Anwendung deformationstheoretischer Methoden zur Liftung des Frobeniusmorphismus

Dissertation zur Erlangung des Grades eines Doktors der Naturwissenschaften

Dem Fachbereich 6
(Mathematik und Informatik)
der Universität Duisburg-Essen

vorgelegt von
Maxim Li
Geboren in Odessa (Ukraine)

Wiesbaden, 24. März 2008

Dissputationstag 6 August 2008
Begutachter: Prof. Dr. Frey, Prof. Dr. Green

Vorwort

Punktezählproblem:
Als Motivation für diese Arbeit dient das Punktezählproblem - das darin besteht, die Anzahl der rationalen Punkte einer Varietät zu bestimmen, wobei diese Varietät über einen endlichen Körper definiert ist.

Dieses Problem hat sowohl eine große theoretische Bedeutung im Zusammenhang mit der Weilschen Zetafunktion als auch wichtige praktische Anwendungen im Bereich der assymetrischen Kryptographie. Diese beiden Seiten des Punktezählproblems beschreiben wir in dem ersten, einführenden Kapitel.

Im letzten Jahrzehnt entstand eine neue Klasse von effizienten p-adischen Punktezählalgorithmen, die auf den Algorithmen von Satoh [Sat] und Kedlaya [Kedl] basieren. Die Algorithmen aus diesen Klassen bestehen aus zwei folgenden Schritten:

1. Berechnung einer p-adischen Liftung $\tilde{F}$ des Frobeniusmorphismus
2. Berechnung der Zetafunktion (bzw. der Anzahl der rationalen Punkte) durch die Betrachtung der von $\tilde{F}$ induzierten Operation auf bestimmten, in Charakteristik 0 definierten, Darstellungsräumen

Im Algorithmus von Kedlaya wird dabei die Monsky-Washnitzer Kohomologie und im Algorithmus von Satoh der Raum der holomorphen Differentialen auf der kanonischen Liftung einer elliptischen Kurve als Darstellungsraum verwendet.

Zielsetzung:
Als Ausgangspunkt dieser Arbeit diente der Liftungsschritt im Kedlaya-Algorithmus (in dem der Frobeniusmorphismus auf den gewissen affinen hyperelliptischen Kurven über den p-adischen Ring $\mathbb{Z}_q$ geliftet wird), sowie zwei folgende triviale Bemerkungen:

- Liftung des Frobeniusmorphismus wird mit einer endlichen p-adischen Genauigkeit berechnet, so dass man eigentlich eine Liftung über den endlichen Quotientenringen $\mathbb{Z}_q/p^n\mathbb{Z}_q$ erhält.

- Liftung des Frobeniusmorphismus auf affinen Varietäten ist nicht eindeutig und die Wahl der Liftung im Algorithmus war ausschließlich durch die schnelle Konvergenz der (bei der Berechnung auftretenden) Potenzreihen motiviert.

- Auch die Wahl der verwendeten affinen Kurven ist durch den Liftungsalgorithmus beeinflüßt.

Diese Beobachtungen führten zu den folgenden Zielsetzungen:

1. Möglichst explizite Parametrisierung aller Liftungen des Frobeniusmorphismus auf affinen Varietäten über den p-adischen Quotientenringen $W(k)/p^nW(k)$.

2. Identifizierung der Liftungen mit vorgegebenen Eigenschaften, zum Beispiel optimiert für den zweiten Schritt des Punktezählalgorithmus.

3. Effiziente Berechnung dieser Liftungen.

Es kamen einige Erweiterungen hinzu, wie zum Beispiel die Verallgemeinerung auf beliebige affine Morphismen oder die Liftung des projektiven Frobeniusmorphismus.

Deformationstheoretische Methoden
Die Liftungen über den p-adischen Quotientenringen kann man als infinitesimale Deformationen auffassen. Diese Tatsache legt es nahe, die deformationstheoretischen Ideen und Methoden für die Parametrisierung der Liftungen anzuwenden.

In der Deformationstheorie hat man viele Beispiele für die Beschreibung des Raumes der infinitesimalen Deformationen erster Ordnung, die oft durch eine Isomorphie zu leicht berechenbaren Tangentialräumen gegeben ist. Diese Deformationen erster Ordnung entsprechen den "kleinen" ($/p^{n-1} \to /p^n$) Liftungen, bei denen die p-adischen Genauigkeit um 1 erhöht wird.

Im Abschnitt 2.3 wenden wir die Techniken der Berechnung der Deformationen ersten Ordnung auf die "kleinen" Liftungen der Homomorphismen zwischen endlich erzeugten Algebren und erhalten dadurch eine Isomorphie des Liftungsraumes zu einem gewissen Derivationsmodul. Diese Beschreibung der kleinen Liftungen ist allerdings nicht unmittelbar geeignet für die praktische Berechnung.

Explizite Parametrisierung der affinen Liftungen
Im Kapitel 3 geben wir eine explizite Parametrisierung der kleinen Liftungen der Morphismen zwischen affinen Varietäten (bzw. der induzierten Homomorphismen zwischen Koordinatenringen) durch eine 1-zu-1 Korrespondenz zu den Lösungen eines linearen Gleichungssystems über einem Koordinatenring in Charakteristik p.

Diese Beschreibung der Liftungen erhalten wir dadurch, dass wir zunächst einen größeren Raum der leicht berechenbaren "quasi-Liftungen" parametrisieren und anschließend solche Parameter finden, für die bestimmte "Hindernisse" verschwinden und wir die gesuchten Liftungen erhalten.

Die Parametrisierung der Liftungen, sowie den entwickelten Liftungsalgorithmus wenden wir im Kapitel 4 auf die Liftungen des Frobeniusmorphismus auf affinen hyperelliptischen Kurven an. An diesem Beispiel zeigen wir wie man die Parametrisierung für die Berechnung der Liftungen mit gewünschten Eigenschaften anwenden kann, indem die Grade der Liftungen minimiert werden.

Die durch diese Optimierung entstehende Liftung ermöglicht eine viel schnellere Durchführung des zweiten Schrittes des Punktezählalgorithmus, sowie die Verbesserung des gesamten Algorithmus. Diese Anwendung, sowie die Laufzeit- und Komplexitätsfragen werden im Abschnitt 4.5 diskutiert.

Erweiterungen und Anwendungen
Eine mögliche Erweiterung der entwickelten Methoden für die Liftung der Morphismen zwischen projektiven Varietäten zeigen wir im Kapitel 5 am Beispiel der elliptischen Kurven und der kanonischen Liftung des Frobeniusmorphismus. Dafür betrachten wir eine affine Überdeckung der projektiven Kurve, und deformieren die Parametrisierungsräume der kleinen Liftungen auf affinen Karten so, dass diese affine Liftung sich auf den Durchschnitten verkleben und wir eine projektive Liftung erhalten.

Die Liftung eines glatten projektiven Morphismus induziert insbesondere eine Operation auf den holomorphen Differentialen. Im Kapitel 6 untersuchen wir solche affine Liftung des Frobeniusmorphismus auf elliptischen Kurven, die eine lineare Operation auf diesen Differentialen induzieren. Aus der hergeleiteten Beschreibung solcher Liftungen folgt insbesondere eine gute Schätzung für die Grade der kanonischen Liftung des Frobeniusmorphismus,

sowie ein expliziter Beweis der Tatsache, dass es keine kanonische Liftungen auf supersingulären elliptischen Kurven gibt.

Die weiteren Anwendungs- und Erweiterungsmöglichkeiten, wie zum Beispiel eine direkte Liftung der Operation auf Differentialen, diskutieren wir im letzten Abschnitt 6.4.

Danksagungen:
Als erstes möchte ich meinem Doktorvater Prof. Dr. Gerhard Frey für gute Betreuung danken, die mir sowohl den mit großem Vertrauen ausgestatteten Freiraum gab, zugleich aber auch meine Arbeit durch wichtige fachliche Impulse lenkte und durch ständige Aufmunterungen voran brachte.

Weiterhin möchte ich mich bei der Arbeitsgruppe „Zahlentheorie“ am Institut der experimentellen Mathematik in Essen und vor allem beim Dr. Ralf Gerkmann für die zahlreichen Diskussionen sowie wichtige Bemerkungen und Anregungen zu der Arbeit bedanken.

Ein weiterer Dank gilt dem Graduiertenkolleg „Mathematische und ingenieurwissenschaftliche Methoden für sichere Datenübertragung und Informationsvermittlung“, der diese Arbeit finanziell unterstützte und insbesondere einen guten Überblick über die vielen Brücken zwischen Theorie und Praxis verschaffte.

Ein besonderer Dank gilt meiner Frau und meinen Eltern, ohne deren Engagement diese Arbeit nie beendet wäre.

Inhaltsverzeichnis

Kapitel 1

p-adische Punktezählalgorithmen

Dieses einführendes Kapitel beginnt mit einer kurzen Übersicht über die kryptographischen Anwendungen des Punktezählproblems. Anschließend beschreiben wir den theoretischen Hintergrund des Problems sowie das Punktezählalgorithmus von Kedlaya.

1.1 Kryptographische Anwendungen

Die kryptographische Relevanz der Punktezählalgorithmen basiert auf der Anwendung der Gruppe der rationalen Punkte als Basis für assymetrische Kryptosysteme, die wir in diesem Abschnitt beschreiben. Für eine ausführliche Beschreibung der Kryptographie auf elliptischen und hyperelliptischen Kurven verweisen wir auf [FC$^+$].

In der klassischen Kryptographie wurden zum verschlüsselten Nachrichtenaustausch lange Zeit ausschließlich die symmetrischen Verfahren eingesetzt, die dasselbe geheime Schlüssel für Ver- und Entschlüsselung verwenden. Das Prinzip der assymetrischen Kryptographie (mit der Aufteilung in "Public Key" und "Secret Key") wurde erst in den 70-er Jahren in der Arbeit von Diffie und Hellman [DH] entwickelt. Dies führte insbesondere zu der Lösung des alten Problems des sicheren Austausches eines gemeinsamen geheimen Schlüssels. Zusätzlich wurden die Möglichkeiten für die Authentifizierung, Sicherung der Datenintegrität und die Erzeugung der digitalen Signaturen geschaffen.

