Kaleidoskopvortrag

Enno Nagel

Inhaltsverzeichnis

1 Gebrochene nicht-Archimedische Differenzierbarkeit

Vorstellung eines gebrochenen nicht-Archimedischen Differenzialkalküls

Annahme. Sei von nun an $\mathbf{K}$ ein vollständiger nicht-trivial nicht-Archimedisch bewerteter Körper.

Definition 1.1. Sei $U \subseteq \mathbf{K}$ offen und $f : U \to \mathbf{K}$ eine Funktion.

- Wir setzen
$$f^{]1[}(x,y) := \frac{f(x) - f(y)}{x - y} \quad \text{mit } x,y \text{ verschieden}$$
- Es ist f eine *$\mathscr{C}^1$-Funktion*, falls $f^{]1[}$ sich zu einer stetigen Funktion $f^{[1]} : U \times U \to \mathbf{K}$ fortsetzt.

Bemerkung (Vergleich mit der Situation im Reellen). Wir erinnern uns daran, dass eine reellwertige Funktion auf einer offenen Teilmenge $U \subseteq \mathbb{R}$ in einem Punkt *differenzierbar* ist, falls ihr Differenzenquotient
$$f^{]1[}(x,y) := \frac{f(x) - f(y)}{x - y} \quad \text{mit } x,y \text{ verschieden}$$
für festes y_0 und $x \to y_0$ einen Limes $f'(y_0)$ besitzt. Es gilt nun folgender

Satz. Die Funktion f' ist stetig, genau dann, wenn $f^{]1[}$ sich zu einer stetigen Funktion $f^{[1]} : U \times U \to \mathbb{R}$ fortsetzt.

Beweis: Dies ist eine direkte Folgerung aus dem Mittelwertsatz. □

Diese Beobachtung wird implizit in vielen grundlegenden Sätzen der reellen Analysis benutzt:

- Ist $f : U \to \mathbb{R}$ mit $U \subseteq \mathbb{R}^n$ partiell stetig differenzierbar, so auch stetig total differenzierbar. (Hier wird der Mittelwertsatz angewandt.)
- Der Raum der stetig differenzierbaren Funktion $f : U \to \mathbb{R}$ mit der natürlichen Supremums-Norm auf f und f' ist vollständig. (Hier benutzt man den Hauptsatz der Differenzial- und Integralrechnung.)

In der nicht-Archimedischen Analysis gibt es leider kein befriedigendes Pendant des Zwischenwertsatzes, dass ähnlich starke Resultate wie den Mittelwert- und Hauptsatz zuließe. Daher behilft man sich wie in Definition 1.1 geschehen damit, obigen Satz zur Definition zu erheben.

Bemerkung (Iterierbarkeit). Da der Differenzenquotient $f^{[1]}$ eine Funktion zweier Variablen ist, ist Definition 1.1 leider nicht gleichermassen offensichtlich iterierbar wie jene über den reellwertigen Funktionen einer Variablen. Es ist also bereits im Falle einer Variablen notwendig, zur Definition zweifacher und höherer Ableitbarkeit die Definition des Differenzenquotienten für den Fall mehrerer Variablen formuliert zu haben.

Annahme. Hierzu setzen wir nun den Definitionsbereich unserer Funktionen stets als Teilmenge $U \subseteq \mathbf{K}^d$ eines $\mathbf{K}$-dimensionalen Vektorraums mit fest gewählten Koordinaten voraus und den Wertebereich als einen $\mathbf{K}$-Banachraum $\mathbf{E}$.

Definition. Sei $U \subseteq \mathbf{K}^d$ offen. Eine Funktion $f : U \to \mathbf{E}$ ist eine $\mathscr{C}^1$-*Funktion*, falls für alle $x + h, x \in U$ mit $h \in \mathbf{K}^{*d}$ die Differenzenquotientenabbildung $A := f^{]1[}(x,y) \in \mathrm{Hom}_{\mathbf{K}\text{-vctsp.}}(\mathbf{K}^d,\mathbf{E})$ definiert durch

$$A(h_k \cdot e_k) := f(h_1 \cdot e_1 + \cdots + h_{k-1} \cdot e_{k-1} + h_k e_k) - f(h_1 \cdot e_1 + \cdots + h_{k-1} \cdot e_{k-1}) \text{ für } k = 1,\ldots,d$$

sich zu einer stetigen Funktion $f^{[1]} : U^{[1]} \to \mathrm{Hom}_{\mathbf{K}\text{-vctsp.}}(\mathbf{K}^d,\mathbf{E})$ mit $U^{[1]} = U \times U$ fortsetzt. (Hierbei sind $e_1,\ldots,e_d \in \mathbf{K}^d$ die kanonischen Einheitsvektoren.)

Definition (Skizze). Nun ist der Definitionsbereich $U \times U \subset \mathbf{K}^d \times \mathbf{K}^d$ der Funktion $f^{[1]}$ wieder eine offene Teilmenge eines $\mathbf{K}$-Vektorraums mit kanonischer Einheitsvektoren-basis und ihr Wertebereich wieder ein $\mathbf{K}$-Banachraum. Also lässt sich diese Definition nun iterieren: Man fordert nun $f^{[1]}$ wieder eine $\mathscr{C}^1$-Funktion zu sein, indem sich

$$f^{]2[} := (f^{[1]})^{]1[} : (U^{[1]})^{]1[} \to \mathrm{Hom}_{\mathbf{K}\text{-vstsp.}}(\mathrm{Hom}_{\mathbf{K}\text{-vstsp.}}(\mathbf{K}^d,\mathbf{E}),\mathbf{E})$$

zu einer stetigen Funktion $f^{[2]}$ auf $U^{[2]} = U^{[1]} \times U^{[1]}$ fortsetzt, und so weiter und so fort.

Das Ziel meiner Arbeit ist die Entwicklung und Untersuchung des Begriffs einer r-fach ableitbaren Funktion für eine reelle Zahl $r \geq 0$. Hierzu schreiben wir $r = \nu + \rho$ mit $\nu \in \mathbb{N}$ und $\rho \in [0,1[$.

Definition. Seien X,Y metrische Räume. Dann ist $f : X \to Y$ eine $\mathscr{C}^\rho$-*Funktion*, falls für alle $a \in X$ und $\varepsilon > 0$, es eine Umgebung $U \ni a$ in X gibt, sodass

$$d(f(x),f(y)) \leq \varepsilon \cdot d(x,y)^\rho \quad \text{für alle } x,y \in U.$$

Bemerkung (Lipschitzsche Eselsbrücke). Es ist dies also eine Verschärfung der üblichen Definition Lipschitz-Stetigkeit, indem man die O-Konvergenzbedingung durch eine o-Konvergenzbedingung ersetzt.

Formal haben wir nun $f^{]\nu[} : \mathrm{U}^{]\nu[} \to \mathrm{Hom}_{\mathbf{K}\text{-vctsp.}}(\mathbf{K}^d, \mathbf{E})$ und $\mathrm{U}^{[\nu]}$ bisher allein für $\nu = 1{,}2$ erklärt. Wir erlauben uns trotzdem folgende Definition zu machen:

Definition. Sei $\mathrm{U} \subseteq \mathbf{K}^d$ offen. Eine Funktion $f : \mathrm{U} \to \mathbf{K}$ ist eine $\mathscr{C}^r$-*Funktion*, falls die Funktion $f^{]\nu[} : \mathrm{U}^{]\nu[} \to \mathbf{K}$ sich zu einer $\mathscr{C}^\rho$-Funktion auf ganz $\mathrm{U}^{[\nu]}$ fortsetzt.

Bemerkung (Ausnutzung zusätzlicher Symmetrien à la Schikhof in letztlich gegebener Definition). Leider ist mit dieser Definition die ν-te Ableitung $f^{[\nu]}$ einer $\mathscr{C}^\nu$-Funktion $f : \mathrm{U} \to \mathbf{K}$ in einer Variablen bereits eine Abbildung in 2^d Variablen. Dies lässt sich durch die Beobachtung von Wim Schikhof, dass es für symmetrische Funktionen genügt, die Differenzierbarkeit in der ersten Variablen zu betrachten und die Ableitungsabbildungen $f^{]n[}$ dies in allen k-ten Koordinaten des $\mathbf{K}^d$ sind, umgehend auf ein lineares Variablenwachstum reduzieren. Hieraus rührt die letztlich gegebene Definition r-facher Differenzierbarkeit meiner Arbeit.

