 1$ Folgeglieder mit denen von s_i übereinstimmen. Da

$$\mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}) - 1 \geq 2\mathrm{grad}(Q_i)$$

ist, erhält man also insbesondere durch Berechnung der ersten $2\mathrm{grad}(Q_i)$ Folgeglieder der erzeugten Folge des i-ten Näherungsbruches, die entsprechenden Glieder von s_i.

Die Berechnung der erzeugten Folge des i-ten Näherungsbruches wird durch den Satz 2.1.4 wesentlich erleichtert. Dieser besagt insbesondere, dass diese Folge eine Schieberegisterfolge mit Minimalpolynom Q_i ist. Es genügen also die ersten $\mathrm{grad}(Q_i)$ Folgeglieder, um die Rekursion - die durch die Koeffizienten von Q_i festgelegt ist - zu starten und damit die Folge zu berechnen. Nun gilt

$$\mathrm{grad}(Q_i) \leq \mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) - 1, \quad i \geq 2$$

und damit bekommt man die Startwerte für die Rekursion aus der entsprechenden Berechnung für $i - 1$.

Zusammengefasst erhält man den folgenden Algorithmus der auf Niederreiter [12] zurückgeht.

Ausgehend von den Polynomen $A_1, A_2, \ldots, A_i$ berechnet man zuerst rekursiv die Folge der Q_j und P_j mit $A_0 = 0$. Weiters bezeichnen wir mit q_j =grad(Q_j). Dann führen wir die folgenden Schritte durch

Schritt 1: Es gilt

$$\frac{P_1}{Q_1} = \frac{1}{Q_1} = c^{-1}x^{-q_1} + \text{Terme niedriger Ordnung},$$

wobei c der Führungskoeffizient von Q_1 ist. Daraus erkennt man die Startwerte zur Berechnung der erzeugten Folge des 1-ten Näherungsbruches. Diese lauten

$$s_1 = 0, s_2 = 0, \ldots, s_{q_1-1} = 0, s_{q_1} = c^{-1}.$$

Mit diesen Werten und der Rekursion, die durch Q_1 festgelegt ist, berechnen wir die ersten $q_1 + q_2 - 1$ Glieder der erzeugten Folge des 1-ten Näherungsbruches.

Schritt j: $(\mathbf{2 \leq j \leq i})$ Die ersten $q_{j-1}+q_j-1$ Glieder der Folge s_i sind schon berechnet. Wir berechnen mit der Rekursion, die durch Q_j festgelegt wird und mit den letzten $\mathrm{grad}(Q_j)$ Gliedern der bereits berechneten Folge, die nächsten $q_j + q_{j+1} - 1$ Folgeglieder falls $j < i$ ist bzw. die nächsten $2q_j$ Folgeglieder falls $j = i$ ist.

Eine kleine Modifikation des Algorithmus kann, in dem für die Anwendung so wichtigen binären Fall, durchgeführt werden. Man weiß nämlich nicht nur, dass die ersten $q_i + q_{i+1} - 1$ Folgeglieder der erzeugten Folge des i-ten Näherungsbruches mit denen von s_i übereinstimmen, sondern auch, dass das $q_i + q_{i+1}$-ste nicht übereinstimmt. Damit ist es aber im binären Fall durch das Kompliment eindeutig bestimmt. Man kann also in jedem Schritt des Algorithmus im binären Fall auch noch das $q_i + q_{i+1}$-ste Bit berechnen.

Wenn man nicht nur die ersten i Polynome betrachtet, sondern den Algorithmus auf die ganze Folge der Polynome anwendet und im letzten Schritt im Falle einer endlichen Folge die Rekursion nicht abbricht, dann erhält man natürlich die gewünschte Folge der s_i.

Damit sind wir in der Lage, Folgen mit vorgegebenem Komplexitätsprofil zu konstruieren.

2.5 Minimalpolynome einer Folge

Im Unterabschnitt 2 dieses Kapitels haben wir für eine Folge ein n-tes Minimalpolynom bestimmt. Wir suchen jetzt alle n-ten Minimalpolynome einer Folge.

Wir beginnen mit einem sehr wichtigen Hilfssatz.

Hilfssatz 2.5.1 *Seien $f, g \in K[x]$ und $S \in K((x^{-1}))$ mit $v(fS - g) < 0$. Dann gibt es ein $j \geq 0$ mit*

$$f = \sum_{h=0}^{j} C_h Q_h \quad \text{und} \quad g = \sum_{h=0}^{j} C_h P_h,$$

wobei $C_h \in K[x]$ und $\operatorname{grad}(C_h) < \operatorname{grad}(A_{h+1})$, $0 \leq h \leq j$.

Ist zusätzlich $f \neq 0$ dann gilt

$$v(fS - g) = \operatorname{grad}(C_i) - \operatorname{grad}(Q_{i+1}),$$

wobei i der kleinste Index ist, sodass $C_i \neq 0$ ist.

Beweis. Für $f = 0$ folgt aus $v(fS - g) < 0$, dass auch $g = 0$ ist und damit ist in diesem Fall die Aussage trivial. Sei also für das folgende $f \neq 0$ vorausgesetzt.

Die Grade der Q_i sind eine streng wachsende Folge. Sei j maximal mit der Eigenschaft $\operatorname{grad}(Q_j) < \operatorname{grad}(f)$ gewählt. Wir dividieren f durch Q_j, den Rest durch Q_{j-1} usw. und erhalten für f die behauptete Darstellung.

Weiters gilt

$$v(C_h Q_h) < v(Q_{h+1}) \quad 0 \leq h \leq j$$

und damit

$$v(C_h) < v(Q_{h+1}) - v(Q_h) = v(A_{h+1}) \quad 0 \leq h \leq j.$$

Wir betrachten nun

$$\begin{aligned} v(C_h(Q_h S - P_h)) &= v(C_h) - v(Q_{h+1}) \\ &< v(A_{h+1}) - v(A_{h+1}) - v(Q_h) \\ &= -v(Q_h) < 0 \end{aligned}$$

mit $0 \leq h \leq j$. Diese Schlusskette ist im Fall $S = \frac{P_j}{Q_j}$ und $h = j$ nicht richtig, aber in diesem Fall ist die Bewertung trivialerweise kleiner als 0.

Damit und mit der Voraussetzung $v(fS - g) < 0$ folgt

$$v\left(g - \sum_{h=0}^{j} C_h P_h\right) = v\left(g - fS + \sum_{h=0}^{j} C_h(Q_h S - P_h)\right) < 0,$$

woraus - weil $g - \sum_{h=0}^{j} C_h P_h$ ein Polynom ist - die behauptete Darstellung für g folgt.

Für den Zusatz betrachten wir

$$v(C_i(Q_iS - P_i)) = v(C_i) - v(Q_{i+1}) \geq -v(Q_{i+1})$$

und von vorher

$$v(C_h(Q_hS - P_h)) < -v(Q_h) \leq -v(Q_{i+1}) \quad i < h \leq j,$$

wobei die Ungleichung im Fall $S = \frac{P_j}{Q_j}$ und $h = j$ wieder trivial gilt.

Damit erhalten wir

$$v(fS - g) = v\left(\sum_{h=i}^{j} C_h(Q_hS - P_h)\right) = v(C_i) - v(Q_{i+1}),$$

wie es behauptet war. ■

Damit können wir alle n-ten Minimalpolynome einer Folge bestimmen. Der Beweis des folgenden Satzes ist eine Mischung aus den Beweisen von [12] und [5].

Satz 2.5.2 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S und $n \in \mathbb{N}$. Weiters sei $i \geq 0$ jener Index für den gilt*

$$\mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) \leq n < \mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}).$$

Dann sind alle n-ten Minimalpolynome der Folge gegeben durch

$$m_n = aQ_i + CQ_{i-1},$$

mit $a \in K, a \neq 0$ und $C \in K[x]$,$\mathrm{grad}(C) < 2\mathrm{grad}(Q_i) - n$.

Beweis. Wir zeigen zuerst, dass jedes n-te Minimalpolynom diese Form haben muss. Sei also m_n ein n-tes Minimalpolynom der Folge.

Nach Hilfssatz 2.2.4 existiert ein Polynom g_n, sodass $\frac{g_n}{m_n}$ das zugehörige rationale Approximationsproblem löst. Es gilt

$$v(m_nS - g_n) = v(m_n) + v\left(S - \frac{g_n}{m_n}\right) < L_n - n \leq 0$$

und damit können wir den Hilfssatz 2.5.1 anwenden. Wir erhalten also

$$m_n = \sum_{h=j}^{i} C_hQ_h \quad \text{und} \quad g_n = \sum_{h=j}^{i} C_hP_h \quad \text{mit} \quad C_j \neq 0$$

und wegen dem Zusatz

$$v(m_nS - g_n) = \text{grad}(C_j) - \text{grad}(Q_{j+1}).$$

Dass die Summe dabei bis i geht, wissen wir schon, denn aus Satz 2.3.1 folgt

$$\text{grad}(m_n) = L_n = \text{grad}(Q_i)$$

und damit ist auch weiters klar, dass $C_i = a, a \in K, a \neq 0$ ist.

Nun gilt

$$\begin{aligned} v(m_nS - g_n) &= v(C_j) - v(Q_{j+1}) \\ &< L_n - n \\ &\leq v(Q_i) - v(Q_{i-1}) - v(Q_i), \end{aligned}$$

woraus $0 < v(Q_{j+1}) - v(Q_{i-1})$ und damit $j = i$ oder $j = i - 1$ folgt.

Im Fall $j = i$ ist die gewünschte Darstellung schon gezeigt.

Im Fall $j = i - 1$ gilt wegen

$$v(C_i) < L_n + v(Q_i) - n = 2v(Q_i) - n$$

ebenfalls die behauptete Darstellung.

Sei nun umgekehrt m_n ein Polynom von der behaupteten Form. Wir wollen zeigen, dass es sich um ein n-tes Minimalpolynom handelt. Im Fall $C = 0$ ist die Aussage trivial. Sei also $C \neq 0$ vorausgesetzt.

Es sei $g_n = aP_i + CP_{i-1}$ und wir betrachten

$$v(Q_iS - P_i) = -v(Q_{i+1}),$$

sowie

$$v(C(Q_{i-1}S - P_{i-1})) = v(C) - v(Q_i) \geq -v(Q_i) > -v(Q_{i+1})$$

und damit

$$\begin{aligned} v\left(S - \frac{g_n}{m_n}\right) &= v(m_nS - g_n) - v(m_n) \\ &= v(C) - v(Q_i) - v(Q_i) < -n, \end{aligned}$$

woraus wegen $\text{grad}(m_n) = \text{grad}(Q_i)$ und Q_i ist n-tes Minimalpolynom folgt, dass $\frac{g_n}{m_n}$ eine Lösung des rationalen Approximationsproblems ist. Daraus folgt wegen Hilfssatz 2.2.4, dass m_n ein n-tes Minimalpolynom ist. ■

Damit haben wir auch das rationale Approximationsproblem vollständig gelöst. Es gilt nämlich

Hilfssatz 2.5.3 *Sei $S \in K((x^{-1}))$ und $n \in \mathbb{N}$. Weiters seien $P, Q \in K[x], Q \neq 0$ mit $\frac{P}{Q}$ ist eine Lösung des rationalen Approximationsproblems. Dann gilt $P = E(QS)$.*

Beweis. Zunächst sei nochmals daran erinnert, dass E(QS) der polynomiale Anteil der Laurentreihe ist. Es gilt

$$v(QS - P) = v(Q) + v\left(S - \frac{P}{Q}\right) < v(Q) - n \leq 0,$$

wobei die letzte Ungleichung aus der Minimalität von $v(Q)$ folgt. Damit folgt die Behauptung aus Hilfssatz 1.3.3. ■

Dies bedeutet insbesondere, dass es beim rationalen Approximationsproblem nur auf die Bestimmung von Q ankommt.

Zusammengefasst erhalten wir also als Lösung für das rationale Approximationsproblem

Satz 2.5.4 *Sei $S \in K((x^{-1}))$ und $n \in \mathbb{N}$. Weiters sei $i \geq 0$ so gewählt, dass gilt*

$$\mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) \leq n < \mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}).$$

Dann sind alle Lösungen des rationalen Approximationsproblems gegeben durch

$$Q = aQ_i + CQ_{i-1} \quad \text{mit} \quad a \in K, a \neq 0, \mathrm{grad}(C) < 2\mathrm{grad}(Q_i) - n$$

und $P = E(QS)$.