Für die Konstruktion der assymetrischen Kryptosysteme benötigt man sogenannte (Trapdoor-)Einwegfunktionen. Diese Funktionen sollen leicht berechenbar sein, die Invertierung soll allerdings ein sehr schweres, praktisch unlösbares, Problem darstellen, sofern man eine zusätzliche Information (Trapdoor) nicht besitzt. Eine solche Einwegfunktion ist gegeben durch die Multiplikation von großen Primzahlen, da die Faktorisierung eines solchen Produktes ein schweres algorithmisches Problem darstellt. Auf dieser Grundlage basiert das bekannte RSA-Kryptosystem.

Eine weitere wichtige Klasse der Einwegfunktionen besteht aus den diskreten Exponentialfunktionen in einer großen zyklischen Gruppe G. Das zugehörige algorithmisch schwere Problem ist die Bestimmung des diskreten Logarithmus (DLP) in dieser Gruppe. Für a, $b \in G$ soll dabei ein solches $m \in \mathbb{N}$ gefunden werden, so dass

$$a^m = b \text{ in } G \text{ gilt}$$

Die einfache Wahl der zyklischen Gruppe $\mathbb{Z}/p\mathbb{Z}$ als Basisgruppe für ein DLP-basiertes Kryptosystem scheitert in der Praxis an den "Index-Calculus" Angriffen. Deswegen verwendet man die Gruppe der rationalen Punkte bestimmter (abelschen) Varietäten über den endlichen Körpern, für die keine subexponentiale Methoden für die Lösung des DLP bekannt sind.

Auf dieser Grundlage wurden die Kryptosysteme ECC und HECC entwickelt, die die Gruppe der rationalen Punkte der elliptischen Kurven, bzw. der jakobischen Varietäten der hyperelliptischen Kurven als Basisgruppe für das Problem des diskreten Logarithmus verwenden. Diese Kryptosysteme sind zwar rechnerisch aufwendiger als RSA, benötigen allerdings kleinere Schlüsselgrößen bei der gleichen Sicherheit und werden deswegen hauptsächlich bei "Embeded Systems" und insbesondere bei elektronischen Chipkarten eingesetzt.

Für die ausreichende Komplexität des diskreten Logaritmierens verwendet man solche Basiskurven, bei der die Ordnung der Gruppe der rationalen Punkte der Kurve (bzw. deren jakobischen Varietät) einen großen Primteiler hat, damit diese Gruppe eine genügend große zyklische Untergruppe besitzt. Deswegen benötigt man schnelle Punktezählalgorithmen, die bei der Suche nach solchen, für Kryptosysteme geeigneten, Kurven eingesetzt werden.

1.2 Die Zetafunktion und p-adische Punktezählalgorithmen

Dieser Abschnitt beschreibt den theoretischen Hintergrund des Punktezählproblems. Wir geben eine kurze Zusammenfassung der Eigenschaften der Weilschen Zetafunktion und erklären den Zusammenhang zwischen der Zetafunktion und dem Frobeniusendomorphismus. Anschließend skizzieren wir die Idee der p-adischen Punktezählalgorithmen, die die p-adische Kohomologien als Darstellungsräume der induzierten Operation des Frobeniusendomorphismus verwenden.

Weilsche Zetafunktion:
Sei C eine über einem endlichen Körper $\mathbb{F}_q = \mathbb{F}_{p^d}$ definierte Kurve. Wir interessieren uns für die Anzahl der rationalen Punkte der Kurve C und deren jakobischen Varietät J_C über dem Körper $\mathbb{F}_q$, sowie über den Erweiterungskörpern $\mathbb{F}_{q^m}$. Diese Anzahl bezeichnen wir im Folgenden mit $\#C(\mathbb{F}_{q^m})$, bzw. $\#J_C(\mathbb{F}_{q^m})$. Die ganze Information über die Kardinalitäten $\#C(\mathbb{F}_{q^m})$ über den Erweiterungskörpern von $\mathbb{F}_q$ ist im folgenden Objekt erhalten:

Definition 1.2.1. *Die **Zetafunktion** von $C/\mathbb{F}_q$ ist gegeben durch die exponentielle Potenzreihe*

$$Z(t) := Z(C/\mathbb{F}_q, t) = \exp\left(\sum_{m=1}^{\infty} \#(C/\mathbb{F}_{q^m})\frac{t^m}{m}\right) \in \mathbb{Q}[[t]]$$

Ein grundlegendes Theorem, genannt Weil-Vermutungen beschreibt die wichtigsten Eigenschaften der Zetafunktion. Für eine ausführlichere Beschreibung der Zetafunktion verweisen wir auf [Ser1].

Theorem 1.2.2. *Sei C eine Kurve vom Geschlecht g über dem endlichen Körper $\mathbb{F}_q$. Die Zetafunktion von C hat folgende Eigenschaften:*

1. *$Z(t)$ ist eine rationale Funktion*
2. *Z erfüllt die Funktionalgleichung $Z(t) = q^{g-1} \cdot t^{2g-2} \cdot Z(\frac{1}{qt})$*
3. *Die Inversen der Nullstellen von $Z(t)$ haben den absoluten Betrag $\sqrt{q}$*

Beweis: s. [Weil].

Die Zetafunktion einer Kurve kann als rationale Funktion explizit beschrieben werden:

Theorem 1.2.3. *Seien die Bezeichnungen wir oben, dann existiert genau ein Polynom $L \in \mathbb{Z}[t]$ vom Grad $2g$ mit der Zusatzeigenschaft*

$$L(t) = q^g \cdot t^{2g} \cdot L(\tfrac{1}{qt})$$

das die folgende Gleichung erfüllt:

$$Z(t) = \tfrac{L(t)}{(1-t)(1-qt)}$$

Beweis: s. [Weil].

Eine wichtige Folgerung aus den obigen Theoremen sind die nach Hasse und Weil benannte Schranken für die Anzahl der rationalen Punkte:

Korollar 1.2.4. *Seien die Bezeichnungen wie oben. Dann gilt:*

$$-2g\sqrt{q} + q - 1 \leq \#C(\mathbb{F}_q) \leq 2g\sqrt{q} + q - 1$$

Frobeniusendomorphismus:
Betrachte den q-Frobeniusautomorphismus des Körpers $\mathbb{F}_q$, bzw. des algebraischen Abschlusses $\bar{\mathbb{F}}_q$, definiert durch

$$a \mapsto a^q \text{ für ein } a \in \bar{\mathbb{F}}_q$$

Dieser Automorphismus induziert einen Endomorphismus F auf den glatten Varietäten über $\bar{\mathbb{F}}_q$. Insbesondere sind die $\mathbb{F}_q$-rationalen Punkte von C, bzw. J_C dadurch charakterisiert, dass sie genau die Fixpunkte von F sind.

Betrachte das charakteristische Polynom χ_F des Endomorphismus F auf J_C. Wegen der Separabilität von $F - \mathrm{id}$ enthält dieses Polynom die Information über die Anzahl der $\mathbb{F}_q$-rationalen Punkte von J_C :

$$\#J_C(\mathbb{F}_q) = \chi_F(1)$$

Der Zusammenhang zwischen dem Frobeniusendomorphismus und der Weilschen Zetafunktion ist durch das folgende Satz gegeben:

Satz 1.2.5. *Das charakteristische Polynom des Frobeniusendomorphismus F und das L-Polynom (aus 1.2.2) erfüllen folgende Gleichung:*

$$L(t) = t^{2g}\chi_F(t^{-1})$$

Beweis: s. [Hart].

p-adische Punktezählalgorithmen
Die p-adischen Methoden wurden bereits beim Dwarkschen Beweis [Dw] der

Rationalität der allgemeinen Zetafunktionen in 1960 verwendet. Nach dem in 1999 erschienen Algorithmus von Satoh [Sat] entstand eine Reihe von effizienten p-adischen Punktezählalgorithmen, die vor allem für eine kleine Charakteristik angewendet werden.

Diese Algorithmen berechnen das L-Polynom (bzw. dessen Nullstellen) durch die Betrachtung der induzierten Operation des Frobenius auf bestimmten (über den p-adischen Zahlen $\mathbb{Z}_q$ definierten) Räumen, die meistens eine Interpretation in Termen der p-adischen Kohomologien haben. Das Grundgerüst eines p-adischen Algorithmus besteht in der Regel aus zwei Schritten:

1. *p-adische Liftung des Frobeniusendomorphismus nach Charakteristik 0*
2. *Berechnung der induzierten Operation auf den p-adischen Kohomologieräumen*

Für eine ausführliche Übersicht über den Einsatz der p-adischen Methoden für die Bestimmung der Zetafunktion verweisen wir auf [Gerk] und [LW].

Die p-adischen Liftungen können nur selten exakt ausgerechnet werden. Dies ist aber auch nicht notwendig wegen der Hasse-Weil Schranken (1.2.4). Dadurch ist es ausreichend, das charakteristische Polynom des Frobenius modulo p^N für ein gewisses N zu kennen, um $\#J_C(\mathbb{F}_q)$ eindeutig bestimmen zu können. Aus diesen Gründen rechnet man mit einer bestimmten p-adischen Genauigkeit: $[d/2] + 1$ bei Satoh und $[d/2] + \log_p(d)$ bei Kedlaya, wobei $d := [\mathbb{F}_q : \mathbb{F}_p]$ der Körpererweiterungsgrad ist.

Relativer p-Frobeniusmorphismus
Ein weiteres Merkmal der p-adischen Methoden besteht darin, dass man anstelle des q-Frobeniusendomorphismus den relativen p-Frobeniusmorphismus liftet. Dabei verwendet man eine Zerlegung des q-Frobeniusendomorphismus in eine Kette von relativen Frobeniusmorphismen.

Sei C eine Kurve mit der definierenden Gleichung $f = \sum a_{i,j} x^i y^j$. Der p-Frobeniusendomorphismus $a \mapsto a^p$ des Körpers $\bar{\mathbb{F}}_q$ induziert einen Morphismus $\sigma : C \to C^\sigma$, definiert durch

$$X \mapsto X^p,\ Y \mapsto Y^p$$

wobei C^σ aus C durch die Operation des p-Frobeniusautomorphismus auf den Koeffizienten der definierenden Gleichung entsteht:

$$f^\sigma := \sum a_{i,j}^p x^i y^j$$

Durch die mehrmalige Anwendung von σ erhalten wir folgende Morphismenkette:

$$C = C_0 \stackrel{\sigma_0}{\to} C_1 \stackrel{\sigma_1}{\to} C_2 \cdots \stackrel{\sigma_{d-1}}{\to} C_d = C \text{ , für } C_i := C_{i-1}^{\sigma}$$

Den q-Frobeniusendomorphismus Σ erhält man dann als Produkt der relativen Morphismen σ_i.