Wir untersuchen diesen Begriff einer r-fach ableitbaren Funktion nun auf alle naiv erwartbaren Eigenschaften. Wir zeigen:

- Die Definition einer $\mathscr{C}^r$-Funktion ist punktweise möglich. (Und in voller Allgemeinheit für lokal kartesische Teilmengen des K^d dessen lokale Faktoren frei von isolierten Punkten).
- Für $r \geq 1$ ist die Verknüpfung zweier $\mathscr{C}^r$-Funktionen wieder eine $\mathscr{C}^r$-Funktion. Hieraus ergibt sich zusammen mit der ersten Eigenschaft der Lokalheit des Begriffs einer $\mathscr{C}^r$-Funktion die Definition einer $\mathscr{C}^r$-Funktion auf einer $\mathscr{C}^r$-Mannigfaltigkeit, die von der Wahl des Atlases (innerhalb des fest gewählten maximalen Atlases) unabhängig ist.
- Der $\mathbf{K}$-Vektorraum der $\mathscr{C}^r$-Funktionen lässt sich in natürlicher Weise mit einer vollständigen lokal konvexen Topologie versehen. Diese ist eine lokal konvexe $\mathbf{K}$-Algebra, falls der Wertebereich der Funktionen dies ist.
- Sei $\mathrm{U} \subseteq \mathbf{K}^d$ offen. Es gilt $\mathscr{C}^{\mathrm{an}}(\mathrm{U},\mathbf{E}) \subseteq \mathscr{C}^\infty = \cap_{r \geq 0} \mathscr{C}^r(\mathrm{U},\mathbf{E})$. Dann kann man zeigen, dass die lokal polynomialen Funktionen vom Höchstgrad ν ebenso wie alle polynomialen Funktionen dicht in $\mathscr{C}^r(\mathrm{U},\mathbf{E})$ liegen (für U lokal kompakt).
- Die stetigen linearen Funktionale $\mathscr{D}(\mathrm{U})$ auf allen $\mathscr{C}^r(\mathrm{U},\mathbf{E})$ für ein $r \geq 0$ bilden in natürlicher Weise einen filtrierten $\mathbf{K}$-Vektorraum. Ist U eine

Gruppe mit $\mathscr{C}^\infty$-Multiplikation, so kann man zeigen, dass durch die Faltung $\mathscr{D}(\mathrm{U})$ zu einer filtrierten $\mathbf{K}$-Algebra wird.

Wir konnten bereits durch Ausnutzung der Symmetrieeigenschaften der Ableitungsfunktion diese vereinfachen. Allerdings ist diese dennoch weit davon entfernt von so einfacher Gestalt wie im Reellen zu sein. In Spezialfällen kommen wir zu folgenden Vereinfachungsresultaten:

- Sei $\mathrm{U} \subseteq \mathbf{K}$ eine offene Teilmenge. Dann ist $f\colon \mathrm{U} \to \mathbf{K}$ eine $\mathscr{C}^r$-Funktion, genau dann, wenn das *ν-te Restglied des Taylorpolynoms*

$$\mathrm{R}_\nu f(x+h,h) := f(x+h) - f(x) - \cdots - f^{(\nu)}/\nu!(x)h^\nu$$

  als Funktion *beider* Variablen $x+h,x$ eine Konvergenzbedingung der Ordnung $o(|h|^r)$ erfüllt.

- Enthalte nun $\mathbf{K} \supseteq \mathbb{Q}_p$ als bewerteten Körper. Der Iwasawa Isomorphismus $\mathbf{K}[[\mathrm{X}]] \xrightarrow{\sim} \mathbf{K}[[\mathbb{Z}_p]]$ liefert zusammen mit einem Dualitätsargument eine ausgezeichnete Orthogonalbasis des $\mathbf{K}$-Banachraums $\mathscr{C}^0(\mathbb{Z}_p,\mathbf{K})$, die sogenannte *Mahler Basis*. Wir zeigen, dass dann die Funktionen $\mathscr{C}^r(\mathbb{Z}_p,\mathbf{K}) \subseteq \mathscr{C}^0(\mathbb{Z}_p,\mathbf{K})$ genau diejenigen sind, deren Mahlerkoeffizienten der Bedingung $|a_{\boldsymbol{n}}||\boldsymbol{n}|^r \to 0$ mit $|\boldsymbol{n}| = n_1 + \cdots + n_d$ für $\boldsymbol{n} \in \mathbb{N}^d$ gehorchen.

- Als Korollar beider obiger Ergebnisse erhalten wir, dass auf offenen Teilmengen $\mathrm{U} \subseteq \mathbb{Q}_p^d$ sich die r-fach ableitbaren Funktionen $f\colon \mathrm{U} \to \mathbf{K}$ ebenfalls durch eine Taylorpolynombedingung charakterisieren lassen.

Differenzierbare Funktionen zur Untersuchung des universellen unitären Gitters einer unverzweigten algebraischen Hauptreihendarstellung

Die Definition r-fach differenzierbarer Funktionen auf Mannigfaltigkeiten war durch einen Artikel von Berger und Breuil motiviert, in welchem die Autoren eine Definition r-fach differenzierbarer Funktionen auf $\mathbb{Z}_p$ geben um die *universelle unitäre Vervollständigung* einer lokal algebraischen Hauptreihendarstellung von $\mathrm{GL}_2(\mathbb{Q}_p)$ explizit zu machen.

Definition. Sei G die topologische Gruppe der rationalen Punkte einer zusammenhängenden reduktiven Gruppe über einem lokalen Körper $\mathbb{F}$ und V ein lokal konvexer $\mathbf{K}$-Vektorraum mit stetiger G-Operation. Dann heißt der universelle $\mathbf{K}$-Banachraum mit einer G-invarianten Norm, in die sich V stetig abbildet die *universelle unitäre Vervollständigung* $\hat{\mathrm{V}}$ *von* V. Das *universelle unitäre Gitter* $\mathfrak{L} \subseteq \mathrm{V}$ ist dann das Urbild der Einheitskugel von $\hat{\mathrm{V}}$.

Im zweiten Kapitel untersuche ich das universelle unitäre Gitter der lokal algebraischen Darstellung

$$V = \mathrm{Ind}_{\bar{P}}^{G}\,\theta \otimes U;$$

hierbei ist $\bar{P}$ eine minimale parabolische Untergruppe von G, weiter $\theta\colon P \to \mathbf{K}^*$ ein unverzweigter Charakter und U eine (o.E. irreduzible) algebraische Darstellung. Wir setzen weiterhin im nicht-glatten Fall (das heißt U nicht-trivial) voraus, dass G zerfällt und $\mathbf{K} \supseteq \mathbb{F}$.

Satz. *Es ist*

$$\mathfrak{L} = \sum_{w \in W} \mathfrak{L}_w$$

mit zyklischen $\mathbf{o}_{[}P]$*-Modulen* $\mathfrak{L}_w$*; hierbei ist* W *die Weyl-Gruppe von* G*, weiter* P *die* $\bar{P}$ *entgegengesetzte parabolische Untergruppe und* $\mathbf{o} \subseteq \mathbf{K}$ *der Bewertungsring.*

Beweis: Das lässt sich durch die endliche Erzeugtheit von V als $\mathbf{o}[P]$-Modul durch seine Iwahori-Invariaten, die Iwasawa Zerlegung G = KP mit kompaktem K und sogenannte Verflechtungssoperatoren zeigen. □

Man kann dann $\mathfrak{L}_w \subseteq \mathscr{C}^{\Psi-\mathrm{pol}}(N,\mathbf{K})$ als Gitter in gewissen lokal polynomialen Funktionen auf dem unipotenten Radikal $N \subseteq P$ auffassen (Hierbei ist N als Varietät einfach ein Produkt von Kopien des Körpers $\mathbb{F}$, und in diesem Sinne ist die Definition einer (lokal) polynomialen Funktion auf N zu verstehen).

Satz. *Jedes der Gitter* $\mathfrak{L}_w \subseteq \mathscr{C}^{\Psi-\mathrm{pol}}(N,\mathbf{K})$ *ist ein freier* $\mathbf{o}$*-Modul.*

Beweis: Hierzu genügt es eine Norm anzugeben, die punktweise nicht kleiner als die von $\mathfrak{L}_w$ auf $\mathscr{C}^{\Psi-\mathrm{pol}}(N,\mathbf{K})$ induzierte Seminorm ist. Dies geschieht durch Konstruktion einer Norm $\boldsymbol{r}$-fach differenzierbarer Funktion auf $\mathscr{C}^{\Psi-\mathrm{pol}}(N,\mathbf{K})$ für ein Tupel $\boldsymbol{r} \in \mathbb{R}_{\geq 0}^{\Phi^+}$. (Hierbei ist Φ^+ die endliche Menge der positiven Wurzeln von G.) □

2 Der Satz von Steele-Yao

Die klassische Komplexitätstheorie unterscheidet im Wesentlichen in der Klasse der berechenbaren Probleme zwischen solchem mit polynomialer — solcher der Klasse P - und nicht-polynomialer Lösungslaufzeit. (Solche mit polynomialer Verifikationslaufzeit werden dann der Klasse NP zugerechnet.) In der *feinen* oder algorithmischen Komplexitätstheorie ist wiederum die spezielle Gestalt des Polynoms $p(n)$, dem sich mit wachsender Eingabelänge n (ist etwa das Argument eine natürliche Zahl x, so ist n die Länge von x in seiner Binärdarstellung) die Laufzeit $t(n)$ asymptotisch annähert, das zu untersuchende Objekt.

Bemerkung. Hierbei ist exakter ein Problem der Komplexität $O(p(n))$, falls für die Laufzeit $t(n)$ in Abhängigkeit der Eingabelänge n gilt, dass

$$\limsup_{n\to\infty} p(n)/t(n) \leq C \quad \text{für eine Konstante } C > 0,$$

das heißt also ab einem gewissen n_0 gilt stets $t(n) \leq C \cdot p(n)$ für alle $n \geq n_0$.