Beweis. Wenn $v(S) < 0$ ist, dann folgt die Aussage aus Hilfssatz 2.2.4, Satz 2.5.2 und Hilfssatz 2.5.3.

Ist $v(S) \geq 0$ dann setzt man $S' = S - E(S)$. Das rationale Approximationsproblem für S' und n besitzt, wegen dem ersten Teil und aufgrund der Definition von S', die behaupteten Lösungen - natürlich mit $P' = E(QS')$. Man überlegt sich sofort, dass man alle Lösungen des Ausgangsproblems erhält, wenn man Q gleichläßt und $P = P' + E(S)Q$ setzt. ■

2.6 Der Berlekamp-Massey Algorithmus

In diesem Unterabschnitt beschränken wir uns auf den binären Fall. Also K ist im Folgenden gleich $\mathbb{F}_2$.

Wir wollen nun die zweite von den beiden Fragen, die wir am Ende des Unterabschnitts 1 dieses Kapitels gestellt haben, beantworten. Wir suchen also einen rekursiven Algorithmus zur Bestimmung einer Folge von Minimalpolynomen.

Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S. Wie üblich setzen wir $q_i = \mathrm{grad}(Q_i), i \geq 0$ und weiters $a_i = \mathrm{grad}(A_i), i \geq 1$ und

$$A_i = \sum_{l=1}^{k_i} x^{a_i - j_{i,l}}$$

mit

$$0 = j_{i,1} < j_{i,2} < \ldots < j_{i,k_i} \leq a_i.$$

Zusätzlich definieren wir noch $j_{i,k_i+1} = q_{i+1} - q_{i-1}, i \geq 1$.

Damit definieren wir

$$A_{i,k} = \sum_{l=1}^{k} x^{a_i - j_{i,k}} \quad i \geq 1, k_i \geq k \geq 1$$

und

$$Q_{i,k} = A_{i,k} Q_{i-1} + Q_{i-2} \quad i \geq 1, k_i \geq k \geq 1,$$

sowie

$$P_{i,k} = A_{i,k} P_{i-1} + P_{i-2} \quad i \geq 1, k_i \geq k \geq 1.$$

Damit verschärfen wir zunächst den Satz 1.2.8 (1).

Hilfssatz 2.6.1 *Mit den Bezeichnungen von vorher gilt*

$$v(Q_{i,k} S - P_{i,k}) = -q_{i-1} - j_{i,k+1} \quad i \geq 1, k_i \geq k \geq 1,$$

also insbesondere $P_{i,k} = E(Q_{i,k} S)$.

Beweis. Für $k = k_i$ ist die Aussage mit Satz 1.2.8 (1) trivial. Sei also $k < k_i$ für das Folgende vorausgesetzt. Zunächst gilt

$$\begin{aligned} v((A_{i,k} + A_i)(Q_{i-1} S - P_{i-1})) &= v(A_{i,k} + A_i) + v(Q_{i-1} S - P_{i-1}) \\ &= a_i - j_{i,k+1} - q_i \geq -q_i > -q_{i+1} \end{aligned}$$

und damit

$$\begin{aligned} v(Q_{i,k}S - P_{i,k}) &= v(A_{i,k}(Q_{i-1}S - P_{i-1}) + Q_{i-2}S - P_{i-2}) \\ &= v((A_{i,k} + A_i)(Q_{i-1}S - P_{i-1}) + Q_iS - P_i) \\ &= a_i - j_{i,k+1} - q_i = -q_{i-1} - j_{i,k+1}, \end{aligned}$$

wie es behauptet war. Die zweite Aussage des Satzes ist trivial. ■

Damit zeigen wir

Satz 2.6.2 *Seien wieder alle Bezeichnungen wie vorher. Wir definieren eine Folge von Polynomen*

$$m_n = \begin{cases} Q_0 & 1 \le n < q_1 \\ Q_{i,k} & i \ge 1, q_{i-1} + q_i + j_{i,k} \le n < q_{i-1} + q_i + j_{i,k+1} \end{cases}$$

und bezeichnen mit $l_n = \mathrm{grad}(m_n)$.

Für diese Folge gelten die folgenden Eigenschaften

1. m_n *ist* n*-tes Minimalpolynom der Folge* s_i.
2. *Für* $n \ge q_1$ *gilt entweder*
   (a) *wenn* m_n *auch* $n+1$*-tes Minimalpolynom ist, dann gilt* $m_{n+1} = m_n$ *andernfalls*
   (b) *erhält man* m_{n+1} *durch*

$$m_{n+1} = \begin{cases} m_n + x^{(j-l_j)-(n-l_n)} m_j & (j - l_j) - (n - l_n) \ge 0 \\ x^{(n-l_n)-(j-l_j)} m_n + m_j & (j - l_j) - (n - l_n) < 0 \end{cases}$$

wobei j *der größte Index ist mit* $l_j < l_n$.

Beweis. Wir zeigen zunächst die erste Eigenschaft.

Für $n < q_1$ ist die Aussage trivial. Es sei also im folgenden $n \ge q_1$ vorausgesetzt. Weiters gelte

$$q_{i-1} + q_i + j_{i,k} \le n < q_{i-1} + q_i + j_{i,k+1}$$

und damit $m_n = Q_{i,k}$.

Es gilt

$$m_n = Q_i + CQ_{i-1} \quad \text{mit} \quad C = \sum_{l=k+1}^{k_i} x^{a_i - j_{i,l}}$$

und

$$v(C) = a_i - j_{i,k+1} < a_i + q_{i-1} + q_i - n = 2q_i - n,$$

weshalb die Behauptung aus Satz 2.5.2 folgt.

Jetzt kommen wir zur zweiten Eigenschaft.

Dazu sei wieder

$$q_{i-1} + q_i + j_{i,k} \leq n < q_{i-1} + q_i + j_{i,k+1}$$

und damit $m_n = Q_{i,k}$.

Wenn nun (a) erfüllt ist, dann gilt wegen Hilfssatz 2.2.4 und Hilfssatz 2.5.3 sowie $g_n = E(m_n S)$

$$v\left(S - \frac{g_n}{m_n}\right) < -n - 1.$$

Nach Hilfssatz 2.6.1 ist $g_n = P_{i,k}$ und es gilt

$$v\left(S - \frac{g_n}{m_n}\right) = v(Q_{i,k}S - P_{i,k}) - v(m_n) = -q_{i-1} - j_{i,k+1} - q_i,$$

wobei die verwendete Beziehung $v(m_n) = q_i$ aus der Definition von $Q_{i,k}$ folgt.

Zusammenfassend erhalten wir

$$n + 1 < q_{i-1} + q_i + j_{i,k+1},$$

woraus folgt, dass $m_{n+1} = Q_{i,k} = m_n$.

Sei nun (b) erfüllt. Dann ist

$$n + 1 = q_{i-1} + q_i + j_{i,k+1}.$$

Dies bedeutet insbesonders

$$m_{n+1} = \begin{cases} Q_{i,k+1} & k < k_i \\ Q_{i+1,1} & k = k_i. \end{cases}$$

Weiters gilt

$$j = q_{i-1} + q_i - 1 \quad \text{und} \quad l_j = q_{i-1} \quad \text{und} \quad m_j = Q_{i-1}$$

und damit

$$(j - l_j) - (n - l_n) = a_i - j_{i,k+1} = \begin{cases} a_i - j_{i,k+1} \geq 0 & k < k_i \\ -a_{i+1} < 0 & k = k_i. \end{cases}$$

Wir unterscheiden also zwei Fälle.

Zunächst sei $(j - l_j) - (n - l_n) \geq 0$. Dann gilt

$$\begin{aligned} m_{n+1} &= Q_{i,k+1} = A_{i,k+1} Q_{i-1} + Q_{i-2} \\ &= (A_{i,k} + x^{a_i - j_{i,k+1}}) Q_{i-1} + Q_{i-2} \\ &= Q_{i,k} + x^{a_i - j_{i,k+1}} Q_{i-1} \\ &= m_n + x^{(j-l_j)-(n-l_n)} m_j. \end{aligned}$$

Bleibt also noch der Fall, das $(j - l_j) - (n - l_n) < 0$ ist.

$$\begin{aligned} m_{n+1} &= Q_{i+1,1} = A_{i+1,1} Q_i + Q_{i-1} \\ &= x^{a_{i+1}} Q_i + Q_{i-1} \\ &= x^{(n-l_n)-(j-l_j)} m_n + m_j \end{aligned}$$

Damit haben wir den Satz vollständig bewiesen. ■

Mit diesem Satz erhalten wir einen rekursiven Algorithmus zur Berechnung einer Folge von Minimalpolynomen.

Sei $(s_i)_{i \geq 1}$ eine Folge in K. Man bestimmt zuerst q_1. Da $q_1 = a_1$ ist dies der erste Index i mit $s_i \neq 0$. Damit sind die ersten $q_1 - 1$ Folgeglieder bestimmt als $Q_0 = 1$. Das nächste erhält man als $Q_{1,1} = x^{q_1}$.

Für die weiteren wendet man die zweite Eigenschaft im Satz 2.6.2 an. Wenn man also die ersten n schon bestimmt hat, dann überprüft man, ob m_n auch $n + 1$-tes Minimalpolynom ist. Wenn dies der Fall ist, dann stimmt m_{n+1} mit m_n überein und andernfalls verwendet man die Berechnungsvorschrift aus Satz 2.6.2 (2) Teil (b).

Zur Überprüfung, ob m_n $n + 1$-tes Minimalpolynom ist, muss man wegen Satz 2.2.4 und Hilfssatz 2.5.3. sowie wegen der Tatsache, dass m_n schon n-tes Minimalpolynom ist, nur zeigen, dass

$$v\left(S - \frac{E(m_n S)}{m_n}\right) < -n - 1.$$

Dieser rekursive Algorithmus zur Berechnung einer Folge von Minimalpolynomen wird als *Berlekamp-Massey Algorithmus* (siehe [8]) bezeichnet. Dieser Zugang zum Berlekamp-Massey Algorithmus ist [5] entnommen.

2.7 Perfektes lineares Komplexitätsprofil

Unser Ziel ist, wie schon zu Beginn dieses Kapitels erwähnt, die Konstruktion von Folgen, die zufällig und unvorhersehbar sind. Dazu müssen wir zunächst einmal klären, was wir unter Zufälligkeit verstehen. Wir brauchen also ein wahrscheinlichkeitstheoretisches Modell.

Betrachtet man das n-te Komplexitätsprofil, dann gehen von jeder Folge nur die ersten n Folgeglieder in die Berechnung ein. Also wird man nur Folgen der Länge n betrachten, die man alle als gleichwahrscheinlich ansieht. Die n-te Komplexität kann dann, auf der Menge dieser Folgen, als Zufallsvariable aufgefasst werden. Rueppel (siehe [20]) hat im binären Fall mit diesem stochastischem Modell gezeigt, dass der Erwartungswert dieser Zufallsvariable $\frac{n}{2} + c_n$ mit $0 \leq c_n \leq \frac{5}{18}$ ist.

Man wird Folgen nun wohl als typisch zufällig ansehen, wenn die Komplexität dieses erwartete Verhalten besitzt. Dies führt zur folgenden Definition

Definition 2.7.1 Sei $(s_i)_{i\geq 1}$ eine Folge in K. Wir sagen die Folge besitzt ein *perfektes lineares Komplexitätsprofil (PLKP)*, wenn gilt

$$L_n = \left[\frac{n+1}{2}\right] \quad \text{für} \quad n \geq 1.$$

Es gilt die folgende Charakterisierung von Folgen mit perfektem linearen Komplexitätsprofil über die erzeugenden Funktionen

Satz 2.7.2 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S. Genau dann besitzt die Folge ein PLKP, wenn S irrational ist und $S = [0; A_1, A_2, \ldots]$, mit $\mathrm{grad}(A_i) = 1, i \geq 1$ gilt.*

Beweis. Wenn S irrational ist und die geforderte Kettenbruchentwicklung besitzt, dann gilt wegen Satz 1.2.7 (3) $\mathrm{grad}(Q_i) = i, i \geq 0$. Damit folgt die Behauptung sofort aus Satz 2.3.1.