Diese Morphismuskette induziert auch eine Zerlegung der induzierten Operation des q-Frobeniusendomorphismus. Hat man die Matrix M_p des relativen Frobeniusmorphismus berechnet, so erhält man den die Matrix M_q des absoluten Frobeniusmorphismus durch

$$M_q = \prod M_p^{\sigma^i}$$

wobei M^{σ} durch die elementenweise Anwendung von σ entsteht. Das charakteristische Polynom der Matrix M_q ist dann exakt das gesuchte charakteristische Polynom des Frobeniusendomorphismus.

1.3 Algorithmus von Kedlaya

Der in 2001 entwickelte Algorithmus von Kedlaya [Ked] berechnet die Ordnung der jakobischen Varietät einer glatten hyperelliptischen Kurve über einen endlichen Körper in Charakteristik $p > 2$. Als Darstellungsraum für die Operation des Frobenius benutzt Kedlaya die, für glatte affine Varietäten definierte, Monsky-Waschnitzer Kohomologie [MW]. In diesem Abschnitt geben wir eine kompakte Beschreibung dieses Algorithmus.

Monsky-Washnitzer Kohomologie der hyperelliptischen Kurven
Sei $C/\mathbb{F}_q$ eine hyperelliptische Kurve vom Geschlecht g mit der definierenden Gleichung $y^2 = f(x)$, wobei $f(x)$ ein Polynom vom Grad $2g + 1$ ohne mehrfache Nullstellen über $\bar{\mathbb{F}}_q$ ist. Wir betrachten die affine Kurve C' mit dem Koordinatenring

$$A := \mathbb{F}_q[x, y, y^{-1}]/(y^2 - f(x))$$

die dem Durchschnitt von C mit der offenen Umgebung $\{y \neq 0\}$ entspricht und aus der projektiven Kurve durch das Wegnehmen der Weierstrasspunkte und des unendlich fernen Punktes entsteht.

Unter einer *schwachen Komplettierung* von A versteht man den Ring

$$A^{\dagger} := \mathbb{Z}_q[x, y]^{\dagger}/(y^2 - \tilde{f}(x)),$$

wobei $\tilde{f}$ eine beliebige Liftung von f über $\mathbb{Z}_q$ und

$$\mathbb{Z}_q[x,y]^\dagger := \{\sum a_{i,j}x^iy^j \quad a_{i,j} \in \mathbb{Z}_q | \, \exists C \in \mathbb{R}^+, \text{s.d. } v_p(a_{i,j}) \geq C(i+j)\}$$

der Ring der überkonvergenten Potenzreihen ist (dabei ist v_p die normalisierte p-adische Bewertung, s. Anhang).

Die Monsky-Washnitzer Kohomologie der affinen Kurve C' ist definiert als De-Rahm Kohomologie der schwachen Komplettierung $A^\dagger$ tensoriert mit $\mathbb{Q}_q$. Also gilt:

$$\mathrm{H}^1_{MW}(C') = \mathrm{H}^1_{DR}(A^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q) = \Omega_{A^\dagger}/dA^\dagger, \text{ wobei}$$

$$\Omega_{A^\dagger} := A^\dagger dx + A^\dagger dy \;\text{ und }\; d(A^\dagger) := A^\dagger \left(\tfrac{\partial(y^2-f)}{\partial x}dx + \tfrac{\partial(y^2-f)}{\partial y}dy\right)$$

die Räume der geschlossenen, bzw. der exakten Differentialen bezeichnen. Der erste Kohomologieraum $\mathrm{H}^1_{MW}(C')$ ist ein $4g+1$-dimensionaler Vektorraum mit der Basis:

$$\left\{\tfrac{x^i dx}{y}\right\}_{0\leq i\leq 2g-1} \bigcup \left\{\tfrac{x^i dx}{y^2}\right\}_{0\leq i\leq 2g}.$$

Liftungen des Frobeniusmorphismus
Wie im vorigen Abschnitt angedeutet, besteht der erste Schritt des Algorithmus darin, eine geeignete Liftung des relativen Frobeniusmorphismus zu finden. So betrachten wir den von $C \to C^\sigma$ induzierten Homomorphismus auf Koordinatenringen:

$$F: \; A^\sigma = \mathbb{F}_q[x,y]/(y^2 - f^\sigma(x)) \to A = \mathbb{F}_q[x,y]/(y^2-f(x))$$
$$x \mapsto x^p, \; y \mapsto y^p$$

und berechnen eine Liftung $F^\dagger : (A^\dagger)^\sigma \to A^\dagger$ von F mit einer vorgegebenen p-adischen Genauigkeit. Beachte, dass diese Liftung $F^\dagger$ nicht eindeutig ist. Die induzierte Operation des Frobenius auf der MW-Kohomologie hängt allerdings nicht von der gewählten Liftung ab.

Eine Liftung $F^\dagger : (A^\dagger)^\sigma \to A^\dagger$ ist eindeutig bestimmt durch die Bilder der Basivariablen $(F^\dagger(x), F^\dagger(y))$, die die Gleichung $\tilde{f}(F^\dagger(x), F^\dagger(y)) = 0$ erfüllen müssen. Wir setzen $F^\dagger(x) := x^p$ und erhalten die Gleichung:

$$F^\dagger(y) := y^p \left(1 + \tfrac{\tilde{f}^\sigma) - \tilde{f}^p}{y^{2p}}\right)^{1/2} \in A^\dagger = y^p \sum_{i=0}^{\infty} \binom{1/2}{i} \tfrac{(F^\dagger(\tilde{f}) - \tilde{f}^p)^i}{y^{2pi}}$$

Das Bild $F^\dagger(y^{-1})$ wird im Originalalgorithmus durch die p-adischen Variante des Newtonschen Iterationsverfahrens mit der gewünschten Genauigkeit

berechnet. Für den Originalalgorithmus ist es dabei erforderlich dass y^{-1} in dem Koordinatenring liegt, dadurch wurde insbesondere die Wahl der verwendeten Kurven motiviert.

Berechnung der induzierten Operation des Frobenius:
Als nächstes betrachten wir die Berechnung der von $F^\dagger$ induzierten linearen Operation F^* auf $\mathrm{H}^1_{MW}(C')$. Dieser Kohomologieraum zerfällt unter der hyperelliptischen Involution in zwei F^*-invariante Eigenräume:

$$H^+ := \{\tfrac{x^i dx}{y^2}\} \text{ und } H^- := \{\tfrac{x^i dx}{y}\}$$

Betrachte die Bilder der Basisvektoren von H^- unter F^*:

$$F^*\left(\tfrac{x^i dx}{y}\right) = \tfrac{DF^\dagger(x^i)dx}{F^\dagger(y)}$$

Für die Berechnung der Matrix von F^* müssen diese geschlossene Differentiale modulo den exakten Differentialen reduziert werden. Durch die Ausnutzung der definierenden Gleichung fassen wir alle geschlossene Differentiale in der folgenden Form auf:

$$\sum_{i=-\infty}^{\infty} y^i \sum_{j=0}^{2g} a_{ij} x^j dx$$

Die Terme $\frac{h(x)dx}{y^i}$ reduzieren wir dabei wie folgt. Wegen der Glattheit der Kurve sind $f(x)$ und $f'(x)$ teilerfremd in $\mathbb{F}_q[x]$ und folglich existieren folgende Polynome $a(x)$ und $b(x)$

$$a(x) \cdot f(x) + b(x) \cdot f'(x) = h(x) \text{ in } \mathbb{F}_q[x]$$

Durch die Betrachtung des exakten Differentials $d\left(\frac{b(x)}{y^{m-2}}\right)$ und der Relation $2y\,dy \equiv f'(x)\,dx$ erhalten wir die Gleichung:

$$\tfrac{h(x)dx}{y^m} \equiv \left(a(x) + \tfrac{2b'(x)}{m-2}\right)\tfrac{dx}{y^{m-2}}$$

die zur Reduktion der y-Potenzen im Nenner verwendet wird. Die dabei auftauchende (durch p teilbare) Nenner führen dazu, dass man für das Punktezählen eine größere p-adische Genauigkeit benötigt, als die die man aus Hasse-Weil Schranken herleiten würde. Kedlaya gibt eine obere Schranke $d \log_p d$ für diese Genauigkeit ($p^d = q$).

Komplexität und Erweiterungen des Algorithmus
In der Originalarbeit wurde für ein festgewähltes p die Zeitkomplexität von $O(g^{3+\epsilon}n^{3+\epsilon})$ für den Liftungsschritt und $O(g^{4+\epsilon}n^{3+\epsilon})$ für den Reduktionsschritt theoretisch bewiesen, wobei die FFT-Multiplikation im $\mathbb{F}_q$ vorausge-

setzt wurde.

Es gibt eine Reihe von Erweiterungen des Algorithmus auf andere Kurven (z.B. C_{ab}-Kurven oder Artin-Schreier Kurven in Charakteristik 2 in [Verk] und allgemeinere Varietäten [Gerk]), bei denen die Liftungen des Frobenius durch p-adische Variationen des Newtonschen Iterationsverfahrens berechnet werden.

Einige Zeit war der Kedlaya-Algorithmus nur über den Körpern in kleiner Charakteristik praktizierbar. In der neulich erschienen Arbeit von Harvey [Harv] wurde jedoch eine neue "vertikale" Reduktionsmethode vorgeschlagen, die Zeitkomplexität in p auf $\sqrt{p}$ reduziert (wobei n-Komplexität auf $n^{4+\epsilon}$ erhöht wird), so dass die gesamte Methode auch auf mittlere Charakteristik anwendbar wird.

Kapitel 2

Liftung der Morphismen als Deformationsproblem

Als Ausgangspunkt dieser Arbeit dient die Wahl der Liftung des Frobeniusmorphismus im Kedlaya Algorithmus. Für die Optimierung dieser Wahl im Hinblick auf die weiteren Schritte des Algorithmus möchten wir alle Liftungen des Frobeniusmorphismus über den p-adischen Quotientenringen möglichst explizit parametrisieren. Wir bedienen uns dabei der Methoden der modernen Deformationstheorie, indem wir diese Liftungen als infinitesimale Deformationen über den lokal artinschen n-ten Wittvektorringen auffassen.