Exempel (Multiplikation zweier Zahlen). Wir setzen hier wie im Folgenden das Maschinenmodell einer R-RAM voraus, hierbei sei in diesem Fall der Rechenbereich $R = \mathbb{N}$. Dieses Modell verfügt über einen Befehl zur Addition (und Subtraktion) zweier Zahlen (nebst Sprung-,Ein- und Ausgabebefehlen), das heißt Errechnung der Summe zweier Zahlen nehmen wir an, dies verursache den Zeitaufwand eines Einheitszeitmaßes. Um nun das Produkt zweier Zahlen a,b mit je n Stellen in der Binärdarstellung zu berechnen, ist naiv (nach dem Distributivgesetz aus der Schule) ein Aufwand von n^2 Multiplikationen notwendig. Folgende Reduktionen sind möglich:

(i) Teile und herrsche, angewandt auf die Ziffernfolgen: Sei zur Veranschaulichung n gerade. Schreibe hierzu das Produkt ab als

$$(a' \cdot 2^{n/2} + a'')(b' \cdot 2^{n/2} + b'') = a'b'2^n + (a'b'' + a''b')2^{n/2} + a''b''.$$

Dann ergibt sich ein Rechenaufwand von etwa $3/4 \cdot n^2$ Multiplikationen, da

$$a'b'' + a''b' = (a' + a'') \cdot (b' + b'') - [a'b' + a''b''].$$

Dadurch ergibt sich iterativ ein Rechenaufwand von etwa $n \log_{4/3} n$ Multiplikationen.

(ii) Teile und herrsche, angewandt auf die Fouriertransformation: Seien $a = \sum a_j 2^j$ und $b = \sum b_k 2^k$. Wir beobachten, dass durch Anwendung der Distributivregel gilt

$$ab = \sum_{i \geq 0} c_i 2^i \quad \text{mit} \quad c_i = \sum_{j+k=i} a_j b_k.$$

Dies ist also ein Faltungsprodukt auf dem additiven Monoid $\mathbb{N}$ für die zu einer Zahl $a = \sum_{i \geq 0} a_i 2^i$ gehörige Funktion $a \colon \mathbb{N} \to \{0,1\}$ definiert durch $i \mapsto a_i$. Durch Anwendung von Fouriertransformation (hin und zurück) lässt sich dies in ein komponentenweises Produkt überführen, für das so transformierte Produkt bedarf es daher allein n Multiplikationen. Der Aufwand für die Fouriertransformation lässt sich nun durch die Berechnungsmethode der sogenannten „schnellen Fouriertransformation“ gering halten. Diese verfährt auch nach dem „Teile und Herrsche“ - Prinzip und erreicht somit einen Rechenaufwand von $n \log_2 n$ Multiplikationsoperationen: Sei zur Veranschaulichung n gerade. Spalte nun die Summen zur Berechnung der Fouriertransformierten auf:

$$\begin{aligned}
\hat{f}(k) &= \sum_{j=0,\ldots,n-1} f(j)\omega^{j \cdot k} \\
&= \sum_{j=0,\ldots,n/2-1} f(2j)\omega^{2j \cdot k} + \sum_{j=0,\ldots,n/2-1} f(2j+1)\omega^{(2j+1) \cdot k} \\
&= \hat{f_1}(k) + \hat{f_2}(k) \quad \text{mit geeigneten } f_1, f_2;
\end{aligned}$$

und führe dies für die auftretenden Summanden genauso fort. Es ergibt sich ein approximativer Aufwand von $\log_2(n)n$ Multiplikationen zur Fouriertransformation.

Bemerkung. Es ist nun ein unbekanntes Problem, ob der approximative Rechenaufwand von $O(\log_2(n)n)$ Schritten bei Eingabelänge n der schnellstmögliche auf diesem Rechnermodell einer $\mathbb{N}$-Ram ist.

Es ist aber möglich, für *Entscheidungsprobleme* eine untere Schranke für die *Entscheidungskomplexität* auf einer $\mathbb{R}$-RAM anzugeben. Dies tut der Satz von Steele-Yao.

Definition (Maschinenmodell). Eine $\mathbb{R}$-*RAM* (oder allgemeiner R-RAM für einen Rechenbereich (= Menge) R) ist ein Rechnermodell mit unendlichen vielen Speicherzellen für reelle Zahlen und besitzt einen Befehlssatz aus Sprung-,Ein- und Ausgabebefehlen und Rechenoperationen Addition und Subtraktion.

(Dies meint, dass für all diese Operationen ein Einheitszeitmaß zur Berechnung der Laufzeit veranschlagt wird.)

Bemerkung. Es gilt zur Abschätzung der Laufzeit einer $\mathbb{N}$-RAM im Vergleich zu dem einer Turingmaschine TM, dass

$$\mathrm{TM-LTIME}(n) \leq \mathbb{N}-\mathrm{RAM}-\mathrm{UTIME}(n) \leq \mathrm{TM-LTIME}(n^3);$$

hierbei bezeichnet LTIME ein Zeitmaß, dass von der Länge der Eingabe proportional abhängt, es kostet also ein Befehl zur Verarbeitung des Arguments $x \in \mathbb{N}$ dann $\log_2(x)$ Rechenschritte (mindestens jedoch einen!).

Definition. Ein *Problem* sei eine Schar partieller Funktionen $(f_n)_{n\in\mathbb{N}^i}$ mit $f : \mathbb{R}^{d_n} \to \mathbb{R}^{e_n}$. Wir sprechen von einem *Entscheidungsproblem*, falls im $f_n \subseteq \{0,1\}$ für alle $n \in \mathbb{N}^i$. Ist $f : \mathbb{R}^d \to \{0,1\}$ ein Entscheidungsproblem (mit festem Parameter n), so heißt $\mathrm{U}_f = f^{-1}\{1\}$ die *Akzeptanzmenge.*

Definition. Die *Lösung* eines Problems $(f_n)_{n\in\mathbb{N}^i}$ auf einer $\mathbb{R}$-RAM die Angabe einer Schar von R-RAM Programmen $(\mathrm{P}_n)_{n\in\mathbb{N}^i}$, die (f_n) berechnet. Es ist also

$$f_n(x) = y \quad \Longleftrightarrow \quad \mathrm{P}_n(x) \text{ terminiert mit Ausgabe } y.$$

Es sei dann $t(\mathrm{P}_n,x)$ die Anzahl der Schritte von P_n zur Berechnung von x und $t(\mathrm{P}_n) = \max\{t(\mathrm{P}_n,x) : x \in \mathrm{dom} f_n\}$. Dann erklären wir die *(Zeit-)Komplexität* des Problems f_n durch

$$t(f_n) = \max\{t(\mathrm{P}_n) : \ \mathrm{P}_n \text{ berechnet } f_n \ \}.$$

Bemerkung. Es ist auch der Verbrauch der Anzahl von Speicherplätzen interessant. Dieser wird im folgenden aber nicht betrachtet.

Bemerkung. Die Komplexität $(t(f_n))$ des Problems (f_n) hängt stark von der Wahl des Rechnermodells und der Parametrisierung ab. Um im Folgenden ein davon möglichst unabhängiges Mass der Zeitkomplexität zu erhalten, betrachten wir von nun an allein die Häufigkeit der *bedingten Sprungbefehle.* Dies führt zum Modell der *algebraischen Entscheidungsbäume.*

Definition. Ein *algebraischer Entscheidungsbaum* in den Variablen $x_1,\ldots,x_n$ im Rechenbereich R ist ein Binärbaum dessen Knoten $f(x_1,\ldots,x_n) > , \geq , = 0$ für ein Polynom $f \in \mathrm{R}[x_1,\ldots,x_n]$.

Satz. *Zum einem* R – RAM *Programm* P *lässt sich in kanonischer Weise ein algebraischer Entscheidungsbaum* T *zuordnen.*

Beweis: Die Knoten enkodieren alle Rechnungen, die bis zu einem bedingten Sprungbefehl gleich ablaufen. □

Definition.

- Die *Höhe* eines Entscheidungsbaums ist die Länge des längsten in ihm auftretenden Pfads.
- Ein *Blatt* eines Entscheidungsbaums ist ein Knoten ohne Nachfolger.
- Die *Ordnung* eines Entscheidungsbaums ist der maximale Grad der auftretenden Polynome.

Bemerkung.

- Jedes Blatt B repräsentiert die Teilmenge $U_B \subseteq U$ der Eingabemenge U, für die P bei Eingabe von x in B endet. Offenbar gilt $U = \dot{\cup} U_B$.
- Es gilt $h = t(P)$, falls h die Höhe ist und $t(P)$ die (maximale) Laufzeit des Programms P, wenn wir nur die Sprungbefehle zählen.

Der springende Punkt

Definition. Wir bezeichnen einen topologischen Raum als *unzusammenhängend*, falls er sich als disjunkte Vereinigung zweier offener echter Teilmengen schreiben lässt. Eine *Zusammenhangskomponente* ist eine maximale zusammenhängende Teilmenge.

Bemerkung. In den folgenden Beispielen wird angewandt, dass ein zusammenhängender *lokal wegzusammenhängender* Raum bereits wegzusammenhängend ist. Dies bedeutet, dass zu jedem Punkt eine Umgebung existiert, in der sich je zwei Punkte durch eine stetige Abbildung mit Definitionsbereich [0,1] und Werten in dieser verbinden lassen.