Besitzt also umgekehrt die Folge ein PLKP. Dann folgt aus $\lim_{n\longrightarrow\infty} L_n = \infty$, dass S irrational ist. Sei also $S = [0; A_1, A_2, \ldots]$ und wir wollen annehmen, dass $\mathrm{grad}(A_i) > 1$ ist, für ein passendes i. Wir betrachten

$$n = \mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) = 2\mathrm{grad}(Q_i) - \mathrm{grad}(A_i)$$

und damit

$$L_n = \mathrm{grad}(Q_i) = \frac{n + \mathrm{grad}(A_i)}{2} > \frac{n+1}{2} \geq \left[\frac{n+1}{2}\right],$$

was ein Widerspruch zum PLKP ist. ∎

Mit diesem Satz erhält man insbesondere auch eine Möglichkeit zur Konstruktion von Folgen mit PLKP. Man gibt sich eine Folge von Polynomen $(A_i)_{i\geq 1}$ vom Grad 1 vor und berechnet die vom Kettenbruch $S = [0; A_1, A_2, \ldots]$ erzeugte Folge mit Hilfe der Methode aus Unterabschnitt 4 dieses Kapitels.

Im wichtigsten Fall für die Anwendung, nämlich wenn der Körper nur zwei Elemente besitzt, ist noch eine wesentlich explizitere Charakterisierung der Folgen mit PLKP möglich. Diese Charakterisierung geht auf Wang und Massey zurück (siehe [22]). Der folgende Beweis stammt von Niederreiter [12].

Satz 2.7.3 (Wang und Massey) *Sei $(s_i)_{i\geq 1}$ eine Folge in $\mathbb{F}_2$. Genau dann hat die Folge PLKP, wenn gilt*

$$s_1 = 1 \quad \textit{und} \quad s_{2i+1} = s_{2i} + s_i \quad \textit{für} \quad i \geq 1.$$

Beweis. Grundidee ist die Betrachtung der folgenden Abbildung in $\mathbb{F}_2((x^{-1}))$

$$D(T) = x^{-1}T^2 + (1 + x^{-1})T + x^{-1} \quad \text{mit} \quad T \in \mathbb{F}_2((x^{-1})),$$

die folgende Eigenschaften besitzt

$$\begin{aligned}
&D(T + U + V) = D(T) + D(U) + D(V) \quad \text{für} \quad T, U, V \in \mathbb{F}_2((x^{-1})),\\
&D(T^{-1}) = D(T)T^{-2} \quad \text{für} \quad T \in \mathbb{F}_2((x^{-1})), T \neq 0,\\
&D(x) + D(c) = c + 1 \quad \text{für} \quad c \in \mathbb{F}_2.
\end{aligned}$$

Diese folgen unmittelbar aus der Definition.

Sei nun $(s_i)_{i\geq 1}$ eine Folge mit PLKP. Dann ist wegen Satz 2.7.2 die erzeugende Funktion S der Folge irrational und für die Kettenbruchentwicklung $S = [0; A_1, A_2, \ldots]$ gilt, dass $A_i = x + a_i, a_i \in \mathbb{F}_2, i \geq 1$ ist. Weiters verwenden wir die üblichen Bezeichnungen des Kettenbruchalgorithmus

$$B_i^{-1} = A_{i+1} + B_{i+1}$$

und erhalten mit den Eigenschaften von D

$$D(B_i)B_i^2 = D(B_i^{-1}) = D(x + a_{i+1} + B_{i+1}) = a_{i+1} + 1 + D(B_{i+1})$$

und daraus durch vollständige Induktion und $B_0 = S$

$$D(S) = \sum_{k=1}^{i} (a_k + 1)B_0^2 B_1^2 \ldots B_{k-1}^2 + B_0^2 B_1^2 \ldots B_{i-1}^2 D(B_i) \quad i \geq 1.$$

Nun gilt $v(B_i) < 0$ und damit aufgrund der Definition von D auch $v(D(B_i)) < 0$ für $i \geq 0$. Mit der obigen Eigenschaft folgt

$$v(D(B_i)) = v(B_i^2) + v(a_{i+1} + 1 + D(B_{i+1}))$$

und wir unterscheiden zwei Fälle.

Wenn unendlich viele der $a_i = 0$ sind, dann ist unendlich oft

$$v(D(B_i)) = v(B_i^2)$$

und damit gilt

$$v(B_0^2 B_1^2 \dots B_{i-1}^2 D(B_i)) \longrightarrow \infty \quad \text{für} \quad i \longrightarrow \infty$$

oder mit der von v induzierten topologischen Struktur von $\mathbb{F}_2((x^{-1}))$

$$\lim_{i \longrightarrow \infty} B_0^2 B_1^2 \dots B_{i-1}^2 D(B_i) = 0.$$

Im zweiten Fall gibt es also einen Index j mit $a_i = 1$ für $i \geq j$. Weiters gilt $B_{j-1} = [0; x+1, x+1, \dots]$ und daraus folgt

$$B_{j-1} = \frac{1}{x + 1 + B_{j-1}}$$

oder umgeformt

$$B_{j-1}^2 + (x+1)B_{j-1} + 1 = 0 = x^{-1} D(B_{j-1}),$$

also $D(B_{j-1}) = 0$ und damit sofort $D(B_i) = 0, i \geq j$.

Also gilt auch in diesem Fall

$$\lim_{i \longrightarrow \infty} B_0^2 B_1^2 \dots B_{i-1}^2 D(B_i) = 0.$$

Insgesamt erhalten wir die Darstellung

$$D(S) = \sum_{k=1}^{\infty} (a_k + 1) B_0^2 B_1^2 \dots B_{k-1}^2 = \left(\sum_{k=1}^{\infty} (a_k + 1) B_0 B_1 \dots B_{k-1} \right)^2 =: U^2,$$

wobei $v(U) < 0$ ist. Die Definition von S eingesetzt und umgeformt liefert

$$S^2 + (x+1)S + 1 = xU^2.$$

Vergleicht man den Koeffizienten von x^0 so erhält man $s_1 = 1$ und die Koeffizienten von x^{-2i} liefern $s_{2i+1} = s_{2i} + s_i, i \geq 1$.

Sei nun umgekehrt eine Folge in $\mathbb{F}_2$ gegeben, die $s_1 = 1$ und $s_{2i+1} = s_{2i} + s_i, i \geq 1$ erfüllt. Aufgrund dieser Eigenschaft erhält man für die erzeugende Funktion S ein $U \in \mathbb{F}_2((x^{-1})), v(U) < 0$ mit

$$S^2 + (x+1)S + 1 = xU^2.$$

Angenommen S wäre entweder rational oder es gilt $\operatorname{grad}(A_i) > 1$ für ein $i \geq 1$. Dann gibt es ein $i \geq 1$ mit

$$v(Q_iS - P_i) < -v(Q_i) - 1.$$

Wir betrachten

$$\begin{aligned}
&v(Q_i^2S^2 - P_i^2) = v((Q_iS - P_i)^2) < 0,\\
&v((x+1)Q_i(Q_iS - P_i)) = 1 + v(Q_i) + v(Q_i - P_i) < 0
\end{aligned}$$

und deshalb gilt für

$$T := P_i^2 + (x+1)P_iQ_i + Q_i^2 + xU^2Q_i^2 = Q_i^2S^2 - P_i^2(x+1)Q_i(Q_iS - P_i),$$

dass $v(T) < 0$ ist.

Wir bezeichnen das konstante Glied von P_i bzw. Q_i mit a bzw. b. Durch betrachten des konstanten Gliedes von T, dass ja 0 sein muss, folgt $a+ab+b = 0$. Diese Gleichung hat in $\mathbb{F}_2$ nur die Lösung $a = b = 0$. Dies ist aber ein Widerspruch zu $\operatorname{ggT}(P_i, Q_i) = 1$.

Damit ist S irrational und es gilt $\operatorname{grad}(A_i) = 1, i \geq 1$ und die Behauptung folgt aus Satz 2.7.2. ■

2.8 Fast perfektes lineares Komplexitätsprofil

Wir haben Folgen mit PLKP betrachtet, weil diese das typische Verhalten von Zufallsfolgen besitzen. Der Satz von Wang und Massey lehrt uns aber, dass Folgen mit PLKP im praktisch wichtigsten Fall eine vorhersehbare Struktur besitzen.

PLKP ist also eine zu starke Forderung und soll im Folgenden abgeschwächt werden.

Wir beginnen mit einer einfachen Folgerung aus dem Satz 2.3.1.

Folgerung 2.8.1 *Sei $(s_i)_{i\geq 1}$ eine Folge in K und $n \in \mathbb{N}$. Weiters sei $i \geq 0$ jener Index für den gilt*

$$\operatorname{grad}(Q_{i-1}) + \operatorname{grad}(Q_i) \leq n < \operatorname{grad}(Q_i) + \operatorname{grad}(Q_{i+1}).$$

Mit der zusätzlichen Definition $\operatorname{grad}(A_0) = -1$ *gilt*

$$\frac{n+1}{2} - \frac{1}{2}\operatorname{grad}(A_{i+1}) \leq L_n \leq \frac{n}{2} + \frac{1}{2}\operatorname{grad}(A_i).$$

Beweis. Zunächst folgt sofort aus der Voraussetzung

$$2\operatorname{grad}(Q_i) - \operatorname{grad}(A_i) \leq n \leq 2\operatorname{grad}(Q_i) + \operatorname{grad}(A_{i+1}) - 1,$$

wobei der Fall $i = 0$ wegen der Zusatzdefinition richtig ist. Umformen ergibt

$$\frac{n+1}{2} - \frac{1}{2}\operatorname{grad}(A_{i+1}) \leq \operatorname{grad}(Q_i) \leq \frac{n}{2} + \frac{1}{2}\operatorname{grad}(A_i)$$

und wegen Satz 2.3.1 erhält man daraus die Behauptung. ∎

Wir führen eine äußerst praktische Größe ein.

Definition 2.8.2 Sei $(s_i)_{i\geq 1}$ eine Folge in K mit irrationaler erzeugenden Funktion S. Weiters sei $S = [0; A_1, A_2, \ldots]$ die Kettenbruchentwicklung von S. Dann bezeichnen wir mit

$$K(S) = \sup_{i\geq 1} \operatorname{grad}(A_i).$$

Damit lässt sich Satz 2.7.2 auch so formulieren: Eine Folge besitzt PLKP dann und nur dann, wenn die erzeugende Funktion S irrational ist und $K(S) = 1$.

Mit dieser neuen Größe erhalten wir eine wichtige Abschätzung des Komplexitätsprofils.

Satz 2.8.3 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit irrationaler erzeugenden Funktion S (oder äquivalent dazu keine Schieberegisterfolge). Dann gilt für das lineare Komplexitätsprofil*

$$\frac{1}{2}(n+1-K(S)) \leq n \leq \frac{1}{2}(n+K(S)) \quad \text{für} \quad n \geq 1.$$

Beweis. Folgt sofort aus Folgerung 2.8.1 und der Definition von $K(S)$. ∎

Wenn wir die Menge aller Folgen mit irrationaler erzeugenden Funktion unterteilen in Klassen mit demselben $K(S)$, dann erhalten wir für jede Klasse dieselben Abschätzungen für das Komplexitätsprofil. In dieser Abschätzung kommt $K(S)$ vor. Die Frage ist, ob man die Abschätzung für eine Klasse verbessern kann, in dem Sinn, dass man $K(S)$ durch eine kleinere, für die Klasse feste Zahl, ersetzt.

Eine Verbesserung ist für die Klassen mit $K(S) < \infty$ nicht möglich. Dazu wählen wir ein $i \geq 1$ mit $\mathrm{grad}(A_i) = K(S)$ und setzen $n = \mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i)$. Durch nachrechnen erhält man, dass dafür die obere Schranke angenommen wird. Weiters setzen wir nochmal $\mathrm{grad}(A_i) = K(S)$ mit $i \geq 1$ bzw. im Fall $K(S) = 1$ setzen wir $i = 2$. Diesmal wählen wir $n = \mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) - 1 \geq 1$. Damit wird die untere Schranke angenommen.

Daraus sieht man, dass auch für keine Teilmenge einer Klasse eine Verbesserung möglich ist.

Der Satz 2.8.3 gibt uns die Möglichkeit Folgen zu konstruieren, bei denen die n-te Komplexität etwas um den Erwartungswert $\frac{n}{2}$ schwankt.