Das Kapitel beginnt mit einem Überblick über ausgewählte Konzepte und Ideen aus der Deformationstheorie, die uns als Motivation dienen. Anschließend geben wir eine induktive Beschreibung der Liftungen der Homomorphismen auf endlich erzeugten Algebren, die die Grundlage für die folgenden Kapiteln schafft.

2.1 Einführung in die Deformationstheorie

In der algebraischen Geometrie kann man unterschiedliche Objekte durch das Variieren der Koeffizienten deren definierenden Gleichungen „deformieren“. Das Studium der dadurch entstehenden Familien nennt man Deformationstheorie. Die exakte Definition einer Deformation hängt stark von den betrachtenden Objekten ab. In diesem Abschnitt geben wir abstrakte Definitionen der Deformation, wobei wir für eine vollständigere Einführung auf [Schl] und [Sern] verweisen.

Deformation der Varietäten
Wir beginnen mit der Definition einer Deformation von Varietäten. Sei X_0 eine Varietät über den Körper k, R ein k-Ring mit der Eigenschaft, dass $S := \mathrm{Spec}(R)$ zusammenhängend ist. Unter einer *Deformation* von X_0 über R (bzw. über S) versteht man ein solches flaches Schema $(\pi : X \to S)$, deren Faserprodukt mit $\mathrm{Spec}(k)$ über S genau die Varietät X_0 ergibt:

$$\begin{array}{ccc} X \times_S \operatorname{Spec} k \cong X_0 & \longrightarrow & X \\ \downarrow & & \downarrow \\ \operatorname{Spec} k & \longrightarrow & S \end{array}$$

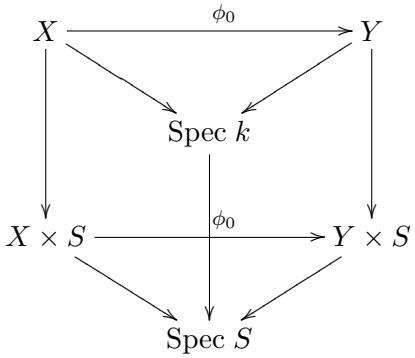
Wenn wir $\operatorname{Spec} k$ als ein Punkt in S auffassen, dann ist X_0 die Faser von $\pi : X \to S$ über $\operatorname{Spec} k$. Für jeden Punkt $s \in S$ ist $(\pi : X \to S)$ eine Deformation des Fasers $(X_s \to k(s))$.

Diese Deformationen betrachten wir modulo folgender Äquivalenzrelation: Zwei Deformationen $\pi : X \to S$ und $\pi' : X' \to S$ von X_0 sind äquivalent, falls es einen Isomorphismus $\phi : X \to X'$ mit $\pi'\phi = \pi$ gibt, der die Identität auf jeder Faser induziert.

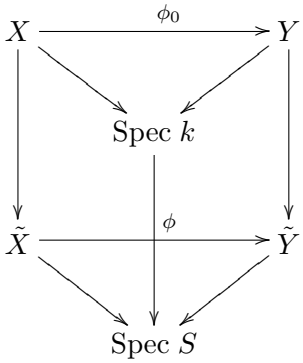
Alle Elemente der durch Deformationen entstehenden Familien sollen dieselben Eigenschaften wie die ursprüngliche Varietät besitzen. Also definiert man Deformation einer glatten (n-dimensionalen, abelschen) Varietät über k als ein glattes (n-dimensionales, abelsches) R-Schema.

Die oben definierten Deformationen der Varietäten kann man auf eine natürliche Weise auf Schemata verallgemeinern. Sei $R \to R_0$ ein surjektiver Ringhomomorphismus und X_0 ein Schema über $S_0 := \mathrm{Spec}(R_0)$. Wir nennen $X \to S := \mathrm{Spec}(R)$ eine *Deformation* von X_0 über R (bzw. über S), falls X_0 isomorph zum Faserprodukt $X \times_S S_0$ ist.

Deformation der Morphismen
Die gegebenen Definitionen kann man auch auf die Morphismen erweitern. Dabei muss man unterscheiden, ob man nur den Morphismus, oder auch die entsprechenden Varietäten deformiert. Unter einer *Deformation des Morphismus $\phi_0 : X \to Y$ über S mit fixierten X und Y* versteht man einen Morphismus $\phi : X \times S \to Y \times S$, der das folgende Diagramm komplettiert:



Unter *einer Deformation des Morphismus ϕ zusammen mit der Varietäten X und Y über S* versteht man Deformationen $\tilde{X}$ von X und $\tilde{Y}$ von Y über S zusammen mit dem Morphismus $\phi : \tilde{X} \to \tilde{Y}$ der das folgende kommutative Diagramm vervollständigt:



Infinitesimale Deformationen, Deformationen 1-er Ordnung:
Da die Untersuchung der (globalen) Deformationen im Allgemeinen sehr schwierig ist, beschränkt man sich oft auf den Fall, in dem der Basisraum S_0 ein lokaler artinscher k-Ring ist. Solche Deformationen, die wir im Folgenden *infinitesimale Deformationen* nennen, enthalten bereits die meiste Information über die Deformationen von X_0.

Eine Schlüsselrolle in der Deformationstheorie nehmen die Deformationen 1-er Ordnung ein, die durch die kleinstmögliche Erweiterung der Basisräume charakterisiert sind. Unter einer *Deformation 1-er Ordnung* von einer k-Varietät X verstehen wir eine infinitesimale Deformation, gegeben durch

ein Schema über den Ring $k[\epsilon]/\epsilon^2$. Analog definieren wir Deformationen 1-er Ordnung anderer Objekte, wie zum Beispiel der Morphismen. zwischen den Varietäten.

Bei den meisten Deformationsproblemen ist die Klasse der Deformationen 1-er Ordnung ein k-Vektorraum, der mit einer Kohomologie einer kohärenten Garbe auf dem deformierenden Objekt identifizierbar und dadurch berechenbar ist. Wir listen eine Reihe von Ergebnissen auf, die uns als Motivation für den nächsten Kapiteln dienten:

Lemma 2.1.1. *Alle Deformationen 1-er Ordnung einer glatten affinen Varietät sind isomorph.*

Beweis: s. [Sern]

Satz 2.1.2. *Die Klasse der Deformationen 1-er Ordnung einer glatten projektiven Varietat X ist gegeben durch den Kohomologieraum $\mathrm{H}^1(X, \Theta_X)$, wobei Θ_X die Tangentialgarbe von X ist.*

Beweis: s. [Sern]

Auch die Räume der Deformationen 1-er Ordnung der Morphismen von glatten Varietäten sind gegeben durch die Kohomologieräume einer Tangentialgarbe, bzw. deren Quotienten:

Satz 2.1.3. *Sei $\phi : X \to Y$ ein Morphismus von glatten Varietäten. Dann ist die Klasse der Deformationen 1-er Ordnung von ϕ mit fixierten X und Y gegeben durch $\mathrm{H}^0(X, \phi^* T_Y)$, wobei T_Y die Tangentialgarbe von Y bezeichnet.*

Beweis: s. [Harr]

Insbesondere ist die Klasse der Deformationen 1-er Ordnung der Identität $\mathrm{id} : X \to X$ genau der Raum der globalen Vektorfelder $\mathrm{H}^0(X, T_X)$.

Satz 2.1.4. *Sei $\phi : X \to Y$ ein Morphismus von glatten Varietäten. Dann ist die Klasse der Deformationen 1-er Ordnung von (ϕ, X) mit fixiertem Y gegeben durch $\mathrm{H}^0(X, \mathcal{N}_\phi)$. Dabei bezeichnet $\mathcal{N}_\phi$ die Normalgarbe von ϕ, definiert durch*

$$\mathcal{N}_\phi := Coker(d\phi : T_X \to \phi^* T_Y)$$

Beweis: s. [Harr]

Den Zusammenhang zwischen den oben angegebenen Darstellungen der Deformation 1-er Ordnung der Varietäten und deren Morphismen hat eine einfache kohomologische Erklärung. Die Randabbildung

$$\delta : \mathrm{H}^0(X, \phi^* T_Y) \to \mathrm{H}^1(X, \mathcal{N}_\phi)$$

der langen exakten Kohomologiesequenz zu der exakten Sequenz:

$$0 \to T_X \to \phi^*(T_Y) \to N_\phi \to 0$$

bildet die Deformationen 1-er Ordnung von (ϕ, X) auf die Deformationen von X durch das „Vergessen“ von ϕ. Der Kern dieser Abbildung besteht genau aus den Deformationen 1-er Ordnung von ϕ (mit fixierten X und Y) modulo Automorphismen von X.

Obstruktionen zu Deformationen
Es ist nicht immer möglich ein über $S = Spec\, R$ definiertes Objekt X über ein affines Schema $S' = \mathrm{Spec}\, R'$ zu deformieren. Bei der Untersuchung der Existenz der Deformationen betrachtet man *Obstruktionen* zu Deformierbarkeit von X über S', die genau dann verschwinden wenn es eine Deformation von X über S' existiert.

Oft liegen diese Obstruktionen in einem Kohomologieraum, den wir einen *Obstruktionsraum von X* nennen.

Satz 2.1.5. *Sei V eine glatte Varietät über k, (V, Θ_V) die Tangentialgarbe von V, dann ist $\mathrm{H}^2(V, \Theta_V)$ ein Obstruktionsraum von V.*

Beweis: s. [Sern]

Das Verschwinden eines Obstruktionraumes impliziert die Existenz der infitesimalen Deformationen von $X \to \mathrm{Spec}R$ über solche lokal artinsche Ringe R', für die ein surjektiver Homomorphismus $R' \to R$ existiert. Eine unmittelbare Folgerung aus dem obigen Satz ist also die Existenz der infinitesimalen Deformationen über beliebige lokal artinsche k-Ringe für glatte affine Varietäten oder für glatte Kurven.

Die Untersuchung des Verschwindens der Obstruktionsräume kann auf die Betrachtung der *kleinen Erweiterungen von k-Ringen* zurückführen, die wir als einen surjektiven Ringhomomorphismus $q : A' \to A$ mit einem zum Körper k isomorphen Kern definieren. Ein Obstruktionsraum von X verschwindet genau dann, wenn für jede kleine Erweiterung $q : A' \to A$ eine Deformation $X' \to \mathrm{Spec}A'$ von X existiert.

2.2 p-adische Liftungen nach Charakteristik 0

In diesem Abschnitt präzisieren wir den Begriff der Liftungen in der Sprache der Deformationstheorie, zeigen dass man durch die Betrachtung der kleinen Liftungen eine Parametrisierung aller Liftungen erhält und erklären die, in den folgenden Kapiteln, angewendete Berechnungsstrategie.