Bemerkung (Entscheidende Einsicht). Sei T ein Baum und h seine Höhe. Dann können wir diese wie folgt durch die Anzahl der Zusammenhangskomponenten von U abschätzen:

- Einerseits gilt
$$\#\{ \text{ Blätter } \} \leq 2^h.$$

- Andrerseits nehmen wir an, dass es für die Anzahl der Zusammenhangskomponenten ρ_B von U_B für alle Blätter B eine obere Schranke $C \geq 1$ gibt. Dann gilt

$$\rho(U) \leq C\#\{ \text{ Blätter } \}.$$

Zusammen ergibt sich

$$h \geq \log_2(\rho(U)) - c$$

für eine Konstante $c \geq 0$. Hierbei hängt C womöglich von h,d und n ab! Im Satz von Steele-Yao hat dies $C = C(d,h,n)$ aber eine besonders einfache Gestalt.

Also lässt sich die Mindestlaufzeit h (unter alleiniger Betrachtung der Sprungbefehle) jedes Programms P bereits an der Geometrie von U ablesen.

Der lineare Fall

Satz. *Ist* T *linear, so ist* U_B *für alle Blätter* B *konvex.*

Beweis: Es ist dann $f(x) \geq 0$ eine Halbebene und ein Durchschnitt solcher ist konvex (Leichte Rechnung). □

Definition. Sei $U \subseteq \mathbb{R}^n$. Wir setzen

$$\rho_{\text{conv}}(U) = \min\{k \in \mathbb{N} : U \text{ ist disjunkte Vereinigung } k \text{ konvexer Polyeder } \}.$$

Theorem. *Es gilt* $h \geq \log_2 \rho_{conv}(U)$.

Beweis: Wende die entscheidende Einsicht mit $C = 1$ an (Denn U_B ist bereits konvex!). □

Korollar (Linearer Steele-Yao). *Ist* f_n *ein Entscheidungsproblem, so hat jedes linear* $\mathbb{R}$*-RAM Programm* P_n *eine Mindestlaufzeit*

$$t_n \geq \log_2 \rho_{conv}(U).$$

Exempel 2.1. Wir betrachten das Problem DUPLICATE. Es ist definiert durch die Akzeptanzmenge

$$U = \{\boldsymbol{x} \in \mathbb{R}^n : x_1, \ldots, x_n \text{ alle verschieden } \}.$$

Wir zeigen mit dem Linearen Satz von Steele-Yao, dass

$$t_n \geq n \log_2(n)$$

für die Mindestlaufzeit t_n jedes linearen $\mathbb{R}$-RAM Programms P_n zur Berechnung von U. Hierzu bemerken wir, dass $U = \dot{\cup} U_\sigma$ mit

$$U_\sigma = \{\boldsymbol{x} \in U : x_{\sigma 1} < \ldots < x_{\sigma n}\};$$

hierbei durchläuft σ alle Permutationen des Tupels $(1,\ldots,n)$. Jede dieser Mengen U_σ ist konvex. Andererseits ist keine Zerlegung der Menge U in weniger konvexe Teilmengen möglich: Seien dazu $x \in U_\sigma, y \in U_\pi$ in verschiedenen konvexen Teilmengen. Dann gibt es $i < j \in \mathbb{N}$ mit $\sigma i < \sigma j$ und $\pi i > \pi j$. (Vertausche hierzu eventuell die Rollen von x und y.) Sei dann

$$\begin{aligned} \tau : [0,1] &\to \mathbb{R}^n \\ t &\mapsto (1-t)\cdot x + t \cdot y \end{aligned}$$

der Pfad der Konvexlinearkombinationen von x und y. Betrachte die Differenz $\Delta(t) = \tau_i(t) - \tau_j(t)$ der i-ten und j-ten Koordinateneinträge. Dann gilt $\Delta(0) = x_i - x_j < 0$ und $\Delta(1) = y_i - y_j > 0$. Daher existiert nach dem Zwischenwertsatz ein t_0 mit $\Delta(t_0) = 0$ und damit $\tau(t_0) \notin U$. Also ist $\rho_{\text{conv}}(U) = n!$ und damit nach dem linearen Satz von Steele-Yao $t_n \geq \log_2(n) \geq c \cdot n \log_2(n)$ für eine positive Konstante $c \leq 1$ für die Laufzeit t_n jedes Programms einer $\mathbb{R}$-RAM zur Berechnung von U.

Der Fall höherer Ordnung

Um in diesem Fall eine Abschätzung der Anzahl der Zusammenhangskomponenten von U_B zu erhalten (die keineswegs mehr konvex zu sein brauchen!), bedarf es folgenden Hilfsmittels aus der algebraischen Geometrie.

Definition. Sei $U \subseteq \mathbb{R}^n$. Wir setzen

$$\rho(U) = \#\{\text{ Zusammenhangskomponenten von U}\}.$$

Satz (Milnor-Thom). *Sei $V \subset \mathbb{R}^n$ eine algebraische Varietät (= Teilmenge, die durch gemeinsame Nullstellenmenge von Polynomen gegeben ist) deren Verschwindungsideal durch Polynome vom Höchstgrad d erzeugt wird. Dann gilt*

$$\rho(V) \leq d(2d-1)^{n-1}.$$

Beweis: Ist V durch die Nullstellenmenge eines Polynoms f gegeben, so ist nach dem chinesischen Restsatz offenbar im Zariski-Sinne $\rho(V) \leq d$. (Denn f lässt

sich als Produkt höchstens d teilerfremder Polynome schreiben.) Der Durchschnitt mit der Nullstellenmenge jedes weiteren Polynoms spaltet dann jeder dieser Komponenten in höchstens $2d-1$ viele Zusammenhangskomponenten auf ... □

Satz (Semialgebraischer Milnor-Thom). *Sei* $V \subset \mathbb{R}^n$ *eine semialgebraische Varietät (= Analogon zur Varietät mit* $\geq / > 0$*), die durch Polynome vom Maximalgrad* d *und* k *Ungleichungen beschrieben wird. Dann gilt*

$$\rho(V) \leq d(2d-1)^{n+k-1}$$

Beweis: Wir beachten zunächst, dass man erstens jede Ungleichung > 0 durch eine der Form $\geq \varepsilon$ mit hinreichend kleinem $\varepsilon > 0$ ersetzen kann, ohne die Anzahl der Zusammenhangskomponenten zu verringern (Wähle $\varepsilon > 0$ so klein, dass jede Zusammenhangskomponente von $\{f > 0\}$ mit $\{f \geq \varepsilon\}$ geschnitten wird!). Dann gilt

$$f(\boldsymbol{x}) \geq 0 \iff \exists y \in \mathbb{R} \text{ derart, dass } f(\boldsymbol{x}) - y^2 = 0,$$

das heißt

$$\{f(\boldsymbol{x}) \geq 0\} = \varprojlim_{\boldsymbol{x}} \{F(\boldsymbol{x},y) = 0\} \text{ mit } F(\boldsymbol{x},y) = f(\boldsymbol{x}) - y^2.$$

Damit können wir V schreiben als

$$V = \varprojlim_{\boldsymbol{x}} W \text{ mit einer algebraischen Varietät } W \subseteq \mathbb{R}^{n+k}.$$

Wegen der Stetigkeit von $\varprojlim_{\boldsymbol{x}}$ gilt damit nach dem Satz von Milnor-Thom, dass

$$\rho(V) \leq \rho(W) \leq d(2d-1)^{n+k-1}.$$

Theorem (Steele-Yao). *Sei* $U \subseteq \mathbb{R}^n$ *die Akzeptanzmenge eines Entscheidungsproblems* $f : U \to \{0,1\}$. *Dann gilt für die Mindestanzahl an bedingten Sprungbefehlen* h*, die jedes* $\mathbb{R}$*-RAM Programm* P *zur Berechnung von* f *auszuführen hat, dass durch einen algebraischen Entscheidungsbaum beschränkter Ordnung* d *modelliert werden kann, dass*

$$h \geq c(\log_2 \rho(U) - n) \quad \textit{für eine Konstante } c > 0;$$

hierbei hängt $c = c(d)$ *allein von der Ordnung* d *ab.*

Beweis: Durch den semi-algebraischen Satz von Milnor-Thom erhalten wir eine Konstante $C \geq 1$ zur Abschätzung der Zusammenhangskomponenten jeder Blattmenge $U_B \subseteq U$. Wende nun die entscheidende Einsicht an. □