Rueppel hat gezeigt, dass für binäre Zufallsfolgen die Standardabweichung der n-ten Komplexität asymptotisch gleich $\frac{1}{9}\sqrt{81} = 1.03\ldots$ ist (siehe [20]). Wir haben schon gesehen, dass Folgen mit PLKP für unsere Anwendungszwecke ungeeignet sind. Wir werden also die Forderung etwas lockern und auch Schwankungen um den Erwartungswert zulassen, die dem asymptotischen Verhalten entsprechen.

Um solche Folgen zu konstruieren, zeigt uns der Satz 2.8.3, dass $K(S) = 2$ und $K(S) = 3$ eine gute Wahl ist. Die Konstruktion erfolgt mit der Methode aus Unterabschnitt 4 dieses Kapitels. Man sagt, dass diese Folgen ein *fast perfektes lineares Komplexitätsprofil* besitzen.

2.9 Das stochastische Modell

In den nun folgenden Unterabschnitten beschränken wir uns auf endliche Körper. Es sei also ab jetzt

$$K = \mathbb{F}_q \quad \text{mit} \quad q = p^t, p \in \mathbb{P}, t \in \mathbb{N}.$$

In den letzten beiden Unterabschnitten haben wir für festes $n \in \mathbb{N}$ die n-te Komplexität L_n als Zufallsvariable betrachtet. Mit den stochastischen Eigenschaften dieser Zufallsvariable konnten wir Folgen konstruieren, die ein typisch zufälliges Verhalten aufweisen.

Jetzt wollen wir die Folge der Zufallsvariablen $(L_n)_{n\geq 1}$ betrachten und insbesondere Eigenschaften für $n \longrightarrow \infty$ studieren. Dazu benötigen wir wieder ein passendes stochastisches Modell.

Mit H bezeichnen wir die Menge aller erzeugenden Funktionen von Folgen

aus K, also
$$H = \{S \in K((x^{-1}))|v(S) < 0\}.$$
Schränkt man die Metrik, die durch v induziert wird auf H ein, so sieht man leicht, dass man einen kompakten metrischen Raum erhält. Weiters ist H mit der Addition eine abelsche Untergruppe von $K((x^{-1}))$. Betrachtet man noch zusätzlich die topologische Struktur von H, dann erhält man eine kompakte abelsche Gruppe. Damit existiert auf dem Messraum $(H, \mathfrak{B})$, wobei $\mathfrak{B}$ die σ-Algebra der Borelschen Mengen in H ist, ein eindeutig bestimmtes Haarmaß h d.h., ein eindeutig bestimmtes translationsinvariantes Wahrscheinlichkeitsmaß. Dieser Wahrscheinlichkeitsraum $(H, \mathfrak{B}, h)$ soll im Folgenden als stochastisches Modell dienen.

Beschreibt dieses Modell unsere Vorstellung von Zufälligkeit? Von einer Zufallsfolge wird man verlangen, dass für ein Folgenglied jeder Wert aus $\mathbb{F}_q$ gleichwahrscheinlich ist. Also wird man von der Gleichverteilung in $\mathbb{F}_q$ ausgehen und damit jedem Element in $\mathbb{F}_q$ die Wahrscheinlichkeit $\frac{1}{q}$ zuordnen. Die Wahrscheinlichkeitstheorie lehrt uns, dass für die Zufälligkeit von Folgen, der unendliche Produktraum dieses Laplaceraumes ein passendes stochastisches Modell ist. Man sieht leicht, dass dieser Wahrscheinlichkeitsraum auf den Folgen, den Wahrscheinlichkeitsraum $(H, \mathfrak{B}, h)$ auf der Menge der erzeugenden Funktionen induziert. Damit ist die Verwendung von $(H, \mathfrak{B}, h)$ als stochastisches Modell motiviert.

Wir wollen zunächst einige interessante Eigenschaften des Wahrscheinlichkeitsraumes $(H, \mathfrak{B}, h)$ herleiten.

Es sei
$$D(S_0; r) := \{S \in H|v(S - S_0) < -r\} \quad \text{mit} \quad S_0 \in H, r \geq 0$$
eine Kreisscheibe um S_0. Aus der Translationsinvarianz von h folgt sofort
$$h(D(S_0; r)) = q^{-r}.$$
Wir führen noch einige Bezeichnungen ein. P sei die Menge aller Polynome in $\mathbb{F}_q$ vom Grad ≥ 1. Weiters bezeichnen wir für ein $S \in H$ die Teilnenner A_i der Kettenbruchentwicklung bzw. die Zähler und Nenner des i-ten Näherungsbruches P_i und Q_i mit $A_i(S)$ bzw. $P_i(S)$ und $Q_i(S)$. Außerdem die n-te lineare Komplexität der erzeugten Folge mit $L_n(S)$.

Wir berechnen nun die Wahrscheinlichkeit einer wichtigen Menge.

Hilfssatz 2.9.1 *Seien $A_1, A_2, \ldots, A_k \in P$ gegeben und wir betrachten die Menge*
$$R(A_1, A_2, \ldots, A_k) := \{S \in H|A_i(S) = A_i \quad \text{für} \quad 1 \leq i \leq k\}.$$

Dann gilt

$$h(R(A_1, A_2, \ldots, A_k)) = q^{-2(\mathrm{grad}(A_1) + \mathrm{grad}(A_2) + \ldots + \mathrm{grad}(A_k))}.$$

Beweis. Seien P_k und Q_k Zähler und Nenner des k-ten Näherungsbruches von $[0; A_1, A_2, \ldots, A_k]$. Dann gilt für $S \in R(A_1, A_2, \ldots, A_k)$

$$v\left(S - \frac{P_k}{Q_k}\right) = -2v(Q_k) - v(A_{k+1}(S)) < -2v(Q_k)$$

und damit $R(A_1, A_2, \ldots, A_k) \subseteq D(\frac{P_k}{Q_k}; -2v(Q_k))$.

Wenn nun umgekehrt $S \in D(\frac{P_k}{Q_k}; -2v(Q_k))$, dann gibt es wegen Hilfssatz 1.5.3 und Satz 1.5.4 ein $a \in \mathbb{F}_q, a \neq 0$, mit $P_k = aP_i(S)$ und $Q_k = aQ_i(S)$ für passendes $i \geq 0$. Daraus folgt

$$[0; A_1, A_2, \ldots, A_k] = \frac{P_k}{Q_k} = \frac{P_i(S)}{Q_i(S)} = [A_0(S); A_1(S), \ldots, A_i(S)]$$

und wegen der Eindeutigkeit der Kettenbruchentwicklung $S \in R(A_1, A_2, \ldots, A_k)$.

Insgesamt erhalten wir also $R(A_1, A_2, \ldots, A_k) = D(\frac{P_k}{Q_k}, -2v(Q_k))$. Aus dem vorher berechneten Wert für Kreisscheiben und aus Satz 1.2.7 (3) folgt sofort die Behauptung. ∎

Wir kommen nun zum Begriff der maßerhaltenden Abbildung.

Definition 2.9.2 Sei $(\Omega, \mathfrak{A}, W)$ ein Wahrscheinlichkeitsraum und X eine Zufallsvariable auf $(\Omega, \mathfrak{A}, W)$ in $(\Omega, \mathfrak{A})$ mit Verteilung W. Dann heißt X eine *maßerhaltende Abbildung.*

Wir definieren nun ein Abbildung von H in H wie folgt

$$T(S) = S^{-1} - E(S^{-1}) \quad \text{für} \quad S \in H, S \neq 0$$

und T(0)=0.

Für diese Abbildung gilt

Hilfssatz 2.9.3 *T ist eine maßerhaltende Abbildung.*

Beweis. Wir müssen zeigen, dass T eine Zufallsvariable ist, die die Verteilung h besitzt, also $\forall B \in \mathfrak{B}$ soll $T^{-1}(B) \in \mathfrak{B}$ sein und $h(T^{-1}(B)) = h(B)$. Es genügt diese Eigenschaften für Kreisscheiben nachzurechnen.

Sei also $D := D(S_0; r)$ eine Kreisscheibe mit $S_0 \in H$ und $r \geq 1$. Zunächst gilt für $S \in H, S \neq 0$, dass $S \in T^{-1}(D)$ dann und nur dann, wenn es ein $p \in P$ gibt mit $v(S^{-1} - S_0 - p) < -r$. Wenn die zweite Bedingung gilt, dann muss $v(S^{-1}) = v(S_0 + p)$ sein und damit sieht man sofort, dass bei festem $p \in P$, die zweite Bedingung dann und nur dann gilt, wenn $S \in D((S_0 + p)^{-1}; r + 2v(p))$ ist.

Damit haben wir gezeigt, dass

$$T^{-1}(D)\backslash\{0\} = \left(\bigcup_{p \in P} D((S_0 + p)^{-1}; r + 2v(p)) \right) \backslash\{0\}$$

und insbesondere $T^{-1}(D) \in \mathfrak{B}$. Weiters gilt, wegen $h(\{0\}) = 0$, dass

$$h(T^{-1}(D)) = h\left(\bigcup_{p \in P} D((S_0 + p)^{-1}; r + 2v(p)) \right).$$

Wir wollen uns jetzt überlegen, dass die obige Vereinigung, eine Vereinigung von disjunkten Mengen ist. Dazu betrachten wir $W_1 = S_0 + p_1, W_2 = S_0 + p_2$ mit $p_1, p_2 \in P, p_1 \neq p_2$ und nehmen indirekt an, dass $D(W_1^{-1}; r + 2v(p_1)) \cap D(W_2^{-1}; r + 2v(p_2)) \neq 0$ ist. Es gilt $v(p_1) = v(W_1), v(p_2) = v(W_2)$ und wegen der Annahme erhält man sofort

$$v(W_1^{-1} - W_2^{-1}) < -r - 2\min(v(W_1), v(W_2)).$$

Andererseits gilt

$$v(W_1^{-1} - W_2^{-1}) = v(W_1 - W_2) - v(W_1) - v(W_2) \geq -2\min(v(W_1), v(W_2)),$$

wobei man diese Aussage durch betrachten von $v(W_1) = v(W_2)$ und $v(W_1) \neq v(W_2)$ sofort erhält. Damit hat man aber einen Widerspruch und die Mengen sind tatsächlich disjunkt.

Daraus erhält man schließlich

$$\begin{aligned} h(T^{-1}(D)) &= h\left(\bigcup_{p \in P} D((S_0 + p)^{-1}; r + 2v(p)) \right) \\ &= \sum_{p \in P} h(D((S_0 + p)^{-1}; r + 2v(p))) \\ &= \sum_{p \in P} q^{-r-2v(p)} \\ &= \sum_{d=1}^{\infty} (q-1) q^d q^{-r-2d} = q^{-r} = h(D), \end{aligned}$$

womit die Behauptung bewiesen wäre. ■

2.10 Grenzwertsätze für Kettenbrüche

Wir beginnen mit einer wichtigen Sprechweise. Eine Eigenschaft soll *h-fast-sicher* gelten (in Zeichen $[h]$), wenn die Menge aller $S \in H$, die diese Eigenschaft besitzen, Wahrscheinlichkeit 1 hat.

Weiters sei erwähnt, dass die Menge der rationalen $S \in H$ Wahrscheinlichkeit 0 besitzt.

Es gilt der folgende sehr wichtige Hilfssatz.

Hilfssatz 2.10.1 *Sei g eine reellwertige Funktion auf P. Wir definieren für $i \geq 1$ die Abbildung $X_i(S) = g(A_i(S))$. Dann ist $(X_i)_{i\geq 1}$ eine unabhängige, identisch verteilte Folge von Zufallsvariablen auf $(H, \mathfrak{B}, h)$.*

Beweis. Die Funktion X_i ist eigentlich nur für irrationale S definiert. Die rationalen Elemente von H haben, wie schon erwähnt, Wahrscheinlichkeit 0 und damit kann die Funktion für rationales S irgendwie definiert werden. Wir setzen $X_i(S) = 0, i \geq 1$ für rationales S.

Es gilt für irrationales S und $i \geq 1$

$$X_i(S) = g(A_i(S)) = g(A_1(B_{i-1}(S))) = X_1(B_{i-1}(S)) = X_1(T^{i-1}(S))$$

und damit $X_i = X_1 \circ T^{i-1}$, wobei die Gültigkeit für rationales S trivial ist. Da wegen Hilfssatz 2.9.3 T maßerhaltend ist folgt, dass die Zufallsvariablen identisch verteilt sind.