Liftungen als Deformationen:
Sei $V \to Spec\, k$ eine glatte Varietät in positiver Charakteristik $p > 0$. Man sagt, V kann nach Charakteristik 0 geliftet werden, falls es einen Integritätsbereich R in Charakteristik 0, einen surjektiven Ringhomomorphismus $R \to k$ und ein glattes Schema $\tilde{V} \to Spec\, R$ gibt, so daß $\tilde{V} \otimes_R k = V$ gilt. Dies entspricht der üblichen Definition einer Liftung, da das Tensorieren mit k über R der Reduktion modulo p entspricht.

Das Schema $\tilde{V}$ in der obigen Definition kann man als eine Deformation von V über R auffassen. Unter einer Liftung von V „im schwachen Sinne“ nach Charakteristik 0 versteht man eine Deformation von V über einen Integritätsbereich R. Im Folgenden beschränken wir uns auf die Deformationen über den Ring der Wittvektoren $W(k)$ von k, die wir *Liftungen von* V nennen (man nennt sie manchmal Liftungen „im starken Sinne“).

Diese Definition der Liftungen nach Charakteristik 0 kann man auf verschiedene Objekte verallgemeinern. Eine ausführliche Übersicht darüber findet man in [Oort 2].

Für die praktischen Berechnungen können wir Liftungen über $W(k)$ nur mit einer beschränkten p-adischen Genauigkeit betrachten. Deswegen konzentrieren wir uns im Folgenden hauptsächlich auf die Liftungen über den Quotientenringen $W_n(k) := W(k)/p^n W(k)$. Die *n-te Wittvektorenringe* $W_n(k)$ sind lokal artinsch, also kann man die Liftungen über $W_n(k)$ als infinitesimale Deformationen auffassen.

Die n-ten Wittvektorenringe, sowie die Liftungen über diese Ringe bilden ein projektives System, wobei die Projektion durch die Reduktion modulo p^i gegeben ist. Die Liftungen über $W(k)$ kann man dann als inverses Limes einer Folge von infinitesimalen Deformationen auffassen.

Raum der kleinen Liftungen:
Wir versuchen die Berechnung dieser Liftungen in kleine aufeinanderfolgen-

de Schritte zu zerlegen. Im Zentrum unserer Betrachtung stehen dabei vor allem die Deformationen eines $W_n(k)$-Objekten X_n über $W_{n+1}(k)$. Solche zu den Deformationen 1-er Ordnung verwandten Liftungen nennen wir im Folgenden *kleine Liftungen* von X_n.

Wegen der Ähnlichkeit der Ringe $k[\epsilon]/\epsilon^2$ und $W(k)/(p^2)$ haben die Räume der Deformationen 1-er Ordnung und die Räume der kleinen Liftungen eine ähnliche Struktur, wie wir am Beispiel der Homomorphismen von endlich erzeugten Algebren im nächsten Abschnitt zeigen werden (der Unterschied zwischen diesen Räumen besteht insbesondere darin, dass $W(k)/(p^2)$ keine k-Algebra Struktur besitzt).

Bei den aufeinander aufbauenden Liftungen eines Objektes sind alle kleinen Schritte ähnlich und für eine Folge der Liftungen von X/k:

$$X = X_0 \hookrightarrow X_1 \hookrightarrow \ldots \hookrightarrow X_n \hookrightarrow \ldots$$

sind alle Räume der kleinen Liftungen von X_i isomorph. Die Beschreibung des Raumes der kleinen Liftungen liefert also eine induktive Beschreibung aller Liftungen über den Ringen $W_{n+1}(k)$.

Auch die Obstruktionen zu den kleinen Liftungen von X_n über $W_{n+1}(k)$ liegen in demselben Raum für jedes n. Deswegen ist die Existenz einer Liftung über $W(k)/p^2$ oft entscheidend für (formale) p-adische Liftbarkeit nach Charakteristik 0.

Einen Beispiel für eine deformationstheoretische Parametrisierung der Liftungen wird zum Beispiel in [Srin] gegeben:

Theorem 2.2.1. *Sei X eine projektive Varietät über k und (X_n, F_n) eine Liftung der Varietät X zusammen mit dem Frobeniusendomorphismus über $W_n(k)$, dann ist ein Obstruktionsraum zu der kleinen Liftungen von (X_n, F_n) gegeben durch $\mathrm{H}^1(V, \mathcal{N}_{\mathcal{F}})$. Wenn dieser Obstruktionsraum verschwindet, dann ist der Raum der kleinen Liftungen von (X_n, F_n) isomorph zu dem Kohomologieraum $\mathrm{H}^0(V, \mathcal{N}_{\mathcal{F}})$.*

Beweis: s. [Srin]

Berechnung der Liftungen:
Die Parametrisierung der kleinen Liftungen die man mit deformationstheoretischen Methoden erhält, ist oft nicht unmittelbar geeignet für die praktische Berechnung der Liftungen. Deswegen verwenden wir an mehreren Stellen die-

ser Arbeit folgende (indirekte) Vorgehenweise:

Sei X_n ein Objekt über $W_n(k)$, bei dem die Berechnung der kleinen Liftungen über $W_{n+1}(k)$ kompliziert ist. Wir schwächen die Bedingungen an X_n ab und erhalten ein Objekt $\hat{X}_n$, das einige Eigenschaften von X_n nicht hat und deren Liftungen man dadurch leichter berechnen kann. Anschließend betrachten wir die parametrisierte Familie der kleinen Liftungen $\hat{X}_{n+1}(\alpha)$ von $\hat{X}$ und untersuchen die Fortsetzbarkeit dieser Liftungen zu einer Liftung X_{n+1} von X in Abhängigkeit von dem Parameter α.

Diese Methode wenden wir zum Beispiel im Kapitel 3 bei der Berechnung der Liftungen der Homomorphismen zwischen Koordinatenringen von affinen Varietäten an, indem wir Verträglichkeit mit den definierenden Gleichungen zunächst „vergessen“ und die Liftungen der Homomorphismen von Polynomringen entlang des Parameterraums so deformieren, dass man diese Verträglichkeit wieder erhält. Hier und im Folgenden verwenden wir den Begriff „deformieren“ im klassischen Sinne der Parametervariation.

Eine weitere Anwendung tritt bei der Liftung eines projektiven Morphismus im Kapitel 5 auf. Wir liften zunächst die Einschränklungen auf affinen Karten und versuchen dann diese affine Liftungen so entlang der Parameterräume zu deformieren, dass sie sich auf den Durchschnitten verkleben.

2.3 Kleine Liftungen der Algebrahomomorphismen

Nach dem Satz 2.1.3 entspricht der Raum der Deformationen erster Ordnung von einem Morphismus $F : X \to Y$ (mit fixierten X und Y) dem Kohomologieraum $\mathrm{H}^0(X, \Phi^*(T_Y))$. In dem affinen Fall ist dieser Raum isomorph zu dem Modul der F-Derivationen zwischen Koordinatenringen, denn die globalen Schnitte dieses Kohomologieraums sind genau die Derivationen der Koordinatenringen von entsprechenden affinen Umgebungen.

Ein ähnliches Ergebnis zeigen wir in diesem Abschnitt für die kleine p-adische Liftung der Morphismen von affinen Varietäten, wobei wir die Liftungen des induzierten Homomorphismen zwischen den Koordinatenringen betrachten.

Sei $F : A \to B$ ein Homomorphismus von kommutativen endlich erzeugten $W_n(k)$-Ringen. Unter einer kleinen Liftung des Homomorphismus F verstehen wir einen $W_{n+1}(k)$-Ringhomomorphismus $\tilde{F} : \tilde{A} \to \tilde{B}$, deren Reduktion

modulo p^{n-1} mit F übereinstimmt. In diesem Abschnitt beschreiben wir den Raum der kleinen Liftungen von F für die gegebenen Liftungen $\tilde{A}$ und $\tilde{B}$.

Als erstes zeigen wir, dass zwei beliebige kleine Liftungen von F sich immer um eine Derivation zwischen den k-Ringen $\bar{A}$ un $\bar{B}$ unterscheiden, wobei $\bar{A}$ und $\bar{B}$ die Reduktionen von A und B modulo p sind. Für die Definition und Beschreibung der Eigenschaften der Derivationen verweisen wir auf die Standardwerke über die kommutative Algebra (z.B. [Mat1], [Mat2] oder [ZS]).

Lemma 2.3.1. *Seien $\tilde{F}$, $\hat{F} : \tilde{A} \to \tilde{B}$ zwei beliebige kleine Liftungen von F, dann existiert eine k-Derivation $\psi \in Der_{\bar{F}}(\bar{A} \to \bar{B})$, die folgende Gleichung für jedes $g \in \tilde{A}$ und deren Reduktion $\bar{g} \in \bar{A}$ erfüllt:*

$$\tilde{F}(g) - \hat{F}(g) = p^n * \psi(\bar{g})$$

(wobei der Operator $*$ im Anhang definiert ist).