Exempel. Wir betrachten das Problem ALLPOINTSEXTREMAL. Es ist definiert durch die Akzeptanzmenge

$$U = \{\boldsymbol{x} \in (\mathbb{R}^2)^n : x_1,\ldots,x_n \in \mathbb{R}^2 \text{ sind Extremalpunkte des von ihnen aufgespannten Polygons im } \mathbb{R}^2\};$$

hierbei ist das *von* $x_1,\ldots,x_n$ *aufgespannte Polygon* die kleinste konvexe Teilmenge im $\mathbb{R}^2$ die $x_1,\ldots,x_n$ enthält und ein Punkt heißt *extremal*, falls er nicht innerhalb einer Verbindungsstrecke in diesem Polygon liegt.
Sei nun $n \geq 3$. Da $(x_1,\ldots,x_n) \in U$ im von Ihnen aufgespannten Polygon G nicht extremal sind, hat dies einen inneren Punkt x_0, durch den wir beginnend bei x_1 die Punkte $x_2,\ldots,x_n$ dem Uhrzeigersinn nach sortieren können (Bild!). Es gilt $U = \dot{\cup} U_\pi$ mit

$$U_\pi := \{\boldsymbol{x} \in U : x_{\pi 2},\ldots,x_{\pi n} \text{ folgen } x_1 \text{ im Uhrzeigersinn }\};$$

hierbei durchläuft π die Permutationen des Tupels $(2,\ldots,n)$.
Dann kann man zeigen (benutze die Charakterisierung des positiven Winkels durch Positiv-Definitheit des Skalarprodukts), dass jede Menge U_π konvex ist.
Wir möchten nun zeigen, dass keine Zerlegung in größer zusammenhängende Teilmengen möglich ist. Hierzu bemerken wir, dass da jedes U_π konvex, insbesondere wegzusammenhängend ist, und damit U lokal wegzusammenhängend. Somit genügt es zu zeigen, dass keine Zerlegung von U in größere wegzusammenhängende Teilmengen möglich ist. Seien dazu $x \in U_\pi, y \in U_\sigma$ in verschiedenen konvexen Teilmengen und

$$\tau : [0,1] \to \mathbb{R}^n$$

eine stetige Abbildung mit $\tau(0) = x$ und $\tau(1) = y$. Sei dann

$$\Delta : [0,1] \to \mathbb{R}$$
$$t \mapsto \text{ Die orientierte Fläche des Dreiecks mit Eckpunkten } \tau(t)_i, \tau(t)_j, \tau(t)_k,$$

hierbei ist die *orientierte Fläche* $\Delta(x,y,z)$ dreier Punkte $x,y,z \in \mathbb{R}^2$ durch

$$\Delta(x,y,z) =< x - z, y - z >$$

gegeben. Dann existiert wegen $\Delta(0) < 0$ und $\Delta(1) > 0$ also ein t_0 mit $\Delta(t_0) = 0$. Damit sind für $z = \tau(t_0)$ die Punkte z_i,z_j und z_k kolinear und damit einer dieser nicht extremal. Also $z \notin \mathrm{U}$. Damit gilt

$$\rho(\mathrm{U}_n) = (n-1)!$$

und aus dem Satz von Steele-Yao folgt

$$f_n \in \Omega(\log_2((n-1)!) - n) = \Omega(n \log_2(n)).$$

Bemerkung. Da leider die Teilraumtopologie von $\mathbb{N}$ innerhalb von $\mathbb{R}$ diskret ist, ist der Satz von Steele-Yao leider nicht im realistischeren Maschinenmodell einer $\mathbb{N}$-RAM anwendbar.

3 Die Anstiegsfiltration von ϕ-Moduln über dem Robba-Ring nach Kedlaya

Setup

Notation. Für einen lokalen Körper $\mathbf{K}$ (vollständig nicht-Archimedisch diskret bewertet mit endlichem Restklassenkörper) sei $\mathbf{o} \subseteq \mathbf{K}$ sein diskreter Bewertungsring, $\mathfrak{m}_{\mathbf{K}}$ sein maximales Ideal, $\mathbf{k}$ sein Restklassenkörper und π ein uniformisierendes Element.

Annahme. Im Folgenden sei stets $\mathbf{K} = \mathbf{K}_0 \supseteq \mathbb{Q}_p$ ein unverzweigter p-adischer Zahlkörper

Bemerkung. Es ist also $\mathbf{o} = \mathrm{W}(\mathbf{k})$, der Witt-Ring über dem perfekten Körper $\mathbf{k}$ und $\mathbf{K} = o[1/p]$.

Definition (Robba Ring). Wir definieren für ein Intervall $\mathrm{I} \subseteq [0,1[$ die *Kreisscheibe* $\mathrm{D}(\mathrm{I}) := \{x \in \mathbf{K} : |x| \in \mathrm{I}\}$ und setzen

$$\mathcal{O}_{\mathrm{I}} := \{\sum_{n\in\mathbb{Z}} a_n u^n : \sum_{n\in\mathbb{Z}} a_n x^n \text{ existiert für alle } x \in \mathrm{D}(\mathrm{I})\}.$$

Wir haben auf $\mathcal{O}_{\mathrm{I}}$ für alle $\rho \in \mathrm{I}$ die Bewertung $|\cdot|_\rho$ definiert durch $|\sum a_n u^n|_\rho = \max\{|a_n|\rho^n\}$.

Der *Robba Ring* $\mathcal{R}$ ist definiert durch

$$\mathcal{R} = \bigcup_{\rho<1} \mathcal{O}_{[\rho,1[}\,.$$

Es wird $\mathcal{R}$ zu einem Fréchet-Raum durch die Bewertungen $\{|\cdot|_\rho : \rho \in [0,1[\cap\mathbb{Q}\}$.

Definition (Frobenius auf dem Robba-Ring). Wir haben auf $\mathcal{O}_{\mathrm{I}}$ die Abbildung

$$\phi_{\mathcal{O}_{\mathrm{I}}/\mathbf{K}} \colon \mathcal{O}_{\mathrm{I}} \to \mathcal{O}_{\sqrt[p]{\mathrm{I}}}, \quad u \mapsto u^p,$$

mit $\sqrt[p]{\mathrm{I}} = [\sqrt[p]{a}, \sqrt[p]{b}]$ für $\mathrm{I} = [a,b]$. Dann erhalten wir einen Operator $\phi_{\mathcal{R}/\mathbf{K}} \colon \mathcal{R} \circlearrowleft$ als direkten Limes der $\phi_{\mathcal{O}_{[\rho,1[}/\mathbf{K}}$ für $\rho \to 1$. Wir setzen dann

$\phi = \phi_{\mathbf{K}} \circ \phi_{\mathcal{R}/\mathbf{K}} \colon \mathcal{R} \circlearrowleft$ mit $\phi_{\mathbf{K}} \colon \mathcal{R} \circlearrowleft$ der Frobenius von $\mathbf{K}$ auf den Koeffizienten.

Definition (Beschränkter und ganzzahliger Unterring). Wir setzen

$$\mathcal{R}^{\mathrm{int}} = \{\sum_{n\in\mathbb{Z}} a_n u^n \in \mathcal{R} : a_n \in \mathbf{o}\} \text{ und } \mathcal{R}^{\mathrm{bdd}} = \{\sum_{n\in\mathbb{Z}} a_n u^n \in \mathcal{R} : \{a_n\} \text{ beschränkt }\}.$$

Wir statten diese Ringe mit der Maximumsnorm aus.

Bemerkung. Der Beweis der Existenz der Anstiegsfiltration (Theorem 3.1) gilt in größerer Allgemeinheit als für die hier vorgestellten Koeffizientenbereiche $\mathbf{K}$ und den Frobenius $\phi\colon \mathscr{R} \curvearrowleft$. Es gilt:

(i) Wir können $\mathbf{K}$ durch einen beliebigen *diskret* bewerteten vollständigen Körper $\mathbf{K}$ ersetzen.

(ii) Wir können $\phi\colon \mathscr{R} \circlearrowleft$ durch einen *Frobenius Lift* ersetzen: Dies ist eine Abbildung

$$\sum_{n\in\mathbb{Z}} a_n u^n \mapsto \sum_{n\in\mathbb{Z}} \phi_{\mathbf{K}}(a_n)\tilde{u}^n,$$

sodass:

(a) Die Abbildung $\phi_{\mathbf{K}}\colon \mathbf{K} \circlearrowleft$ ist eine Isometrie.

(b) Es gilt $\tilde{u} \cong u^q \bmod \mathfrak{m}_{\mathbf{K}}\cdot\mathscr{R}^{\mathrm{int}}$ für ein $q > 1$. (Insbesondere ist $\tilde{u} \in \mathscr{R}^{\mathrm{int}}$ vorausgesetzt.)

Noch allgemeiner: Wir können $\mathscr{R}$ durch einen Ring, der hinreichend viele Eigenschaften mit dem Robba-Ring teilt ersetzen: Die Bezout-Eigenschaft (Jedes endliche erzeugte Ideal ist zyklisch, und damit ist jeder Torsions-freie Modul frei), Erfüllung einer (Bij)-Eigenschaft (siehe weiter unten), Existenz eines Unterrings $\mathscr{R}^{\mathrm{bdd}}$ mit $(\mathscr{R}^{\mathrm{bdd}})^* = \mathscr{R}^*$ usw.

Bemerkung.

- Da $\phi\colon \mathscr{R} \circlearrowleft$ isometrisch auf $\mathscr{R}^{\mathrm{int}} \subseteq \mathscr{R}^{\mathrm{bdd}}$ operiert, werden beide stabilisiert.
- Es ist $\mathscr{R}^{\mathrm{bdd}}$ ein Körper (Theorie der Newton-Polygone) und $\mathscr{R}^* = (\mathscr{R}^{\mathrm{bdd}})^*$. Er ist nicht vollständig, aber zumindest henselsch.

Definition. Ein ϕ-*Modul* M über einem Ring R mit einem Endomorphismus $\phi\colon$ R $\circlearrowleft$ ist ein endlicher freier R-Modul mit einem Isomorphismus $\phi\colon \phi^*\mathrm{M} \to$ M.

Bemerkung.

- Es ist $\phi^*\mathrm{M} = \mathrm{M}\otimes_{\mathscr{R},\phi}\mathscr{R}$ die Skalar*erweiterung* von M mit $r\cdot(m\otimes s) = m\otimes r\cdot s$ und $m \otimes r = \phi(m)\cdot m \otimes 1$. Die Definition besagt, dass $\phi\colon$ M $\circlearrowleft$ eine ϕ-semilineare Abbildung mit invertierbarer darstellender Matrix A ist.
- Beachte: Sind f,g beide ϕ-semilinear, so ist $f \circ g$ dann ϕ^2-semilinear.