Um zu zeigen, dass die Folge $(X_i)_{i\geq 1}$ unabhängig ist, muss man nur zeigen, dass die ersten k Zufallsvariablen unabhängig sind. Weiters ist offensichtlich, dass diese unabhängig sind, wenn die Ereignisse $A_1(S) = A_1, A_2(S) = A_2, \ldots, A_k(S) = A_k$, für $A_1, A_2, \ldots, A_k$ Polynome aus P, unabhängig sind. Dies ist mit Hilfssatz 2.9.1 sofort klar. ■

Auf diese Folge von identisch verteilten und unabhängigen Zufallsvariablen kann man die klassischen Sätze der Wahrscheinlichkeitstheorie anwenden und erhält eine Reihe von neuen Aussagen.

Wir beginnen mit dem starken Gesetz der großen Zahlen.

Satz 2.10.2 **(Starkes Gesetz der großen Zahlen für Kettenbrüche)** *Sei g eine reellwertige Funktion auf P, für die die Reihe $\sum_{p\in P} |g(p)| q^{-2\mathrm{grad}(p)}$*

konvergiert. Dann gilt

$$\lim_{n \longrightarrow \infty} \frac{1}{n} \sum_{i=1}^{n} g(A_i(S)) = \sum_{p \in P} g(p) q^{-2\mathrm{grad}(p)} \qquad [h].$$

Beweis. Wir definieren die Zufallsvariablen wie in Hilfssatz 2.10.1. Diese sind unabhängig, identisch verteilt und es gilt für das erste Moment

$$\int_H |X_1| dh = \sum_{p \in P} |g(p)| q^{-2\mathrm{grad}(p)}$$

und damit folgt die Existenz aus der Voraussetzung über g. Wir können das starke Gesetz der großen Zahlen, etwa in der Form von [2] Satz 12.2, anwenden und erhalten die Behauptung. ■

Durch Wahl eines speziellen g erhalten wir

Folgerung 2.10.3 *Es gilt*

$$\lim_{n \longrightarrow \infty} \frac{\mathrm{grad}(Q_n(S))}{n} = \frac{q}{q-1} \qquad [h].$$

Beweis. Wir setzen in Satz 2.10.2 $g(p) = \mathrm{grad}(p), p \in P$. Dann gilt

$$\sum_{p \in P} g(p) q^{-2\mathrm{grad}(p)} = \sum_{d=1}^{\infty} (q-1) q^d d q^{-2d} = \frac{q}{q-1}$$

und damit folgt zusammen mit Satz 1.2.7 (3) die Behauptung. ■

Wir wenden noch einmal das starke Gesetz der großen Zahlen an.

Satz 2.10.4 *Sei A ein Polynom in P. Dann gilt* $[h]$

$$\lim_{n \longrightarrow \infty} \frac{1}{n} |\{1 \leq i \leq n | A_i(S) = A\}| = q^{-2\mathrm{grad}(A)}.$$

Beweis. Diesmal wählen wir in Hilfssatz 2.10.1 als g die charakteristische Funktion der einelementigen Menge $\{A\}$. Damit erhalten wir für den Erwartungswert der Zufallsvariablen wegen Hilfssatz 2.9.1

$$\int_H X_1 dh = q^{-2\mathrm{grad}(A)}$$

und weiters mit dem starken Gesetz der großen Zahlen die Behauptung. ■

Dieser Satz liefert insbesondere die Verteilung der Teilnenner eines Kettenbruches von einer zufälligen erzeugenden Funktion.

Als nächstes wenden wir den Satz vom iterierten Logarithmus auf unsere Folge an.

Satz 2.10.5 (Satz vom iterierten Logarithmus für Kettenbrüche) *Sei g eine nichtkonstante reellwertige Funktion auf P, für die die Reihe $\sum_{p\in P} g(p)^2 q^{-2\mathrm{grad}(p)}$ konvergiert. Weiters sei*

$$E = \sum_{p\in P} g(p) q^{-2\mathrm{grad}(p)}, \quad \sigma = (\sum_{p\in P} g(p)^2 q^{-2\mathrm{grad}(p)} - E^2)^{1/2},$$

dann gilt [h]

$$\limsup_{n\longrightarrow\infty} \frac{1}{\sigma(2n\log\log(n))^{1/2}} (\sum_{i=1}^{n} g(A_i(S)) - nE) = 1,$$
$$\liminf_{n\longrightarrow\infty} \frac{1}{\sigma(2n\log\log(n))^{1/2}} (\sum_{i=1}^{n} g(A_i(S)) - nE) = -1.$$

Beweis. Wir betrachten wieder die Folge von Zufallsvariablen aus dem Hilfssatz 2.10.1. Dann ist E der Erwartungswert und σ die Varianz der Zufallsvariablen und insbesondere existiert wegen der Voraussetzung das zweite Moment und es gilt $\sigma > 0$. Damit können wir das Hartman-Wintersche Gesetz vom iterierten Logarithmus anwenden (siehe etwa [3]) und erhalten die Behauptung. ■

Wieder erhält man durch Spezialisierung von g

Folgerung 2.10.6 *Es gilt* [h]

$$\limsup_{n\longrightarrow\infty} \frac{q-1}{(2qn\log\log(n))^{1/2}} (\mathrm{grad}Q_n(S) - \frac{nq}{q-1}) = 1,$$
$$\liminf_{n\longrightarrow\infty} \frac{q-1}{(2qn\log\log(n))^{1/2}} (\mathrm{grad}Q_n(S) - \frac{nq}{q-1}) = -1.$$

Beweis. Wir setzen im Satz 2.10.5 $g(p) = \mathrm{grad}(p)$. Damit gilt

$$\sum_{p\in P} g(p)^2 q^{-2\mathrm{grad}(p)} = \sum_{d=1}^{\infty} (q-1) q^d d^2 q^{-2d} = \frac{q^2+q}{(q-1)^2}$$

und nach elementarer Rechnung

$$\sigma^2 = \frac{q}{(q-1)^2},$$

wobei E schon in Folgerung 2.10.3 berechnet wurde. Einsetzen liefert die Behauptung. ■

Als nächstes wenden wir den Zentralen Grenzwertsatz auf unsere Folge an.

Satz 2.10.7 (Zentraler Grenzwertsatz für Kettenbrüche) *Seien g, E, σ wie im Satz 2.10.5. Dann gilt für $a, b \in \mathbb{R} \cup \{-\infty, \infty\}$ mit $a < b$*

$$\lim_{n \longrightarrow \infty} h(\{S \in H | a\sigma\sqrt{n} \leq \sum_{i=1}^{n} g(A_i(S)) - nE \leq b\sigma\sqrt{n}\}) = \frac{1}{2\pi} \int_a^b e^{-t^2/2} dt.$$

Beweis. Wir betrachten dieselbe Folge von Zufallsvariablen wie im Beweis von Satz 2.10.5 und wenden den Zentralen Grenzwertsatz aus der Wahrscheinlichkeitstheorie (siehe [19]) an. ■

Wieder können wir g spezialisieren.

Folgerung 2.10.8 *Für $a, b \in \mathbb{R} \cup \{-\infty, \infty\}$ mit $a < b$ gilt*

$$\lim_{n \longrightarrow \infty} h(\{S \in H | a\sqrt{qn} \leq (q-1)\mathrm{grad}(Q_n(S)) - nq \leq b\sqrt{qn}\}) = \frac{1}{2\pi} \int_a^b e^{-t^2/2} dt.$$

Beweis. Definiere g wie in Folgerung 2.10.6. ■

Abschließend wollen wir noch einen Satz für Kettenbrüche zeigen, der sehr ähnlich dem Lemma von Borel-Cantelli ist (siehe [9]).

Satz 2.10.9 (Lemma von Borel-Cantelli für Kettenbrüche) *Sei $f : \mathbb{N} \longrightarrow \mathbb{R}$ eine nichtnegative Funktion. Dann gilt*

1. $\sum_{i=1}^{\infty} q^{-f(i)} < \infty \Longrightarrow$ *es gilt [h], dass $\mathrm{grad}(A_i(S)) \leq f(i)$ für hinreichend großes i,*

2. $\sum_{i=1}^{\infty} q^{-f(i)} = \infty \Longrightarrow$ *es gilt [h], dass $\mathrm{grad}(A_i(S)) > f(i)$ für unendlich viele i.*

Beweis. Es sei $g(i)$ die kleinste ganze Zahl $> f(i)$ für alle $i \geq 1$. Nach Hilfssatz 2.10.1 sind die Ereignisse $\Omega_i = [\mathrm{grad}(A_i(S)) \geq g(i)], i \geq 1$ unabhängig.

Weiters gilt wegen Hilfssatz 2.9.1

$$\begin{aligned} h(\Omega_i) &= \sum_{p \in P, \mathrm{grad}(p) \geq g(i)} q^{-2\mathrm{grad}(p)} \\ &= \sum_{d=\mathrm{grad}(g(i))}^{\infty} (q-1) q^d q^{-2d} = q^{1-g(i)}. \end{aligned}$$

Klarerweise konvergiert die Reihe $\sum_{i=1}^{\infty} q^{-f(i)}$ dann und nur dann, wenn die Reihe $\sum_{i=1}^{\infty} q^{1-g(i)}$ konvergiert und damit folgt die Behauptung aus dem klassischem Lemma von Borel-Cantelli. ■

Als Folgerung erhalten wir

Folgerung 2.10.10 *Es gilt [h]*

$$\limsup_{n \longrightarrow \infty} \frac{\mathrm{grad}(A_i(S))}{\log i} = \frac{1}{\log q}.$$

Beweis. Setzt man $f(i) = (1+\epsilon)\frac{\log i}{\log q}$ dann gilt

$$\sum_{i=1}^{\infty} q^{-f(i)} = \sum_{i=1}^{\infty} i^{-(1+\epsilon)}$$

und diese Reihe divergiert für $\epsilon = 0$ und konvergiert für $\epsilon > 0$. Damit folgt die Behauptung sofort aus Satz 2.10.9. ■

Abschließend wollen wir noch einmal die Folge von unabhängigen und identisch verteilten Zufallsvariablen $(X_i)_{i \geq 1}$ aus Hilfssatz 2.10.1 mit $g = \mathrm{grad}(p)$, $p \in P$ betrachten.

Wir haben schon den Erwartungswert $E = \frac{q}{q-1}$ (siehe Folgerung 2.10.3) und die Varianz $\sigma^2 = \frac{q}{(q-1)^2}$ (siehe Folgerung 2.10.6) berechnet. Weiters nehmen die Zufallsvariablen nur nichtnegative ganze Zahlen als Werte an und aus Hilfssatz 2.9.1 folgt, dass $m \geq 0$ mit der Wahrscheinlichkeit $(q-1)q^{-m}$ angenommen wird. Wir kennen also auch die Verteilung dieser Zufallsvariablen.

Aus dem Unterabschnitt 3 dieses Kapitels wissen wir, dass für ein $S \in H$ die Folge $(X_i(S))_{i \geq 1}$ mit der Sprungkomplexität von der erzeugten Folge von S übereinstimmt.

Zusammenfassend kann das Sprungkomplexitätsprofil einer zufälligen Folge als unabhängige und identisch verteilte Folge von Zufallsvariablen aufgefasst werden, wobei jede Variable den Wert m mit der Wahrscheinlichkeit $(q-1)q^{-m}$ annimmt.

Dies bedeutet insbesondere, dass für das Komplexitätsprofil einer zufälligen Folge, welches nach Folgerung 2.3.2 stets die Form

$$q_0, q_0, \ldots, q_0, q_1, q_1, \ldots, q_1, \ldots, q_i, q_i, \ldots, q_i, \ldots,$$

hat, für die Sprunghöhe $\frac{q}{q-1}$ und für die Anzahl derselben Werte zwischen zwei Sprüngen $\frac{2q}{q-1}$ zu erwarten ist.

Man kann also statistische Tests durchführen, indem man als Nullhypothese annimmt, dass die Folge ist zufällig, also das Sprungkomplexitätsprofil ist eine Folge unabhängiger, identische verteilter Zufallsvariablen, mit der obigen Verteilung. Um zu überprüfen, ob eine Folge wirklich zufällig ist, berechnet man deren Sprungkomplexitätsprofil nach dem Berlekamp-Massey Algorithmus und verwirft die Nullhypothese oder nimmt sie an, je nachdem ob das Verhalten dem zufälligen Verhalten entspricht.

Man kann für diese Tests auch eine andere Folge von Zufallsvariablen wählen, indem man im Hilfssatz 2.10.1 ein anderes g wählt.