Beweis:
Sowohl $\tilde{F}$ als auch $\hat{F}$ sind Liftungen von F. Folglich gilt :

$$\tilde{F} \equiv F \equiv \hat{F} \mod p^{n-1}$$

Betrachte die Abbildung $\tilde{F} - \hat{F} : \tilde{A} \to \tilde{B}$. Diese Abbildung verschwindet modulo p^{n-1} wegen der obigen Äquivalenz und definiert nach (A.3) eine eindeutige Abbildung $\psi : \bar{A} \to \bar{B}$ mit der Eigenschaft

$$p^n * \psi := \tilde{F} - \hat{F}.$$

Um zu zeigen, daß ψ eine Derivation ist, müssen wir die Derivationseigenschaften nachprüfen:

$D1$) Die Konstanten verschwinden unter ψ wegen $\tilde{F}(1_A) = 1_B = \hat{F}(1_A)$

Im Folgenden seien $\bar{g}, \bar{h} \in \bar{A}$ die Reduktion von $g, h \in \tilde{A}$ modulo p

$D2$) Die Abbildung ψ ist additiv wegen:

$$\begin{aligned} p^n * \psi(\bar{g} + \bar{h}) &= \tilde{F}(g + h) - \hat{F}(g + h) \\ &= \tilde{F}(g) + \tilde{F}(h) - \hat{F}(g) - \hat{F}(h) \\ &= (\tilde{F}(g) - \hat{F}(g)) + (\tilde{F}(h) - \hat{F}(h)) \\ &= p^n * \psi(\bar{g}) + p^n * \psi(\bar{h}) \end{aligned}$$

Und folglich gilt:

$$\psi(\bar{g} + \bar{h}) = \psi(\bar{g}) + \psi(\bar{h})$$

$D3)$ die Abbildung ψ erfüllt die Multiplikationsregel wegen:

$$\begin{aligned} p^n * \psi(\overline{gh}) &= (\tilde{F} - \hat{F})(gh) = \tilde{F}(g)\tilde{F}(h) - \hat{F}(g)\hat{F}(h) \\ &= \tilde{F}(g)\tilde{F}(h) - \tilde{F}(g)\hat{F}(h) + \tilde{F}(g)\hat{F}(h) - \hat{F}(g)\hat{F}(h) \\ &= \tilde{F}(g)(\tilde{F}(h) - \hat{F}(h)) + \hat{F}(h)(\tilde{F}(g) - \hat{F}(h)) \\ &= \tilde{F}(g) \cdot p^n * \psi(\bar{h}) + \hat{F}(h) \cdot p^n * \psi(\bar{g}) \end{aligned}$$

Also erhalten wir die Äquivalenz

$$\psi(gh) \equiv \tilde{F}(g) \cdot \psi(\bar{h}) + \hat{F}(h) \cdot \psi(\bar{g})) \bmod p^n$$

und wegen der Äquivalenz $\tilde{F}(t) \equiv \overline{F(t)} \equiv \hat{F}(t) \bmod p$ für jedes $t \in \tilde{A}$ gilt die gewünschte Gleichung in B:

$$\psi(\overline{gh}) = \overline{F(g)}\psi(\bar{h}) + \overline{F(h)}\psi(\bar{g})$$

□.

Sei $\hat{F}$ eine festgewählte kleine Liftung von F. Wir definieren eine Abbildung aus dem Raum der kleinen Liftungen von F in den Derivationsmodul $Der_{\bar{F}}(A, B)$ durch die Zuordnung:

$$\rho_{\hat{F}} : \hat{F} \to \psi := \tfrac{\tilde{F} - \hat{F}}{p^n}$$

Nach dem Lemma (2.3.1) ist diese Abbildung wohldefiniert. Mit dieser Abbildung erhalten wir eine vollständige Beschreibung des Raumes der kleinen Liftungen von F durch die Derivationen wegen:

Satz 2.3.2. *Sei $\hat{F}$ eine kleine Liftung von F, dann ist die oben definierte Abbildung $\rho_{\hat{F}}$ bijektiv.*

Beweis:
Die Injektivität der Abbildung $\rho_{\hat{F}}$ folgt aus ihrer Definition, denn eine weitere Derivation τ würde mit ψ übereinstimmen wegen:

$$\psi(\bar{g}) = \tfrac{\tilde{F}(g) - \hat{F}(g)}{p^n} = \tau(\bar{g}) \ \forall g \in \tilde{A}$$

Die Surjektivität folgt aus dem folgenden Lemma 2.3.3. □.

Lemma 2.3.3. *Sei ψ eine Derivation aus dem Modul $Der_{\bar{F}}(A \to B)$, dann ist $\tilde{F} := \hat{F} + p^n * \psi$ eine kleine Liftung von F*

Beweis:
Die Abbildung $\tilde{F}$ ist additiv, weil $\hat{F}$ und ψ additiv sind. Die Multiplikativität von $\tilde{F}$ kann wie folgt bewiesen werden:

Seien $\bar{g}, \bar{h} \in \bar{A}$ die Reduktion von $g, h \in \tilde{A}$ modulo p, dann gilt :

$$\begin{aligned}\tilde{F}(g) \cdot \tilde{F}(h) &= (\hat{F}(g) + p^n * \psi(\bar{g})) \cdot (\hat{F}(h) + p^n * \psi(\bar{h})) \\ &= \hat{F}(g) \cdot \hat{F}(h) + \hat{F}(g) \cdot p^n * \psi(\bar{h}) + \hat{F}(h) \cdot p^n * \psi(\bar{g}) \\ &= \hat{F}(g) \cdot \hat{F}(h) + p^n * (\psi(h) \cdot \overline{F(g)} + \psi(g) \cdot \overline{F(h)}) \\ &= \hat{F}(g \cdot h) + p^n * (\psi(\overline{g \cdot h})) = \tilde{F}(g \cdot h)\end{aligned}$$

Wegen der offensichtlichen Gleichheit $\tilde{F}(1_A) = \hat{F}(1_A) = 1_B$, haben wir damit bewiesen, daß $\tilde{F}$ ein Homomorphismus ist. Da die Reduktion von $\tilde{F}$ modulo p^{n-1} gleich F ist, ist $\tilde{F}$ eine Liftung von F. $\square$.

Korollar 2.3.4. *Es gibt eine 1-zu-1 Korrespondenz zwischen den kleinen Liftungen von F und den Derivationen aus $Der_{\bar{F}}(A \to B)$.*

Definition 2.3.5. *Wir sagen, eine Derivation ψ induziert eine kleine Liftung $\tilde{F}$, falls es $\rho_{\hat{F}}(\tilde{F}) = \psi$ gilt.*

Die Ergebnisse dieses Abschnittes ermöglichen die Berechnung aller kleinen Liftungen eines Homomorphismus F (für die fixierten Liftungen der Bild- und Urbildalgebren) ausgehend von einer „Basis“-Liftung $\hat{F}$. Im nächsten Kapitel zeigen wir, wie man eine „Basis“-Liftung berechnen kann.

Kapitel 3

Liftungen der Morphismen zwischen affinen Varietäten

In diesem Kapitel geben wir eine explizite Beschreibung der Liftungen der Morphismen zwischen affinen Varietäten über den p-adischen Quotientenringen $R_n := W(k)/p^{n+1}W(k)$, bzw. der Liftungen der induzierten Homomorphismen zwischen den Koordinatenringen. Dabei ist k ein perfekter Körper in Charakteristik $p > 0$.

Aus Übersichtlichkeitsgründen beginnen wir zunächst mit den Morphismen zwischen Hyperflächen in $\mathbb{A}^2_k$ (die nur eine definierende Gleichung in 2 Variablen haben), während die Erweiterung auf allgemeine affine Varietäten im Abschnitt 3.4 beschrieben wird. Wie bereits angedeutet, konzentrieren wir uns dabei auf die kleinen Liftungsschritte, in denen eine bekannte R_{n-1}-Liftung eines Morphismus über den Ring R_n geliftet wird (diese p-adischen Quotientenringe R_i und deren Eigenschaften sind im Anhang beschrieben).

Eine theoretische Charakterisierung der kleinen Liftungen der Morphismen zwischen affinen Varietäten für die gegebenen Liftungen der Varietäten haben wir in 2.5 gezeigt. Diese Beschreibung basiert allerdings auf einer bereits berechneten kleinen Liftung und ist dadurch für die Entwicklung eines Liftungsalgorithmus nicht unmittelbar geeignet. In diesem Kapitel geben wir eine explizite Parametrisierung der Liftungen durch die Lösungen einer linearen Gleichung über einem Koordinatenring, die eine praktische Berechnung der Liftungen ermöglicht.

In diesem Kapitel sei

$$F:\ B = k[x,y]/(g) \to A = k[x,y]/(f)$$

ein Homomorphismus zwischen Koordinatenringen von affinen Kurven und

$$F_{n-1}:\ B_{n-1} = R_{n-1}[x,y]/(g_{n-1}) \to A_{n-1} = R_{n-1}[x,y]/(f_{n-1})$$

eine Liftung von F über den Ring R_{n-1}. Im Folgenden verstehen wir unter einer *Liftung* Üblicherweise eine Liftung des Morphismus F über einen p-adischen Quotientenring R_i, sofern nicht anders spezifiziert.

Wir untersuchen, beschreiben und berechnen die kleinen Liftungen

$$F_n : B_n \to A_n$$

zunächst für die fixierten Liftungen der Koordinatenringe

$$B_n := R_n[x,y]/(g_n) \text{ und } A_n := R_n[x,y]/(f_n)$$

und zeigen anschließend wie der Raum der kleinen Liftungen von F_{n-1} von der Wahl der Liftungen der definierenden Gleichungen f_n und g_n abhängt.

Als wichtigstes Beispiel dient uns dabei die Liftung des relativen Frobeniusmorphismus (s. 1.2), bzw. des induzierten Homomorphismus auf Koordinatenringen:

$$F : A^\sigma = \mathbb{F}_q[x,y]/(f^\sigma) \to A = \mathbb{F}_q[x,y]/(f)$$

definiert durch $F(x) := x^p$ und $F(y) := y^p$. Eine Liftung dieses Homomorphismus nennen wir im Folgenden einfach als *Liftung des Frobenius* und bezeichnen es gelegentlich als (A_n, F_n), falls die Liftung der definierenden Gleichung nicht festgelegt ist.

3.1 Quasi-Liftungen und Hindernisse

Die Schwierigkeit der Liftung eines Homomorphismus zwischen Koordinatenringen besteht darin, die Verträglichkeit mit den definierenden Gleichungen zu behalten. Deswegen liften wir F_{n-1} erst als einen Homomorphismus zwischen Polynomringen und nicht zwischen deren Quotienten (modulo den definierenden Gleichungen). In diesem Fall ist die Beschreibung der Liftungen trivial.

Wir untersuchen die Einschränkbarkeit eines solchen Homomorphismus auf Polynomringen zu einem Homomorphismus auf den Quotientenringen und

beschreiben das entstehende Hindernis. Diese Hindernisse sollen nicht mit den in 2.3 definierten Obstruktionen zur (generellen) Liftbarkeit von F_{n-1} über R_n verwechselt werden.

Wir untersuchen, wie man die Liftungen auf Polynomringen „deformieren" sollte, damit die Hindernisse verschwinden und man einen Homomorphismus auf den Koordinatenringen erhält. Als Ergebnis erhalten wir eine Parametrisierung der kleinen Liftungen von F_{n-1} durch Derivationen wie in 2.3, die allerdings als Basis eine leicht zu berechende Liftung auf Polynomringen hat und dadurch für eine algorithmische Anwendung geeignet ist.