- Die Anforderung, dass A invertierbar ist, ist der bestmögliche Ersatz der Bijektivität von $\phi\colon M \circlearrowleft$ unter der Voraussetzung, dass $\phi\colon \mathscr{R} \circlearrowleft$ es nicht notwendigerweise ist. Wir haben aber:
  - Es gilt: A ist invertierbar $\iff$ $\operatorname{im}\phi$ erzeugt M als R-Modul.
  - Sei $\phi\colon R \circlearrowleft$ ein Isomorphismus. Es gilt: A ist invertierbar $\iff$ ϕ ist surjektiv $\iff$ ϕ ist injektiv $\iff$ ϕ ist bijektiv.

Formulierung des Anstiegsfiltrationstheorems

Definition.

- Ein ϕ-Modul M über $\mathscr{R}$ ist *étale* oder *rein vom Anstieg* 0, falls M durch Skalarerweiterung eines ϕ-Moduls M_{int} über $\mathscr{R}^{\text{int}}$ entsteht.
- Ein ϕ-Modul M ist *rein vom Anstieg* r/s, falls der ϕ-Modul $\pi^{-s}\phi^r\colon M \circlearrowleft$ étale ist.

Bemerkung.

(i) Das heißt M ist étale, falls $\phi\colon M \circlearrowleft$ eine darstellende Matrix mit Koeffizienten in $\mathscr{R}^{\text{int}}$ besitzt.

(ii) Wir zeigen, dass diese Begriffe jene über einem bewerteten Körper $\mathbf{K}$ mit dem isometrischem Automorphismus $\phi\colon \mathbf{K} \circlearrowleft$ nachbilden: Der *erste Anstieg* (= „größte Bewertung eines Eigenwerts“) eines ϕ-Moduls V ist definiert durch

$$v_{\text{sp}}(\phi) := \lim_{n\to\infty} 1/n \cdot v(\phi^n) \qquad \text{mit } v(\phi^n) := \min_{x\in V} v(\phi^n \cdot x) - v(x)$$

für eine beliebige Bewertung v von V. (Der Limes-Prozess macht diese Invariante unabhängig von der Wahl von v, da all solche Bewertungen äquivalent sind.)
Der *Anstieg* (= „durchschnittliche Bewertung eines Eigenwerts“) von V ist definiert durch

$$\mu(V) = v_{\text{av}}(\phi) := v(\det(\phi))/r,$$

falls r der Rang von V ist.
Wir nennen V *rein vom Anstieg* $\mu(V)$, falls

$$v_{\text{sp}}(\phi) = v_{\text{av}}(\phi).$$

Dies ist genau dann der Fall, wenn für $\tilde{\phi} := \pi^{-s}\phi^r : V \circlearrowleft$ gilt, dass $v(\tilde{\phi}(x)) = v(x)$ für alle $x \in V$ und damit V durch Skalarerweiterung eines ϕ-Moduls über $\mathbf{o}$ entstanden ist.

(iii) In diesem Sinne ist ein ϕ-Modul M über $\mathscr{R}$ rein vom Anstieg $\mu(M)$, falls M durch Skalarerweiterung eines im obigen Sinne reinen ϕ-Moduls über dem Körper $\mathscr{R}^{\mathrm{bdd}}$ mit Anstieg $\mu(M)$ entsteht.

Theorem 3.1 (Kedlayas Anstiegsfiltration). *Sei* M *ein* ϕ*-Modul über* $\mathscr{R}$*. Dann existiert eine eindeutige Filtrierung*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_r = M$$

durch ϕ*-Untermoduln, sodass die Graduierungsschritte* M_i/M_{i-1} *alle* ϕ*-Moduln über* $\mathscr{R}$ *sind und rein von wachsendem Anstieg* $s_1 < \ldots < s_r$*.*

Konstruktion der Anstiegsfiltration

Wir verfolgen folgende Strategie zur Konstruktion der Anstiegsfiltration:

(i) Konstruktion der Harder-Narasimhan(NH)-Filtration mit semistabilen Graduierungsschritten.

(ii) Semistabilität impliziert Reinheit.

Bemerkung. Wir merken an, dass sogar die Begriffe Semistabilität und Reinheit über dem Robba-Ring sogar äquivalent sind (und für die Eindeutigkeit der Anstiegsfiltration auch benötigt wird!). Die Implikation 'Rein $\Longrightarrow$ Semistabil' ist leichter zu zeigen als die hier betrachte Implikation. Aus der Äquivalenz dieser Begriffe ergibt sich dann sofort die Eindeutigkeit der Anstiegsfiltration aus der Eindeutigkeit der gleich folgenden Harder-Narasimhan-Filtration.

Die HN-Filtration

Definition. Für einen ϕ-Modul M über $\mathscr{R}$ vom Rang r sei

$$\mu(M) := v(\det(\phi))/r$$

der *Anstieg* von M. Dann heißt M *semistabil*, falls $\mu(N) \geq \mu(M)$ für jeden Untermodul N.

Bemerkung. Da $\mathscr{R}^* = \mathscr{R}^{\mathrm{bdd}^*}$ und Basiswechsel die Bewertung $v(\det(A))$ für eine darstellende Matrix A von ϕ nicht ändert, ist $\mu(M)$ wohldefiniert.

Satz 3.2 (HN-Filtration). *Jeder* ϕ*-Modul* M *über* $\mathscr{R}$ *hat eine eindeutige Filtration durch* ϕ*-Untermoduln*

$$0 = M_0 \subset M_1 \subset \ldots \subset M_r = M$$

mit semistabilem Graduierungsschritt M_i/M_{i-1} *von wachsendem Anstieg* $\mu(M_1/M_0) < \ldots < \mu(M_r/M_{r-1})$.

Beweis: Der Beweis erfolgt in vier Schritten.
1.: Die Menge $A := \{\mu(N) : N \subseteq M$ von Null verschiedener ϕ-Untermodul$\}$ ist nach unten beschränkt.
2.: Nach Definition sind ϕ-Untermoduln gleichen Anstiegs unter Summenbildung abgeschlossen.
3.: Da A diskret ist, existiert nach dem 1. und 2. Schritt ein maximaler Untermodul $M_1 \subseteq M$ kleinsten Anstiegs.
4.: Finde in $\bar{M} := M/M_1$ durch den 3. Schritt erneut einen maximalen ϕ-Untermodul $\bar{M}_2$. Definiere $M_1 \subseteq M_2 \subseteq M$ durch das Urbild der kanonischen Projektion; und so weiter und so fort. □

Semistabilität impliziert Reinheit

Wir verfolgen folgende Strategie zum Beweis der Implikation 'Semistabil $\Longrightarrow$ Rein':

(i) Konstruktion eines größeren Robba-Rings $\tilde{\mathscr{R}} \supseteq \mathscr{R}$ über dem jeder étale ϕ-Modul trivial ist. (Oder äquivalent dazu — und hier nicht benutzt — eine Dieudonne'-Manin Klassifikation ermöglicht.)

(ii) Beweis der Implikation über $\tilde{\mathscr{R}}$.

(iii) Benutze treuflachen Abstieg, um zu zeigen, dass für jeden $\mathscr{R}$-Modul M gilt, dass

  (a) Ist M semistabil, so auch $M \otimes_{\mathscr{R}} \tilde{\mathscr{R}}$.

  (b) Ist $M \otimes_{\mathscr{R}} \tilde{\mathscr{R}}$ rein, so auch M.

Der große Robba-Ring.

Definition. Wir wollen nun $\tilde{\mathcal{R}} \supseteq \mathcal{R}$ erklären.

(i) Wir ersetzen zunächst $\mathbf{K}$ durch seinen *Differenzen-Abschluss*, seine kleinste diskret bewertete vollständige Körperweiterung über die jeder étale ϕ-Modul trivial ist (und somit eine Dieudonne'-Manin-Klassifikation ermöglicht). Wenn wir $\mathbf{K} = \mathbf{K}_0$ als unverzweigten p-adischen Zahlkörper voraussetzen, ist dies durch die Erweiterung $\mathrm{W}(\bar{\mathbf{k}})[1/p] \supseteq \mathbf{K}_0$ der Fall.

(ii) Sei dazu $\tilde{\mathcal{R}}$ die Menge aller $f = \sum_{i \in \mathbb{Q}} a_i t^i$, sodass ein $0 < \alpha = \alpha(f)$ existiert mit:

  (a) Die Summe existiert für $t \mapsto x \in \mathrm{D}([\alpha,1[)$. (Nachbildung der Konvergenzeigenschaft des Robba-Rings.)

  (b) Für jedes $c > 0$ ist die Menge $\{i : |a_i| \geq c\} \subseteq \mathbb{Q}$ wohl-geordnet. (Für die Wohldefiniertheit der Multiplikation erforderlich.)

  Wir versehen $\tilde{\mathcal{R}}$ mit dem Frobenius $\phi\colon \tilde{\mathcal{R}} \circlearrowleft$ definiert als Hintereinanderschaltung $\phi = \phi_{\tilde{\mathcal{R}}/\mathbf{K}} \circ \phi_{\mathbf{K}}$. Hierbei ist $\phi_{\tilde{\mathcal{R}}/\mathbf{K}} : \tilde{\mathcal{R}} \circlearrowleft$ gegeben durch $t^i \mapsto t^{iq}$ und $\phi_{\mathbf{K}}\colon \tilde{\mathcal{R}} \circlearrowleft$ der Frobenius auf den Koeffizienten.