Tests basierend auf dieser Idee werden *Kettenbrüche-Tests* genannt und gehen auf Niederreiter [13] zurück.

2.11 Grenzwertsätze für die lineare Komplexität

Aus den Sätzen des vorigen Unterabschnittes und dem Zusammenhang zwischen linearer Komplexität von Folgen und der Kettenbruchentwicklung erhalten wir sofort stochastische Aussagen über das lineare Komplexitätsprofil.

Wir beginnen mit dem folgenden Resultat

Satz 2.11.1 *Es gilt* $[h]$

$$\lim_{n\longrightarrow\infty}\frac{L_n(S)}{n}=\frac{1}{2}.$$

Beweis. Zunächst wählen wir für $S\in H, n\in\mathbb{N}$ jenen Index $i\geq 0$ für den gilt

$$\operatorname{grad}(Q_{i-1}(S))+\operatorname{grad}(Q_i(S))\leq n<\operatorname{grad}(Q_i(S))+\operatorname{grad}(Q_{i+1}(S)).$$

Es folgt dann aus Folgerung 2.8.1 die Ungleichung

$$\left|L_n(S)-\frac{n}{2}\right|\leq\frac{1}{2}\max\{\operatorname{grad}(A_i(S)),\operatorname{grad}(A_{i+1}(S))\}$$

und mit $n\geq L_n(S)=\operatorname{grad}(Q_i(S))$

$$\left|\frac{L_n(S)}{n}-\frac{1}{2}\right|\leq\frac{1}{2}\max(1-\frac{Q_{i-1}}{Q_i},\frac{Q_{i+1}}{Q_i}-1).$$

Wegen Folgerung 2.10.3 gilt $[h]$

$$\lim_{i\longrightarrow\infty}\frac{Q_{i+1}(S)}{Q_i(S)}=\lim_{i\longrightarrow\infty}\frac{Q_{i+1}(S)/(i+1)}{Q_i/i}\frac{i+1}{i}=1$$

und weil für irrationales S mit $n \longrightarrow \infty$ auch $i \longrightarrow \infty$ konvergiert, folgt die Behauptung. ■

Mit anderen Worten gilt für Zufallsfolgen, dass $L_n = o(\frac{n}{2})$. Wir wollen jetzt die Abweichung vom asymptotischen Wert $\frac{n}{2}$ untersuchen.

Satz 2.11.2 *Sei $f : \mathbb{N} \longrightarrow \mathbb{R}$ eine nichtnegative, monoton wachsende Funktion mit $\sum_{i=1}^{\infty} q^{-f(i)} < \infty$. Dann gilt $[h]$*

$$\left| L_n(S) - \frac{n}{2} \right| \leq \frac{1}{2} f(n) \quad \textit{für hinreichend großes } n.$$

Beweis. Aus dem Lemma von Borel-Cantelli für Kettenbrüche folgt, dass $[h]$ gilt, $\mathrm{grad}(A_i(S)) \leq f(i)$ für hinreichend großes i.

Damit gilt $[h]$, wegen der Abschätzung von $L_n(S)$ im Beweis des Satzes 2.11.1,

$$\left| L_n(S) - \frac{n}{2} \right| \leq \frac{1}{2} f(i+1) \quad \text{für hinreichend großes } n.$$

Weiters ist für $i \geq 2$

$$n \geq \mathrm{grad}(Q_{i-1}(S)) + \mathrm{grad}(Q_i)(S) \geq 2i - 1 \geq i + 1$$

und damit $f(i+1) \leq f(n)$, womit die Behauptung bewiesen ist. ■

Satz 2.11.3 *Sei $f : \mathbb{N} \longrightarrow \mathbb{R}$ eine nichtnegative, monoton wachsende Funktion mit $\sum_{i=1}^{\infty} q^{-f(i)} = \infty$. Dann gilt $[h]$*

$$\begin{aligned} L_n(S) &> \frac{n}{2} + \frac{1}{2} f(n) \quad \textit{für unendlich viele } n, \\ L_n(S) &< \frac{n}{2} - \frac{1}{2} f(n) \quad \textit{für unendlich viele } n. \end{aligned}$$

Beweis. Es divergiert auch $\sum_{i=1}^{\infty} q^{-f(5i)}$. Damit folgt aus dem Lemma von Borel-Cantelli für Kettenbrüche, dass $[h]$ gilt, $\mathrm{grad}(A_i(S)) > f(5i)$ für unendliche viele i. Wir wählen so ein S und i.

Wegen Folgerung 2.10.3 können wir voraussetzen, dass dieses S folgende Bedingung erfüllt

$$\lim_{n \longrightarrow \infty} \frac{Q_n(S)}{n} = \frac{q}{q-1}$$

und, wegen $\frac{q}{q-1} < \frac{5}{2}$ folgt weiters

$$\frac{Q_j(S)}{j} < \frac{5}{2} \quad \text{für hinreichend großes } j.$$

Unser i sei auch so groß gewählt, dass obige Eigenschaft gilt.

Wir setzen $n = \text{grad}(Q_{i-1}(S)) + \text{grad}(Q_i(S))$ und betrachten

$$L_n(S) - \frac{n}{2} = \frac{1}{2}\text{grad}(A_i(S)) > \frac{1}{2}f(5i) \geq \frac{1}{2}f(2\text{grad}(Q_i(S))) \geq \frac{1}{2}f(n),$$

womit die erste Behauptung bewiesen wäre.

Die zweite Behauptung folgt im wesentlichen analog, wenn man verwendet, dass [h] gilt, $\text{grad}(A_{i+1}(S)) > f(5i+5)+1$ für unendlich viele i und $n = \text{grad}(Q_i(S)) + \text{grad}(Q_{i+1}(S)) - 1$ setzt. ■

Aus den letzten beiden Sätzen können wir eine wichtige Folgerung ziehen.

Satz 2.11.4 (Satz vom Logarithmus für lineare Komplexität) *Es gilt* [h]

$$\limsup_{n \longrightarrow \infty} \frac{L_n(S) - (n/2)}{\log n} = \frac{1}{2\log q},$$
$$\liminf_{n \longrightarrow \infty} \frac{L_n(S) - (n/2)}{\log n} = -\frac{1}{2\log q}.$$

Beweis. Wir betrachten dieselbe Funktion f wie im Beweis von Folgerung 2.10.10 und wenden die Sätze 2.11.2 und 2.11.3 an. ■

2.12 Pipers Bedingung an die Komplexität

Hat man eine Eigenschaft die [h] gilt, dann kann diese als eine typische Eigenschaft von Zufallsfolgen angesehen werden. Bei der Konstruktion von Pseudozufallsfolgen ist also darauf zu achten, dass diese Eigenschaft erfüllt wird.

Piper (siehe [17]) hat noch eine zusätzliche Forderung gestellt. Wenn $(s_i)_{i\geq 1}$ die konstruierte Folge ist, dann soll nicht nur diese Folge die Eigenschaft besitzen, sondern auch jede geshiftete Folge $(s_i)_{i\geq m+1}, m = 1, \ldots$. Man sagt die Folge besitzt diese Eigenschaft *für jeden Startpunkt.*

Dass diese Forderungen sinnvoll ist, zeigt die folgende Überlegung

Satz 2.12.1 *Sei $\prod$ eine Eigenschaft für Folgen, die* [h] *gilt. Weiters betrachten wir die Menge aller Folgen, die diese Eigenschaft für jeden Startpunkt erfüllen. Dann hat auch diese Menge Wahrscheinlichkeit 1.*

Beweis. Mit P bezeichnen wir die Menge aller Folgen mit der Eigenschaft $\prod$ und mit V alle Folgen, die diese Eigenschaft für jeden Startpunkt erfüllen.

Weiters betrachten wir die folgende Abbildung auf $\mathbb{F}_q^\infty$

$$\tau((s_1, s_2, s_3, \ldots)) = (s_2, s_3, \ldots) \quad \text{für} \quad (s_1, s_2, s_3, \ldots) \in \mathbb{F}_q^\infty .$$

Es gilt $(s_i)_{i \geq m+1} = \tau^m((s_i)_{i \geq 1}), m = 0, 1, \ldots$ und weiters $(s_i)_{i \geq m+1} \in P \Leftrightarrow (s_i)_{i \geq 1} \in \tau^{-m} P$. Wir erhalten also $V = \bigcap_{m=0}^{\infty} \tau^{-m} P$.

Nun ist τ eine maßerhaltende Funktion (siehe dazu [7]) und daraus folgt $h(\tau^{-m} P) = h(P) = 1$ und weiters $h(V) = 1$. ■

Dieses Ergebnis zieht mit den Sätzen aus den vorigen Abschnitten eine Reihe von Folgerungen mit sich. Wir wollen nur ein exemplarisches Beispiel geben.

Satz 2.12.2 *Es gilt* [h]

$$\lim_{n \longrightarrow \infty} \frac{L_n(S_m)}{n} = \frac{1}{2} \quad \text{für m=0,1,\ldots,}$$

Beweis. Folgt aus Satz 2.12.1 und Satz 2.11.1. ■

2.13 Gutes lineares Komplexitätsprofil

Die Definitionen und Sätze der nächsten beiden Unterabschnitte gehen auf Niederreiter [14] zurück.

Wir wollen uns wieder vom Fall, dass K ein endlicher Körper ist lösen und betrachten ab jetzt wieder beliebige Körper.

Für das folgende bezeichnen wir mit $\mathrm{Log}(t) = \max\{1, \log t\}, t \geq 1$.

Wir betrachten jetzt eine Menge von Folgen, die eine für Zufallsfolgen typische Eigenschaft erfüllen. Der Satz 2.10.4 soll dabei als Motivation dienen.

Definition 2.13.1 Sei $(s_i)_{i \geq 1}$ eine Folge in K. Wir sagen die Folge besitzt ein *gutes lineares Komplexitätsprofil (GLKP)*, wenn es eine Konstante C gibt, sodass gilt

$$\left| L_n - \frac{n}{2} \right| \leq C \mathrm{Log}(n) \quad n \geq 1.$$

Im Fall eines endlichen Körpers hat die Menge aller Folgen mit GLKP,wegen Satz 2.11.4 Wahrscheinlichkeit 1.

Wir wollen die Folgen mit GLKP anders charakterisieren. Dazu zeigen wir zunächst

Hilfssatz 2.13.2 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S. Wenn S irrational ist und es ein C gibt mit* $\mathrm{grad}(A_i) \leq CLog(i), i \geq 1$, *dann gilt*

$$\left| L_n - \frac{n}{2} \right| \leq \frac{C}{2}\mathrm{Log}(n) \quad n \geq 1.$$

Beweis. Sei $n \in \mathbb{N}$ und $i \geq 0$ jener Index mit

$$\mathrm{grad}(Q_{i-1}) + \mathrm{grad}(Q_i) \leq n < \mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i+1}).$$

Mit Hilfssatz 2.8.1 erhalten wir

$$\left| L_n - \frac{n}{2} \right| \leq \frac{1}{2}\max\{\mathrm{grad}(A_i), \mathrm{grad}(A_{i+1})\} \leq \frac{C}{2}\mathrm{Log}(i+1).$$

Im Fall $i = 0$ und $i = 1$ gilt

$$\mathrm{Log}(i+1) = 1 \leq \mathrm{Log}(n)$$

und im Fall $i \geq 2$

$$\mathrm{Log}(i+1) \leq \mathrm{Log}(\mathrm{grad}(Q_i) + 1) \leq \mathrm{Log}(\mathrm{grad}(Q_i) + \mathrm{grad}(Q_{i-1})) \leq \mathrm{Log}(n),$$

also insgesamt die Behauptung. ■

Weiters zeigen wir

Hilfssatz 2.13.3 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S. Weiters gelte*

$$\left| L_n - \frac{n}{2} \right| \leq C\mathrm{Log}(n) \quad n \geq 1,$$

mit einem $C \geq 1$. Dann ist S irrational und es gilt

$$\mathrm{grad}(A_i) < (4C\mathrm{Log}(C) + 8C)\mathrm{Log}(i) \quad i \geq 1.$$

Beweis. Zunächst folgt aus der Voraussetzung

$$\lim_{n \longrightarrow \infty} L_n = \infty$$

und damit ist S irrational.

Um die zweite Behauptung zu zeigen, nehmen wir an, dass sie falsch sei. Weiters bezeichne i den kleinsten Index für den sie nicht gilt.