Quasi-Liftungen:
Sei $\hat{F}_{n-1} : R_{n-1}[x,y] \to A_{n-1}$ ein von F_{n-1} induzierter Homomorphismus, definiert durch dieselben Bilder der Basisvariablen x und y:

$$\hat{F}_{n-1}(x) := F_{n-1}(x) \text{ und } \hat{F}_{n-1}(y) := F_{n-1}(y).$$

Definition 3.1.1. *Eine kleine Liftung $\hat{F}_n : R_n[x,y] \to A_n$ von $\hat{F}_{n-1}$ nennen wir im Folgenden eine* ***quasi-Liftung von*** F_{n-1}.

Die kleinen quasi-Liftungen sind Trivialerweise berechenbar, denn jede Liftung $(U, V \in A_n)$ des Paares $(\hat{F}_{n-1}(x), \hat{F}_{n-1}(y) \in A_{n-1})$ induziert einen Homomorphismus

$$\hat{F}_n : R_n[x,y] \to A_n \text{ durch } \hat{F}_n(x) := U \text{ und } \hat{F}_n(x) := V$$

Wir geben nun eine Parametrisierung der quasi-Liftungen durch Derivationen, die eine ausgewählte quasi-Liftung als Basis verwendet:

Lemma 3.1.2. *Sei $\hat{F}_n : R_n[x,y] \to A_n$ eine quasi-Liftung von F_{n-1}. Dann ist jede weitere quasi-Liftung $\tilde{F}_n : R_n[x,y] \to A_n$ induziert durch eine eindeutige Derivation ψ aus $\mathcal{D} := Der_F(k[x,y], A)$ via*

$$\tilde{F}_n := \hat{F}_n + p^n * \psi.$$

Beweis: die Aussage des Lemmas folgt unmittelbar aus 2.3.2 angewendet auf die quasi-Liftungen $\hat{F}_n$ und $\tilde{F}_n$. □.

Hindernisse zur Einschränkung der quasi-Liftungen:
Eine quasi-Liftung $\hat{F}_n$ von F_{n-1} ist im Allgemeinen nicht mit der definierenden Gleichung g_n des Koordinatenringes B_n verträglich. Diese Verträglichkeit (definiert durch die Bedingung $\hat{F}_n(g_n) = 0$ in A) ist genau dann erfüllt, wenn $\hat{F}_n$ ein Homomorphismus zwischen den Koordinatenringen ist. In diesem Kapitel bezeichnen wir solche, mit g_n verträgliche Liftungen, als

echte Liftungen um den Unterschied zu den quasi-Liftungen herauszuheben.

Die Verträglichkeitsbedingung legt es nahe, den Term $\hat{F_n}(g_n) \in A_n$ als Hindernis zu der Einschränkung von $\hat{F_n}$ zu einem Homomorphismus auf Koordinatenringen zu betrachten. Dieser Term liegt in $p^n A_n \subset A_n$ und ist eindeutig bestimmt durch ein Polynom aus $k[x,y]/(f) = A$

Lemma 3.1.3. *Seien die Bezeichnungen wie oben. Dann existiert ein eindeutiges $\kappa \in A$, das die Gleichung*

$$p^n * \kappa = \hat{F_n}(g_n) \quad \textit{erfüllt.}$$

Dieses κ verschwindet genau dann, wenn $\hat{F_n}$ eine echte Liftung ist.

Beweis:
Die Reduktion von $\hat{F_n}(g)$ modulo p^{n-1} verschwindet, weil es eine Liftung von $F_{n-1}(g_{n-1}) = 0 \in A_{n-1}$ über R_n ist. Also folgt die erste Behauptung des Lemmas aus (A.3). Die zweite Behauptung des Lemmas gilt wegen der Verträglichkeitsbedingung. □.

Definition 3.1.4. *Wir nennen $\kappa := \kappa(\hat{F_n}) = \frac{\hat{F_n}(g_n)}{p^n} \in A$* ***das Hindernis zu Einschränkung von $\hat{F_n}$ zu einer echten Liftung****, oder kurz das Hindernis zu $\hat{F_n}$.*

Wegen dem Lemma 3.1.3 ist das Hindernis zu einer quasi-Liftung wohldefiniert.

Parametrisierung der einschränkbaren quasi-Liftungen:
Als nächstes wenden wir die Verträglichkeitsbedingung auf den Parameterraum der quasi-Liftungen an. Das folgende Lemma liefert die notwendige und hinreichende Bedingung an den Parameter $\psi \in \hat{\mathfrak{D}}$, damit die induzierte quasi-Liftung $\tilde{F_n} = \hat{F_n} + p^n * \psi$ zu einer echten Liftung von F_{n-1} wird:

Lemma 3.1.5. *Seien die Bezeichnungen wie vorher. Dann ist die durch $\psi \in \hat{\mathfrak{D}}$ induzierte quasi-Liftung $\tilde{F_n}$ genau dann eine echte Liftung, wenn ψ die folgende Gleichung erfüllt:*

$$\kappa(\hat{F_n}) + \psi(g) = 0$$

Beweis:
Die Aussage des Lemmas folgt direkt aus den Definitionen der Derivation ψ und des Hindernisses $\kappa(\hat{F_n})$:

$$0 = \tilde{F_n}(g_n) = \hat{F_n}(g_n) + p^n * \psi(\bar{g}_n) \Leftrightarrow$$

$$0 = p^n * \kappa(\hat{F}_n) + p^n * \psi(g) \Leftrightarrow$$
$$0 = \kappa(\hat{F}_n) + \psi(g)$$

□.

Wir betrachten nun den Raum der Derivationen, die eine echte Liftung induzieren und geben eine zu (2.3.4) ähnliche Parametrisierung des kleinen Liftungsraumes von F_{n-1}, die allerdings auf einer (leicht zu bestimmenden) quasi-Liftung als Basis aufbaut:

Satz 3.1.6. *Seien die Bezeichnungen wie oben. Dann gibt es eine 1-zu-1 Korrespondenz zwischen den Raum der kleinen Liftungen von F_{n-1} und dem Derivationsmodul:*

$$\mathcal{D}_g(\kappa) := \{\psi \in Der_F(k[x,y], A) |\ \psi(g) + \kappa(\hat{F}_n) = 0\}$$

gegeben durch die Zuordnung

$$\psi \rightsquigarrow F_n = \hat{F}_n + p^n * \psi$$

Beweis: folgt aus 3.1.2 und 3.1.5. □.

Unabhängigkeit der Parametrisierung von der gewählten Basis: Seien die Bezeichnungen wie in dem Satz und $\tilde{F}_n$ eine weitere quasi-Liftung von F_{n-1}. In dem von $\tilde{F}_n$ induzierten Parameterraum erhält man die kleine Liftung:

$$F_n := \hat{F}_n + p^n * \psi = \tilde{F}_n + p^n * \tilde{\psi}$$

durch die Wahl der Derivation $\tilde{\psi} := \psi + \eta$, wobei die Derivation $\eta \in \mathcal{D}$ der Differenz von $\hat{F}_n$ und $\tilde{F}_n$ entspricht (s. 2.3.1):

$$p^n * \eta := \hat{F}_n - \tilde{F}_n$$

Folglich spielt die Wahl der quasi-Liftung $\hat{F}_n$ keine Rolle für die Berechnung und Parametrisierung der kleinen Liftungen. Deswegen (sofern die Wahl der quasi-Liftung nicht spezifiziert ist) verwenden wir im Folgenden die triviale quasi-Liftung $\hat{F}_n$ von F_{n-1}, die durch die triviale Liftung (s. A.1) der Bilder der Basisvariablen gegeben ist:

$$\hat{F}_n(x) := (F_{n-1}(x))_n \text{ und } \hat{F}_n(y) := (F_{n-1}(y))_n$$

und bezeichnen das zugehörige Hindernis $\kappa(\hat{F}_n(x))$ als *Hindernis zur trivialen Liftung von F_{n-1}*. Wir werden die Bilder von F_{n-1} gelegentlich als Elemente des Ringes A_n auffassen, in diesem Fall wird stets die triviale Liftung dieser Bilder gemeint.

Variation der Liftung der definierenden Gleichungen:
Bisher haben wir festgewählte Liftungen A_n und B_n der Koordinatenringe betrachtet. In dem Rest des Abschnittes zeigen wir, wie das Hindernis κ sich in Abhängigkeit von der Liftung der definierenden Gleichungen ändert.

Zunächst betrachten wir die Änderung der Liftung der definierenden Gleichung g_n zu $\tilde{g}_n := g_n + p^n * \mu$ für ein $\mu \in k[x,y]$:

Lemma 3.1.7. *Seien die Bezeichnungen wir oben. Betrachte eine neue Liftung $\tilde{B}_n := k[x,y]/\tilde{g}_n$ des Koordinatenringes B. Dann erhält man das Hindernis $\tilde{\kappa}$ zur trivialen Liftung von $\hat{F}_{n-1}$ auf $\tilde{B}_n$ via*

$$\tilde{\kappa} = \kappa + F(\mu)$$

Beweis:
Die Aussage des Lemmas folgt aus der folgenden Rechnung:

$$\begin{aligned} p^n * \tilde{\kappa} &= \hat{F}_n(\tilde{g}_n) = \hat{F}_n(g_n + p^n * \mu) \\ &= \hat{F}_n(g_n) + p^n * F(\mu) = p^n * (\kappa + F(\mu)) \end{aligned}$$

$\square$.

Für die Untersuchung der Abhängigkeit von der Liftung f_n, betrachten für die Elemente $\bar{h} \in A_n$ folgenden Darstellung in $k[x,y]$:

$$\bar{h} = h + \pi f_n$$

So existiert ein eindeutiges $\bar{\pi} \in k[x]$, definiert durch:

$$F(g) = 0 + \bar{\pi} \cdot f \text{ in } k[x,y].$$

Betrachte nun eine weitere Liftung $\tilde{f}_n := f_n + p^n * \tau$ von f_{n-1} für ein $\tau \in k[x,y]$:

Lemma 3.1.8. *Seien die Bezeichnungen wir oben. Betrachte eine neue Liftung $\tilde{A}_n := k[x,y]/\tilde{f}_n$ des Koordinatenringes A. Dann erhält man das Hindernis $\tilde{\kappa}$ zur trivialen Liftung $\hat{F}_{n-1}$ auf $\tilde{A}_n$ via*

$$\tilde{\kappa} = \kappa + \bar{\pi} \cdot \tau$$

Beweis:
Betrachte die Darstellung des Hindernisses $p^n * \kappa$ in $R_n[x,y]$:

$$p^n * \kappa = \hat{F}_n(g_n) + \pi \cdot f_n \text{ für ein } \pi \in R_n[x,y]$$

Die Aussage des Lemmas folgt aus der folgenden Rechnung:

$$\hat{F}_n(g_n) = p^n * \kappa - \pi \cdot f_n = p^n * \kappa - \pi \cdot \tilde{f}_n + \pi \cdot p^n * \tau \text{ in } k[x,y] \Leftrightarrow$$

$$\hat{F}_n(g_n) = p^n * \kappa + p^n * (\bar{\pi} \cdot \tau) = p^n * \tilde{\kappa} \text{ in } \tilde{A}_n$$

□.