(iii) Es seien $\tilde{\mathcal{R}}^{\mathrm{int}} \subseteq \tilde{\mathcal{R}}^{\mathrm{bdd}} \subseteq \tilde{\mathcal{R}}$ die Teilringe mit ganzzahligen bzw. beschränkten Koeffizienten.

Bemerkung.

- Es wird im folgenden wichtig sein, dass $\tilde{\mathcal{R}}$ mit $\mathcal{R}$ die Eigenschaften Bezout und (Bij) teil — siehe hierzu weiter unten.
- Es ist $\tilde{\mathcal{R}}^{\mathrm{bdd}} \subseteq \tilde{\mathcal{R}}$ ein henselscher diskret bewerteter Körper und $(\tilde{\mathcal{R}}^{\mathrm{bdd}})^* = \tilde{\mathcal{R}}^*$.
- Damit ist $\phi\colon \tilde{\mathcal{R}} \circlearrowleft$ bijektiv. Weiterhin ist der Restklassenkörper $\mathbf{k}_{\tilde{\mathcal{R}}^{\mathrm{bdd}}} = \mathbf{k}((t^{\mathbb{Q}}))$ algebraisch abgeschlossen. (Diese Eigenschaften sind wichtig um zeigen zu können, dass jeder ϕ-Modul über $\tilde{\mathcal{R}}^{\mathrm{int}}$ bereits trivial ist. Dies kommt im zweiten Teil des Beweises der Implikation zum Einsatz, in der wir zeigen, dass wir in einem semistabilen ϕ-Modul stets einen echten ϕ-Untermodul mit gleicher Steigung finden können.)

Annahme. Im Folgenden denken wir uns den Begriff des ϕ-Modules und deren Reinheit bzw. Semistabilität über $\tilde{\mathcal{R}}$ analog zu denen über $\mathcal{R}$ formuliert.

Die (Bij)-Eigenschaft.

Satz. *Der Ring* $\tilde{\mathrm{R}}$ *erfüllt die* (Bij)-Eigenschaft*: Für jeden* ϕ*-Modul* M *über* $\tilde{\mathrm{R}}^{int}$ *ist die von*

$$\check{\phi} := \mathrm{id} - \phi \colon \mathrm{M} \circlearrowleft$$

auf $\mathrm{M} \otimes \tilde{\mathcal{R}}/\mathrm{M} \otimes \tilde{\mathcal{R}}^{bdd}$ *induzierte Abbildung* bijektiv.

Korollar 3.3. *Jede Erweiterung etaler* ϕ*-Moduln über* $\tilde{\mathcal{R}}$ *ist étale, das heißt: Ist*

$$0 \to \mathrm{M}' \longrightarrow \mathrm{M} \longrightarrow \mathrm{M}'' \to 0$$

eine kurze exakte Sequenz mit M′ *und* M″ *étale, so ist* M *étale.*

Beweis: Sei $\mathrm{R} = \tilde{\mathcal{R}}, \tilde{\mathcal{R}}^{\mathrm{bdd}}$ oder $\tilde{\mathcal{R}}^{\mathrm{int}}$. Wir haben

$$\mathrm{Ext}^1(\mathrm{M},\mathrm{N}) = \mathrm{H}^1(\mathrm{M}^\wedge \otimes_{\mathrm{R}} \mathrm{N}) \quad \text{für } \phi\text{-Moduln M,N über R}$$

mit

$$\mathrm{H}^1(\mathrm{V}) := \mathrm{coker}(\mathrm{id} - \phi)$$

für jeden ϕ-Modul V über R. (Hierbei ist $\mathrm{M}^\wedge := \mathrm{Hom}_{\phi\text{-mod.}}(\mathrm{M},\mathrm{R})$ der ϕ-Modul der R-linearen mit $\phi \colon \mathrm{M} \circlearrowleft$ und $\phi \colon \mathrm{R} \circlearrowleft$-kompatiblen Homomorphismen $\mathrm{M} \to \mathrm{R}$.)

Daher genügt es zu zeigen, dass für die Abbildung $\check{\phi} := \mathrm{id} - \phi : \mathrm{M}$ auf einem ϕ-Modul M über $\tilde{\mathcal{R}}^{\mathrm{int}}$ gilt, dass

$$\mathrm{coker}\,\check{\phi} \otimes \tilde{\mathcal{R}}^{\mathrm{bdd}} \twoheadrightarrow \mathrm{coker}\,\check{\phi} \otimes \tilde{\mathcal{R}}.$$

Dies ist die Surjektivität in der Formulierung der Eigenschaft (Bij). □

Bemerkung. Wir können das Korollar griffig so formulieren, dass aus der Surjektivität in der Formulierung von (Bij) - sozusagen (Surj) - folgende Surjektion folgt:

$\{\text{Erweiterungen reiner } \phi\text{-Moduln über } \tilde{\mathcal{R}}^{\mathrm{bdd}}\} \twoheadrightarrow \{\text{Erw. reiner } \phi\text{-Moduln über } \tilde{\mathcal{R}}\}$.

Beweis der Implikation.

Satz. *Jeder semistabile* ϕ*-Modul* M *ist rein.*

Beweis: Wir können ohne Einschränkung nach Twists, die weder die Semistabilität noch Reinheit berühren, annehmen, dass $\mu(M) = 0$. Wir müssen nun zeigen, dass M étale ist. Durch Induktion über den Rang r von M genügt es durch folgende Überlegung hierzu einen etalen ϕ-Untermodul $N \subseteq M$ vom Rang 1 zu finden:
In diesem Fall haben wir nämlich eine exakte Sequenz

$$0 \longrightarrow N \longrightarrow M \longrightarrow \bar{M} \longrightarrow 0\,.$$

Da $\mu(N) = \mu(M) = 0$, gilt damit auch $\mu(\bar{M}) = 0$. Weil $\bar{M}$ wiederum semistabil ist, ist er nach Induktionsvoraussetzung rein, also étale. Somit ist N und $\bar{M}$ étale und damit ist nach Korollar 3.3 auch M étale.

Es ist nun zu zeigen:

(i) Es existiert ein ϕ-Untermodul $N \subseteq M$ vom Rang 1.

(ii) Unter all solchen existiert einer mit $\mu(N) = 0$.

Ad 1.: Die Existenz von N meint die eines Eigenvektors von ϕ, das heißt es genügt ein $m \in M$ mit $\phi(m) = \pi^{\mathbf{k}} m$ für $k \gg 0$ zu finden (Notwendigerweise positiv, da M semistabil!).
Es gilt

$$\phi(m) = \pi^{\mathbf{k}} m \iff F(v) = v \iff \check{F}(v) = 0 \quad \text{mit} \quad F = \pi^{-k} A\phi \text{ und } \check{F} = F - 1;$$

hier identifizieren wir $M = \tilde{\mathcal{R}}^d$ und $\phi = A\phi$. Habe A Einträge in $\tilde{\mathcal{R}}_{[\rho^q,1[}$. Dann möchten wir eine in $\tilde{\mathcal{O}}_{[\rho,\rho]}$ konvergente Folge $v_n \to v \neq 0$ konstruieren mit $\check{F}(v_n) =: w_n \to 0$. Wegen $\phi v = \pi^k v$ gilt dann $v \in \tilde{\mathcal{O}}^d_{[\rho,\sqrt[q]{\rho}[}$ und iterativ $\mathcal{O}^d_{[\rho,\sqrt[q^n]{\rho}[}$ für alle $n \in \mathbb{N}$. Damit also $v \in \tilde{\mathcal{O}}^d_{[\rho,1[} \subseteq \tilde{\mathcal{R}}^d$.

Wir setzen dazu rekursiv

$$v_{n+1} = v_n + f(w_n)$$

mit einer noch zu bestimmenden Funktion $f : M \circlearrowleft$. Um $w_n \to 0$ zu gewährleisten, möchten wir gerne, dass $|w_{n+1}|_\rho < |w_n|_\rho$. Es gilt

$$w_{n+1} = \check{F}(v_{n+1}) = w_n + \check{F}(f(w_n)).$$

Es erscheint nun plausibel, dass f so gewählt ist, dass $\check{F}(f(w_n))$ einerseits den Summand w_n aufhebt, andererseits der verbleibende Ausdruck echt kleiner ist.