Als erstes betrachten wir den Fall $i = 1$. Dann gilt

$$\operatorname{grad}(A_1) \geq 4C\operatorname{Log}(C) + 8C.$$

Es sei $n = \operatorname{grad}(A_1) - 1$ und damit gilt

$$n \geq 4C\operatorname{Log}(C) + 7C \geq e.$$

Wegen $L_n = 0$ und da die Funktion $t/\log(t)$ für $t \geq e$ monoton wachsend ist, gilt

$$\left| L_n - \frac{n}{2} \right| = \frac{n}{2} = \frac{n}{2\log(n)} \log(n) \geq \frac{4C\operatorname{Log}(C) + 7C}{2\log(4C\operatorname{Log}(C) + 7C)} \log(n).$$

Durch getrennte Betrachtung der beiden Fälle $1 \leq C \leq e$ und $C > e$ zeigt man sofort, dass

$$4\operatorname{Log}(C) + 7 > 2\log(4C\operatorname{Log}(C) + 7C) \quad C \geq 1$$

und damit folgt

$$\left| L_n - \frac{n}{2} \right| > C\operatorname{Log}(n),$$

was ein Widerspruch zur Voraussetzung ist.

Sei also nun $i \geq 2$. Wir setzen zur Akürzung

$$C_1 = 4C\operatorname{Log}(C) + 8C.$$

Es gilt nach Voraussetzung $\operatorname{grad}(A_j) < C_1\operatorname{Log}(j), 1 \leq j < i$ und wegen Satz 1.2.7 (3)

$$\begin{aligned} \log\operatorname{grad}(Q_i) &< \log(\operatorname{grad}(A_i) + C_1 \sum_{j=1}^{i-1} \operatorname{Log}(j)) \\ &\leq \log(\operatorname{grad}(A_i) + C_1(i-1)\operatorname{Log}(i)). \end{aligned}$$

Weiters ist die Funktion $t^{-1}\log(t + C_1(i-1)\operatorname{Log}(i))$ monoton fallend für $t \geq e$ und $\operatorname{grad}(A_i) \geq C_1\operatorname{Log}(i)$, woraus folgt

$$\log\operatorname{grad}(Q_i) < \frac{\log(C_1 i \operatorname{Log}(i))}{C_1\operatorname{Log}(i)} \operatorname{grad}(A_i).$$

Wir setzen $n = \operatorname{grad}(Q_{i-1}) + \operatorname{grad}(Q_i)$ und erhalten

$$\begin{aligned} \left| L_n - \frac{n}{2} \right| &= \left|\operatorname{grad}(Q_i) - \frac{1}{2}(\operatorname{grad}(Q_{i-1}) + \operatorname{grad}(Q_i))\right| \\ &= \frac{1}{2}\operatorname{grad}(A_i) \\ &> \frac{C_1\operatorname{Log}(i)}{2\log(C_1 i\operatorname{Log}(i))} \log\operatorname{grad}(Q_i) \\ &> \frac{C_1\operatorname{Log}(i)}{2\log(C_1 i\operatorname{Log}(i))} \log\frac{n}{2}. \end{aligned}$$

Weiters gilt

$$n \geq \mathrm{grad}(A_i) + 2\mathrm{grad}(A_{i-1}) \geq C_1 \mathrm{Log}(i) + 2$$

und damit

$$\left| L_n - \frac{n}{2} \right| > \frac{C_1 \mathrm{Log}(i)}{2\log(C_1 i \mathrm{Log}(i))}(1 - \frac{\log(2)}{\log(C_1 \mathrm{Log}(i) + 2)}) \log(n).$$

Um also zum Widerspruch $|L_n - (n/2)| > C\mathrm{Log}(n)$ zu kommen, müssen wir zeigen

$$(2\mathrm{Log}(C) + 4)(1 - \frac{\log(2)}{\log(C_1 \mathrm{Log}(i) + 2)}) \geq \frac{\log(C_1 i \mathrm{Log}(i))}{\mathrm{Log}(i)}.$$

Dazu betrachten wir zunächst den Fall $i = 2$. Dann erhalten wir die folgende, einfachere Form

$$(2\mathrm{Log}(C) + 4)(1 - \frac{\log(2)}{\log(C_1 + 2)}) \geq \log(2C_1).$$

Wir betrachten

$$\begin{aligned} (2\mathrm{Log}(C) + 4)(1 - \frac{\log(2)}{\log(C_1 + 2)}) &\geq (2\mathrm{Log}(C) + 4)(1 - \frac{\log(2)}{\log(14)}) \\ &> (1.47)\mathrm{Log}(C) + 2.94. \end{aligned}$$

Wenn $1 \leq C \leq e$ ist, erhalten wir die Aussage mit

$$\begin{aligned} (2\mathrm{Log}(C) + 4)(1 - \frac{\log(2)}{\log(C_1 + 2)}) &> 4.41 > \log(24e) \\ &\geq \log(24C) = \log(2C_1). \end{aligned}$$

Die Funktion $(0.47)t - \log(t+2)$ ist monoton wachsend für $t \geq 1$ und damit gilt

$$(0.47)t + 0.86 > \log(t + 2) \quad t \geq 1,$$

sowie durch einsetzen

$$(0.47)\log(C) + 0.86 > \log(\log(C) + 2) \quad C \geq e.$$

Daraus folgt für $C \geq e$ die Aussage durch

$$(1.47)\log(C) + 2.94 > \log(C) + \log(8) + \log(\log(C) + 2) = \log(2C_1).$$

Bleibt also noch der Fall $i \geq 3$. Zunächst gilt

$$1 - \frac{\log(2)}{\log(C_1 \mathrm{Log}(i) + 2)} \geq 1 - \frac{\log(2)}{\log(12\log(3) + 2)} > 0.74.$$

Weil die Funktion $\log(C_1 t \log(t))/\log(t)$ für $t \geq e$ monoton fallend ist, haben wir die Behauptung in diesem Fall bewiesen, wenn

$$(1.48)\mathrm{Log}(C) + 2.96 \geq \frac{\log(3C_1\log(3))}{\log(3)}.$$

Im Fall $1 \leq C \leq e$ folgt diese Ungleichung aus

$$(1.48)\mathrm{Log}(C) + 2.96 = 4.44 > \frac{\log(36e\log(3))}{\log(3)} \geq \frac{\log(3C_1\log(3))}{\log(3)}.$$

Die Funktion $(0.62)t - \log(t+2)$ ist monoton wachsend für $t \geq 1$ und damit gilt

$$(0.62)t + 0.67 > \log(t+2) \quad t \geq 1,$$

sowie durch einsetzen

$$(0.62)\log(C) + 0.67 > \log(\log(C) + 2) \quad C \geq e.$$

Addiert man $\log(C) + \log(12\log(3))$ auf beiden Seiten und dividiert man durch $\log(3)$, dann erhält man die Behauptung.

Damit ist der Beweis der Aussage erbracht. ■

Wenn man die letzten beiden Hilfssätze zusammenfasst, erhält man die folgende Charakterisierung von Folgen mit GLKP.

Satz 2.13.4 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit erzeugenden Funktion S. Genau dann besitzt die Folge GLKP, wenn gilt, dass S irrational ist und es ein C gibt mit* $\mathrm{grad}(A_i) \leq C\mathrm{Log}(i), i \geq 1$.

Beweis. Folgt aus Hilfssatz 2.13.2 und 2.13.3. ■

Als nächstes wollen wir zeigen, dass Folgen mit GLKP diese Eigenschaft schon für jeden Startpunkt besitzen. Dazu zunächst einige Hilfsergebnisse

Hilfssatz 2.13.5 *Sei $S \in K((x^{-1}))$ und $f, g \in K[x], f \neq 0$. Dann folgt aus $v(fS - g) < -v(f)$, dass es ein $i \geq 0$ und ein $D \in K[x], D \neq 0$ gibt, mit $f = DQ_i$ und $g = DP_i$.*

Beweis. Zunächst sei $f = D'f'$ und $g = D'g'$ mit $(f', g') = 1$. Wir betrachten

$$v\left(S - \frac{g'}{f'}\right) = -v(f') + v(f'S - g') = -v(f') + v(fS - g) - v(D') < -2v(f').$$

Damit folgt aus Hilfssatz 1.5.3 und Satz 1.5.4, dass es ein $a \in K, a \neq 0$ gibt, sodass $f' = aQ_i$ und $g' = aP_i$ für $i \geq 0$. Setzt man $D = D'a$ dann folgt die Behauptung. ■

Hilfssatz 2.13.6 *Sei $S \in K((x^{-1}))$ und $f, g \in K[x], fg \neq 0$. Weiters sei $\frac{f}{g}S = [A'_0; A'_1, A'_2, \ldots]$ und mit P'_i/Q'_i bezeichnen wir den i-ten Näherungsbruch von $\frac{f}{g}S$. Gilt dann für ein $i \geq 1$, dass $v(A'_i) > v(f) + v(g)$, dann gibt es ein $j \geq 1$ mit $v(A'_i) \leq v(A_j) + v(f) + v(g)$ und $v(Q_{j-1}) \leq v(Q'_{i-1}) + v(f)$.*

Beweis. Wenn $v(A'_i) = \infty$ ist, dann ist die Aussage trivial.

Wir können also $v(A'_i) < \infty$ voraussetzen und betrachten

$$\begin{aligned} v(Q'_{i-1}fS - P'_{i-1}g) &= v(g) + v\left(Q'_{i-1}\frac{f}{g}S - P'_{i-1}\right) \\ &= v(g) - v(Q'_i) \\ &< v(g) - v(A'_i) - v(Q'_{i-1}) \\ &< -v(f) - v(Q'_{i-1}) = -v(fQ'_{i-1}). \end{aligned}$$

Damit können wir Hilfssatz 2.13.5 anwenden und es gibt ein $D \in K[x], D \neq 0$ und ein $j \geq 1$, mit $fQ'_{i-1} = DQ_{j-1}$ und $gP'_{i-1} = DP_{j-1}$.

Wir erhalten

$$v(Q_{j-1}) \leq v(DQ_{j-1}) = v(fQ'_{i-1}) = v(Q'_{i-1}) + v(f),$$

sowie

$$\begin{aligned} v(A'_i) &\leq v(A'_i) - v(Q_{j-1}) + v(Q'_{i-1}) + v(f) \\ &= -v(Q_{j-1}) - v(fQ'_{i-1}S - gP'_{i-1}) + v(f) + v(g) \\ &= -v(Q_{j-1}) - v(DQ_{j-1}S - DP_{j-1}) + v(f) + v(g) \\ &\leq -v(Q_{j-1}) - v(Q_{j-1}S - P_{j-1}) + v(f) + v(g) = v(A_j) + v(f) + v(g), \end{aligned}$$

wie es behauptet war. ■

Mit diesen beiden Hilfssätzen können wir zeigen

Satz 2.13.7 *Sei $(s_i)_{i \geq 1}$ eine Folge in K mit erzeugenden Funktion S.*

Weiters besitze die Folge ein GLKP. Dann besitzt für alle $f, g \in K[x], fg \neq 0$ auch die von der Laurentreihe $S' = \frac{f}{g}S - E(\frac{f}{g}S)$ erzeugte Folge ein GLKP.

Beweis. Wir betrachten $\frac{f}{g}S$ und verwenden die Bezeichnungen aus Hilfssatz 2.13.6. Weiters gibt es nach Satz 2.13.4 ein C mit $v(A_i) \leq C\mathrm{Log}(i), i \geq 1$.

Sei nun $v(A_i') > v(f) + v(g)$ für ein $i \geq 1$. Dann gibt es ein $j \geq 1$ mit $v(A_i') \leq v(A_j) + v(f) + v(g)$. Damit erhalten wir

$$v(A_i') \leq C\mathrm{Log}(j) + v(f) + v(g)$$

und

$$j \geq v(Q_{j-1}) + 1 \geq v(Q_{i-1}') + v(f) + 1.$$

Zusammengefasst gilt

$$v(A_i') \leq C\mathrm{Log}(v(Q_{i-1}') + v(f) + 1) + v(f) + v(g).$$

Dies ist für i mit $v(A_i') \leq v(f) + v(g)$ trivial erfüllt und gilt damit für alle $i \geq 1$.

Für $n \in \mathbb{N}$ gilt wegen Folgerung 2.8.1 mit einem passenden $i \geq 0$

$$\begin{aligned}
\left| L_n(S') - \frac{n}{2} \right| &\leq \frac{1}{2}\max\{v(A_i'), v(A_{i+1}')\} \\
&\leq \frac{C}{2}\mathrm{Log}(v(Q_i') + v(f) + 1) + \frac{1}{2}v(f) + \frac{1}{2}v(g) \\
&\leq \frac{C}{2}\mathrm{Log}(n + v(f) + 1) + \frac{1}{2}v(f) + \frac{1}{2}v(g) \\
&\leq C_1\mathrm{Log}(n)
\end{aligned}$$

mit einem passenden C_1 und damit ist die Behauptung gezeigt. ■

Als Folgerung erhalten wir sofort

Folgerung 2.13.8 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit GLKP. Dann besitzt auch jede geshiftete Folge ein GLKP.*

Beweis. Betrachte für $n \in \mathbb{N}$ die Polynome $f = x^n$ und $g = 1$ und wende Satz 2.13.7 an. ■

Wenn eine Folge eine irrationale erzeugenden Funktion S besitzt, für die $K(S) < \infty$ gilt (vgl. Definition 2.8.2), dann folgt aus Satz 2.13.4, dass die Folge ein GLKP besitzt.

Daraus sieht man, dass Folgen mit PLKP und mit fast PLKP auch ein

GLKP besitzen. Insbesonders kann man Folgen mit GLKP damit konstruieren.

Weiters hat auch jede geshiftete Folge ein GLKP. Man kann sogar noch mehr sagen. Dazu zeigen wir zunächst

Satz 2.13.9 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit irrationaler erzeugenden Funktion S und $K(S) < \infty$. Weiters betrachten wir für $f, g \in K[x], fg \neq 0$ die Laurentreihe $S' = \frac{f}{g}S - E(\frac{f}{g}S)$. Dann gilt*

$$K(S') \leq K(S) + v(f) + v(g).$$

Beweis. Wir betrachten $\frac{f}{g}S$ und verwenden dieselben Bezeichnungen wie im Hilfssatz 2.13.6. Gilt also für ein $i \geq 1$, dass $v(A_i') > v(f) + v(g)$ ist, dann erhalten wir $v(A_i') \leq K(S) + v(f) + v(g)$ und für ein i mit $v(A_i') \leq v(f) + v(g)$ gilt dies in trivialer Weise. Daraus folgt die Behauptung. ■

Dieser Satz gilt natürlich auch für $K(S) = \infty$, aber dort ist die Aussage uninteressant.

Als Folgerung erhalten wir

Folgerung 2.13.10 *Sei $(s_i)_{i\geq 1}$ eine Folge in K mit irrationaler erzeugenden Funktion S und $K(S) < \infty$. Weiters bezeichnen wir mit S_m die erzeugenden Funktion der geshifteten Folge $(s_i)_{i\geq m+1}, m \geq 0$. Dann gilt*

$$K(S_m) \leq K(S) + m \quad m \geq 0.$$

Beweis. Wähle $f = x^m$ und $g = 1$. Dann gilt mit den Bezeichnungen des Satzes 2.13.9 $S' = S_m$ und es folgt sofort die Behauptung. ■

Für eine Folge mit irrationaler erzeugenden Funktion S und $K(S) < \infty$ besitzt also auch die erzeugenden Funktion der geshifteten Folge diese Eigenschaft.

Die Abschätzung in Folgerung 2.13.10 kann nicht verschärft werden.

Dazu betrachten wir $K = \mathbb{F}_2$ und die Folge mit $s_i = 1$ für $i = 2^j - 1, j \geq 1$ und $s_i = 0$ sonst. Mit dem Satz von Massey und Wang (Satz 2.7.3) folgt sofort, dass diese Folge PLKP besitzt und damit ist wegen Satz 2.7.2 die erzeugenden Funktion S irrational und $K(S) = 1$.

Wir wählen jetzt $m = 2^j - 1$ für ein $j \geq 1$. Dann beginnt S_m mit x^{-2^j} und der erste Teilnenner in der Kettenbruchentwicklung hat Grad 2^j. Deshalb gilt $K(S_m) \geq 2^j$. Wegen der Folgerung 2.13.10 gilt $K(S_m) \leq 2^j$, also insgesamt $K(S_m) = 2^j$.

Dies bedeutet insbesondere $K(S_m) = K(S) + m$ für unendlich viele m.

2.14 Gleichmäßig gutes lineares Komplexitätsprofil

Sei $(s_i)_{i\geq 1}$ eine Folge in K. Wir bezeichnen mit S_m die erzeugenden Funktion der geshifteten Folge $(s_i)_{i\geq m+1}, m \geq 0$ und deren Kettenbruchentwicklung mit $S_m = [0; A_1^{(m)}, A_2^{(m)}, \ldots]$.

Im vorigen Unterabschnitt haben wir gezeigt, dass wenn eine Folge ein GLKP besitzt, dies auch für jede geshiftete Folge gilt. Ist also $(s_i)_{i\geq 1}$ eine Folge mit GLKP, dann gibt es zu jedem $m \geq 0$ eine Konstante C_m, sodass gilt

$$\left| L_n(S_m) - \frac{n}{2} \right| \leq C_m \mathrm{Log}(n) \quad n \geq 1.$$

Damit liegt die folgende Definition auf der Hand

Definition 2.14.1 Sei $(s_i)_{i\geq 1}$ eine Folge in K. Wir sagen die Folge besitzt ein *gleichmäßig gutes lineares Komplexitätsprofil (GGLKP)*, wenn es ein C gibt, sodass gilt

$$\left| L_n(S_m) - \frac{n}{2} \right| \leq C \mathrm{Log}(n) \quad n \geq 1, m \geq 0.$$

Man beachte, dass die Konstante bei dieser Definition zwar von der Folge abhängt, aber nicht mehr von m.

Handelt es sich bei dieser Eigenschaft um eine typische Eigenschaft von zufälligen Folgen? Der nächste Satz verneint dies.

Satz 2.14.2 *Sei $K = \mathbb{F}_q, q = p^t, p \in \mathbb{P}, t \geq 1$. Dann hat die Menge aller Folgen mit GGLKP Wahrscheinlichkeit 0.*

Beweis. Sei W die Menge aller Folgen mit GGLKP.

Wir betrachten eine Folge $(s_i)_{i\geq 1} \in W$ mit der Eigenschaft, dass ab dem Folgeglied s_{k+1} die nächsten $r \geq 1$ Folgeglieder 0 sind. Dann gilt $L_r(S_k) = 0$ und damit mit einer Konstante C

$$\left| L_r(S_k) - \frac{r}{2} \right| = \frac{r}{2} \leq C \mathrm{Log}(r).$$

Daraus erkennt man, dass die Menge der Längen der Strings von $(s_i)_{i\geq 1}$, die nur aus 0 bestehen, beschränkt sein muss.

Bezeichne $B_r, r \geq 1$ die Menge aller Folgen, wo diese Schranke r ist. Dann gilt $W \subseteq \bigcup_{r=1}^{\infty} B_r$.

Weiters bezeichnen wir mit $B_r^{(t)}, r \geq 1, t \geq 0$ die Menge aller Folgen $(s_i)_{i \geq 1}$ mit der Eigenschaft, dass für $j = 0, 1, \ldots t$ mindestens eines der Elemente $s_{j(r+1)+1}, s_{j(r+1)+2}, \ldots, s_{(j+1)(r+1)}$ ungleich 0 ist.

Klarerweise gilt $B_r \subseteq \bigcap_{t=0}^{\infty} B_r^{(t)}$ und mit dem Satz von Poincare aus der Wahrscheinlichkeitstheorie erhält man sofort $h(B_r^{(t)}) = (1 - q^{-r-1})^{t+1}$.

Damit gilt

$$h(B_r) \leq (1 - q^{-r-1})^{t+1} \quad t \geq 0$$

und mit $t \longrightarrow \infty$, dass $h(B_r) = 0$ ist.

Dies hat aber $h(W) = 0$ zur Folge. ■

Auch die Folgen mit GGLKP lassen sich über die Kettenbruchentwicklung charakterisieren.

Satz 2.14.3 *Sei $(s_i)_{i \geq 1}$ eine Folge in K. Genau dann hat die Folge GGLKP wenn die erzeugende Funktion irrational ist und es eine Konstante C mit* $\mathrm{grad}(A_i^{(m)}) \leq CLog(i), i \geq 1, m \geq 0$ *gibt.*

Beweis. Folgt aus Hilfssatz 2.13.2 und 2.13.3. ■

Eine Folge $(s_i)_{i \geq 1}$ mit irrationaler erzeugenden Funktion und

$$\sup_{m \geq 0} K(S_m) < \infty$$

besitzt nach diesem Satz ein GGLKP. Die Existenz einer solchen Folge ist noch ungelöst.

Auch die Existenz einer Folge mit GGLKP ist noch ein ungelöstes Problem.

Literaturverzeichnis

[1] E. Artin: Quadratische Körper im Gebiete der höheren Kongruenzen I, Thesis, Math. Zeitschrift 19, S.153-206, 1924.

[2] H. Bauer: Wahrscheinlichkeitstheorie, 4nd ed., de Gruyter, Berlin, 1991.

[3] N. H. Bingham: Variants on the law of the iterated logarithm, Bull. London Math. Soc. 18, 433-467, 1986.

[4] P. Bundschuh: Einführung in die Zahlentheorie, Springer, Berlin, 1996.

[5] Z. Dai und K. Zeng: Continued Fractions and the Berlekamp-Massey Algorithm, Advances to Cryptology - AUSCRYPT '90, Lecture Notes in Computer Science, Vol. 453, S. 24-31, Springer, Berlin, 1990.

[6] A. Khintchine: Kettenbrüche, B.G.Teubner, Leipzig, 1956.

[7] U. Krengel: Ergodic Theorems, de Gruyter, Berlin, 1985.

[8] R. Lidl und H. Niederreiter: Finite Fields, Addison-Wesley, Reading, Mass., 1983.

[9] M. Loeve: Probability Theory, 3rd ed., Van Nostrand, New York, 1963.

[10] B. de Mathan, Approximations Diophantiennes dans un corps local, Bull. de la Soc. Math. de France, Suppl. Mem. 21, 1970.

[11] H. Niederreiter: Continued fractions for formal power series, pseudorandom numbers, and linear complexity of sequences, Contributions to General Algebra 5 (Proc. Salzburg Conf., 1986), S.221-233, Teubner, Stuttgart, 1987.

[12] H. Niederreiter: Sequences with almost perfect linear complexity profile, Advances in Cryptology - EUROCRYPT '87 (D. Chaum und W. L. Price, eds.), Lecture Notes in Computer Science, Vol. 304,S.37-51, Springer, Berlin, 1988.

[13] H. Niederreiter: The probabilistic theory of linear complexity, Advances in Cryptology - EUROCRYPT '88 (C. G. Günther, ed.), Lecture Notes in Computer Science, Vol. 330, S. 191-209, Springer, Berlin, 1988.

[14] H. Niederreiter: Keystream sequences with a good linear complexity profile for every starting point, Advances in Cryptology - EUROCRYPT '89 (J.-J. Quisquater und J. Vandewalle, eds.), Lecture Notes in Computer Science, Vol. 434, S. 523-532, Springer, Berlin, 1990.

[15] H. Niederreiter: Finite Fields and Cryptology, Finite Fields, Coding Theory, and Advances in Communication and Computing (G.L. Mullen und P.J.-S. Shiue, eds), S.359-373, M.Dekker, New York, 1993.

[16] W.Nöbauer und J. Wiesenbauer: Zahlentheorie, Prugg, Eisenstadt, 1981.

[17] F. Piper: Stream ciphers, Elektronik und Maschinenbau 104, S. 564-568, 1987.

[18] A.M. Rockett und P. Szüsz: Continued Fractions, World Scientific, Singapore, 1992.

[19] M. Rosenblatt: Random Processes, 2nd ed., Springer, New York, 1974.

[20] R.A. Rueppel, Analysis and Design of Stream Ciphers, Springer, Berlin, 1986.

[21] G. Scheja und U. Storch: Lehrbuch der Algebra 1, Teubner, Stuttgart, 1980.

[22] M.-Z. Wang und J. L. Massey: The characterization of all binary sequences with a perfect linear complexity profile, Paper presented at EUROCRYPT '86, Linköping, 1986.

[23] M. Wang: Linear Complexity Profiles and Continued Fractions, Advances in Cryptology - EUROCRYPT '89, Lecture Notes in Computer Science, Vol. 434, S. 571-585, Springer, Berlin, 1990.