Um letztes zu gewährleisten, benutzen wir, dass $\phi\colon \tilde{\mathcal{O}}_{[\rho,\rho]} \circlearrowleft$ auf den positiven Potenzen bzw. von $\phi^{-1}\colon \tilde{\mathcal{O}}_{[\rho,\rho]} \circlearrowleft$ auf den negativen Potenzen die Norm $|\cdot|_\rho$ verkleinert: Für $f = \sum_{i\in\mathbb{Q}} a_i t^i \in \tilde{\mathcal{R}}$ sei hierzu

$$f^+ = \sum_{i\geq d} a_i t^i \quad \text{und} \quad f^- = \sum_{i<d} a_i t^i.$$

Diese Definition überträgt sich komponentenweise auf Spaltenvektoren $v \in \mathrm{M}$. Wir setzen nun

$$f = \cdot^+ - \mathrm{F}^{-1}\cdot^- .$$

Dann gilt

$$w_{n+1} = w_n + \check{\mathrm{F}}(f(w_n)) = w_n + \mathrm{F} - 1(w_n^+ - \mathrm{F}^{-1}w_n^-) = \mathrm{F}w_n^+ + \mathrm{F}^{-1}w_n^- = g(w_n)$$

mit $g := \mathrm{F}\cdot^+ + \mathrm{F}\cdot^-$. Wählen wir nun d in der Definition von $\mathrm{id} = \cdot^+ + \cdot^-$ geschickt, so ist tatsächlich g kontrahierend und damit $w_n \to 0$. Es gilt

$$\|g(w)\|_\rho = \|g(w^+) + g(w^-)\|_\rho.$$

Wir schätzen ab:

$$\begin{aligned}\|gw^+\|_\rho &\leq \max(\|\mathrm{F}w^+\|_\rho \\ &= |\pi|^{-k}\|\mathrm{A}\phi(w^+)\|_\rho \leq |\pi|^{-k}\|\mathrm{A}\|_\rho\|\phi(w^+)\|_\rho \leq |\pi|^{-k}\|\mathrm{A}\|_\rho\rho^{d(q-1)}\|w^+\|_\rho\end{aligned}$$

und

$$\begin{aligned}\|gw^-\|_\rho &\leq \|\mathrm{F}^{-1}w^-\|_\rho \\ &\leq |\pi|^{k}\|\phi^{-1}\mathrm{A}^{-1}(w^-)\|_\rho \leq |\pi|^{k}\|\mathrm{A}^{-1}\|_{\rho^q}\|\phi^{-1}(w^-)\|_\rho \leq |\pi|^{k}\|\mathrm{A}^{-1}\|_\rho\rho^{d(q^{-1}-1)}.\end{aligned}$$

Somit gilt für die Operator-Norm

$$\|g\|_\rho \leq \max\{|\pi|^{-k}\|\mathrm{A}\|_\rho\rho^{d(q-1)}, |\pi|^{k}\|\mathrm{A}^{-1}\|_\rho\rho^{d(q^{-1}-1)}\}.$$

Wir wollen also, dass $\mathrm{C}\eta^d, \mathrm{C}^{-1}\theta^d = \mathrm{C}^{-1}\eta^{-d}(\theta\eta)^d < 1$ mit $0 < \eta < 1 < \theta$ und $\eta\theta < 1$, wobei $\mathrm{C} = \mathrm{C}(k) = |\pi|^{-k}\|\mathrm{A}\|_\rho$ und $\eta = \rho^{q-1}$ und $\theta = \rho^{q^{-1}-1}$. Es ist also $\mathrm{C} = \mathrm{C}(k) \gg 0$ und d zu finden, sodass $(\theta\eta)^d < \mathrm{C}\eta^d < 1$ oder äquivalent dazu $\theta^d < \mathrm{C} < (1/\eta)^d$. Wegen $\theta < 1/\eta$ ist diese Ungleichung sicher erfüllbar.

Somit gilt für diese Wahl von k und d daher $w_n \to 0$ und damit $\mathrm{F}v_n \to v$. Wählen wir etwa $v_0 = (u^d, 0, \ldots, 0)$, so ist $v \neq 0$. Dies liefert den gewünschten Eigenvektor.

Ad 2.: Wir haben nun zu zeigen, dass wir einen solchen zyklischen ϕ-Untermodul $\mathrm{N} \subseteq \mathrm{M}$ von minimalem Anstieg 0 finden können.

Hierzu benötigen wir zur Vorbereitung etwas Strukturtheorie der ϕ-Moduln über $\tilde{\mathrm{R}}$.

Satz 3.4. *Jeder étale* ϕ*-Modul über* $\tilde{\mathcal{R}}$ *ist trivial.*

Beweis: Hier geht entscheidend ein, dass $\phi\colon \tilde{\mathcal{R}} \circlearrowleft$ bijektiv operiert und der Restklassenkörper $\mathbf{k}((t^{\mathbb{Q}}))$ des komplettierten Ringes $\hat{\tilde{\mathcal{R}}}^{\mathrm{int}}$ algebraisch abgeschlossen ist. Unter diesen Voraussetzungen gilt nämlich, dass nach dem allgemeinen Argument [Scho9, Korollar 2.2] jeder ϕ-Modul über $\mathbf{k}((t^{\mathbb{Q}}))$ und damit wegen der Kategorienäquivalenz durch den Wittvektoren-Funktor über $\hat{\tilde{\mathcal{R}}}^{\mathrm{int}}$ trivial ist. Dann lässt sich durch [Kedo8, Proposition 2.5.8] zeigen, dass dies bereits über $\tilde{\mathcal{R}}^{\mathrm{int}}$ gilt. □

Über einem diskret bewerteten vollständigen Körper haben reine ϕ-Moduln M,N mit $\mathrm{Hom}_{\phi\text{-mod.}}(M,N) \neq 0$ stets $\mu(M) = \mu(N)$. Über $\tilde{\mathcal{R}}$ gilt nur die Abschwächung $\mu(M) \geq \mu(N)$. Dies ist bestmöglich:

Satz 3.5. *Seien* M,N *reine* ϕ*-Moduln über* $\tilde{\mathcal{R}}$ *und* $\mu(N) > \mu(M)$. *Dann gilt*

$$\mathrm{Hom}_{\phi\text{-}mod.}(N,M) \neq 0.$$

Exempel. Betrachte etwa den trivialen ϕ-Modul $M = \mathcal{R} \cdot e$. Dann ist $x := \log(1+t) \in \mathcal{R}$ und es gilt $\phi(x) = p \cdot x$. Somit $\mu(N) = 1 > 0 = \mu(M)$ für $N := \mathcal{R} \cdot (xe) \subset M$.

Sei nun c der minimale Anstieg all solcher ϕ-Untermoduln. Indem wir den ϕ-Modul M durch den ϕ^r-Modul $\tilde{M} := [r]_* M$ definiert durch $\phi^r\colon M \circlearrowleft$ ersetzen, gilt dann notwendigerweise $c \in \mathbb{N}$. Wir möchten $c = 0$ zeigen.
Angenommen $c > 0$. Durch Twisten können wir ohne Einschränkung $c = 1$ annehmen, bezeugt etwa durch den ϕ^r-Modul $\tilde{N} \subseteq \tilde{M}$.
Dann erhalten wir durch Adjunktion einen Homomorphismus von ϕ-Moduln $N := [r]^* \tilde{N} \xrightarrow{f} M$ mit $[r]^*$ der adjungierte Funktor zu $[r]_*$. [Fasst man ϕ-Moduln/$\tilde{\mathcal{R}}$ als Moduln über dem ϕ-getwisteten Polynomring $\tilde{\mathcal{R}}[T]$ auf, so ist $[a]_*$ die Skalar-Einschränkung von T auf T^a und $[a]^*$ die Skalar-Erweiterung (per Tensorprodukt) von T^a zu T.] Wir unterscheiden die beiden folgenden Fälle.

1. Fall: $\mu(f(N)) < 1/r$. Wegen $\mathrm{rank}\, f(N) < r$ gilt dann schon $\mu(f(N)) \leq 0$. Dann können wir aus der Strukturtheorie der ϕ-Moduln über $\tilde{\mathcal{R}}$ folgern, dass $H^0(f(N)) = \{x \in f(N) : \phi x = x\} \neq 0$ gilt:
Sei nach Induktionsannahme $f(N)_1$ der erste Schritt der Anstiegsfiltration von $f(N)$. Wir unterscheiden die beiden folgenden Fälle.

1.1. Fall: Es ist $\mu(f(N)_1) = 0$. Dann ist also $f(N)_1$ rein und vom Anstieg 0, das heißt étale. Wegen Satz 3.4 ist dann der ϕ-Modul $f(N)_1$ trivial.

1.2. Fall: Es ist $\mu(f(N)_1) < 0$. Wegen Satz 3.5 ist dann $\mathrm{Hom}_{\phi\text{-mod.}}(E, f(N)_1) \neq 0$ für alle ϕ-Moduln E mit $\mu(E) > \mu(f(N)_1)$. Damit enthält $f(N)_1$ wiederum einen ϕ-Fixvektor.

2. Fall: $\mu(f(N)) = 1/r$. Dann zeigt eine langwierige Rechnung (siehe [Kedo8, Proposition 2.1.7]), dass M einen ϕ-Fixvektor hat.

□

Der treuflache Abstieg.

Satz. *Sei* M *ein* ϕ*-Modul über* $\mathscr{R}$. *Dann gilt:*

(i) *Ist* M *semistabil, so auch* $M \otimes_{\mathscr{R}} \tilde{\mathscr{R}}$.

(ii) *Ist* $M \otimes_{\mathscr{R}} \tilde{\mathscr{R}}$ *rein, so auch* M.

Literatur

[Ked08] K. S. Kedlaya, *Slope filtrations for relative Frobenius*, Astérisque (2008), no. 319, 259–301, Représentations p-adiques de groupes p-adiques. I. représentations galoisiennes et (ϕ,Γ)-modules. MR 2493220.

[Sch09] P. Schneider, *Die Theorie des Anstiegs*, 2008/09. Confer http://wwwmath.uni-muenster.de/u/schneider.

Westfälische Wilhelms-Universität Münster, Einsteinstrasse 62, 48149 Münster
e-mail address: enno.nagel@math.uni-münster.de