Betrachte nun die Abhängigkeit der kleinen Liftungen des Frobenius F_{n-1} von der Liftung $\tilde{f}_n := f_n + p^n * \tau$ der definierenden Gleichung:

Lemma 3.1.9. *Seien die Bezeichnungen wie oben und $\tilde{\kappa}$ das Hindernis zur trivialen Liftung von F_{n-1} auf $\tilde{B}_n = R_n[x,y]/(\tilde{f}_n)$. Dann gilt*

$$\tilde{\kappa} = \kappa + \mu^p \ ,$$

wobei κ das Hindernis zur trivialen Liftung von F_{n-1} auf B_n ist.

Beweis:
Zunächst bemerke, dass oben definiertes $\bar{\pi}$ verschwindet in A, denn

$$F(f^\sigma) = f^p \text{ und folglich } \bar{\pi} = f^{p-1} \text{ gilt.}$$

Nach dem Lemma 3.1.8 hat die Liftung des Koordinatenringes A keine Auswirkung auf das Hindernis und nach dem Lemma 3.1.7 ändert sich das Hindernis κ zu $\tilde{\kappa} = \kappa + F(\mu^\sigma) = \kappa + \mu^p$. □.

3.2 Explizite Parametrisierung der kleinen Liftungen

Die im Satz (3.1.6) gegebene Parametrisierung des Liftungsraumes liefert einen Ansatz zur Berechnung der Liftungen, bei dem man eine beliebig gewählte quasi-Liftung so entlang des Parameterraums deformiert, dass das zugehörige Hindernis verschwindet. In diesem Abschnitt führen wir den Deformationsvorgang auf das Lösen einer linearen Gleichung zurück.

Darstellung der Derivationen:
Für die Umsetzung des skizzierten Ansatzes benötigen wir eine konkretere Beschreibung des Parameterraums $\mathcal{D} = \mathrm{Der}_F(k[x,y], A)$ der quasi-Liftungen, sowie des Unterraums $\mathcal{D}_g(\kappa) := \{\psi \in \mathcal{D} | \psi(g) + \kappa = 0\}$ der echten Liftungen.

Die Derivationen aus $\mathcal{D}$ haben die Eigenschaft, dass $\psi(h)$ für jedes $h \in k[x,y]$ folgende eindeutige Darstellung als lineare Kombination von $\psi(x)$ und $\psi(y)$ besitzt:

$$\psi(h) = F(\tfrac{\partial h}{\partial x}) \cdot \psi(x) + F(\tfrac{\partial h}{\partial y}) \cdot \psi(y)$$

Insbesondere ist jedes $\psi \in \mathcal{D}$ durch die Bilder der Basisvariablen x und y

eindeutig bestimmt. Umgekehrt definiert jedes Paar $(U, V) \in A \times A$ eine Derivation $\psi \in \mathcal{D}$, die durch $\psi(x) := U$ und $\psi(y) := V$ gegeben ist. Diese Darstellung liefert folgende Charakterisierung des Untermoduls $\mathcal{D}_g(\kappa) \subset \mathcal{D}$:

Lemma 3.2.1. *Eine Derivation $\psi \in \mathcal{D}$ liegt genau dann in $\mathcal{D}_g(\kappa)$, wenn die Bilder der Variablen $\psi(x)$ und $\psi(y)$ folgende Gleichung in A erfüllen:*

$$F(\tfrac{\partial g}{\partial x}) \cdot \ \psi(x) + F(\tfrac{\partial g}{\partial y}) \cdot \ \psi(y) = \kappa$$

Beweis: folgt aus der Definition von $\mathcal{D}_g(\kappa)$ sowie den Derivationseigenschaften. □

Charakteristische Gleichung:
Eine unmittelbare Folgerung aus dieser Darstellung der Derivationen ist die Parametrisierung der kleinen Liftungen durch die Lösungen einer linearen Gleichung in dem Koordinatenring A.

Theorem 3.2.2. *Sei κ das Hindernis zur trivialen Liftung von F_{n-1}. Dann existiert eine 1-zu-1 Korrespondenz zwischen dem Raum der kleinen Liftungen von F_{n-1} und dem Lösungsraum der Gleichung:*

$$F(\tfrac{\partial g}{\partial x}) \cdot \psi_x + F(\tfrac{\partial g}{\partial y}) \cdot \psi_y + \kappa = 0$$

in den Unbekannten $\psi_x, \psi_y \in A$.

Beweis: folgt aus (3.2.1) und (3.1.6). □.

Definition 3.2.3. *Die lineare Gleichung aus dem Satz 3.2.2 nennen wir die* ***charakteristische Gleichung von*** F_{n-1} .

Ist das Paar (ψ_x, ψ_y) eine Lösung der charakteristischen Gleichung von $\hat{F}_n$, dann erhalten wir eine echte Liftung F_n von F_{n-1} durch:

$$F_n(x) := \hat{F}_n(x) + p^n * \psi_x \qquad F_n(y) := \hat{F}_n(y) + p^n * \psi_y$$

Umgekehrt liefert jede echte Liftung $\tilde{F}_n$ von F_{n-1} folgende Lösung der charakteristischen Gleichung:

$$\left(\tfrac{\tilde{F}_n(x) - \hat{F}_n(x)}{p^n}, \tfrac{\tilde{F}_n(y) - \hat{F}_n(y)}{p^n}\right)$$

Lösbarkeit der charakteristischen Gleichungen:
Die in 3.2.2 angegebene Gleichung ist immer lösbar, wenn man die Glattheit der Kurve C_B (mit dem Koordinatenring B) über den algebraischen Abschluss des Körpers k voraussetzt:

Lemma 3.2.4. *Seien die Bezeichnungen wie oben, wobei wir die Glattheit der Kurve C_B zusätzlich voraussetzen. Dann ist die charakteristische Gleichung von F_{n-1} lösbar.*

Beweis:
Nach dem Jakobi Glattheitskriterium sind die partiellen Ableitungen $\frac{\partial g}{\partial x}$ und $\frac{\partial g}{\partial y}$ teilerfremd in B und folglich existieren solche U_x und U_y, s.d. folgende Gleichung in B gilt:

$$\frac{\partial g}{\partial x} \cdot U_x + \frac{\partial g}{\partial y} \cdot U_y + 1 = 0$$

Wir wenden den Morphismus $\hat{F}$ auf diese Gleichung an:

$$F(\frac{\partial g}{\partial x}) \cdot F(U_x) + F(\frac{\partial g}{\partial y}) \cdot F(U_y) + 1 = 0$$

skalieren sie mit dem Hindernis κ

$$F(\frac{\partial g}{\partial x}) \cdot F(U_x) \cdot \kappa + F(\frac{\partial g}{\partial y}) \cdot F(U_y) \cdot \kappa + \kappa = 0$$

und erhalten daraus folgende Lösung der charakteristischen Gleichung:

$$\psi_x := F(U_x) \cdot \kappa \text{ und } \psi_y := F(U_y) \cdot \kappa$$

□.

Mit diesem Lemma haben wir insbesondere einen konstruktiven Existenzbeweis für die Liftungen der Morphismen auf glatten affinen Hyperflächen gegeben:

Korollar 3.2.5. *Sei $F : C_A \to C_B$ ein Morphismus zwischen affinen Hyperflächen, wobei C_B glatt ist. Für die Liftungen $\tilde{C}_A$ und $\tilde{C}_B$ über den artinschen Ring R_n existiert stets eine Liftung $\tilde{F} : \tilde{C}_A \to \tilde{C}_B$ von F über R_n.*

Beweis: der Satz 3.2.2 kombiniert mit 3.2.4 sichert die Existenz der kleinen Liftungen, deren induktive Berechnung die Behauptung des Lemmas beweist. □.

Lösung der charakteristischen Gleichungen:
Der Beweis des Lemmas 3.2.4 liefert zugleich einen Ansatz für die algorithmische Lösung einer charakteristischen Gleichung. In der Tat haben alle charakteristischen Gleichungen eine ähnliche Form:

$$F(\frac{\partial g}{\partial y}) \cdot \psi_y + F(\frac{\partial g}{\partial x}) \cdot \psi_x + \kappa = 0$$

und können auf das Lösen der folgenden normierten Gleichung zurückgeführt werden:

$$F(\tfrac{\partial g}{\partial y}) \cdot \breve{\psi}_y + F(\tfrac{\partial g}{\partial x}) \cdot \breve{\psi}_x + 1 = 0$$

Ist $(\breve{\psi}_x,\ \breve{\psi}_y)$ eine Lösung dieser Gleichung, so ist

$$(\psi_x := \kappa \cdot \breve{\psi}_x, \psi_y := \kappa \cdot \breve{\psi}_y)$$

eine Lösung der charakteristischen Gleichung von F_{n-1}. Diese normierte Gleichung hängt nur von der definierenden Gleichung g ab und wird im Folgenden die *Basisgleichung von B* genannt.

Die Basisgleichung kann im allgemeinen mit generischen Gröbnerbasen Algorithmen (z.B. Buchberger) gelöst werden, wenn es auch für konkrete Ausprägungen viel effizientere Methoden gibt, die wir im nächsten Abschnitt sowie in 4.2 an einigen Beispielen zeigen.

Parametrisierung des Raumes der kleinen Liftungen:
Zunächst seien die Liftung der Koordinatenringe vorgegeben. Die kleinen Liftungen $F_n : B_n \to A_n$ von F_{n-1} entsprechen nach dem Satz 3.2.2 genau den Lösungen der charakteristischen Gleichung von F_{n-1}. Also erhält man eine Parametrisierung der kleinen Liftungen indem man die Lösungen der charakteristischen Gleichung parametrisiert.

Sei (ψ_x, ψ_y) eine solche Lösung, dann erhält man alle anderen Lösungen dieser Gleichung durch Addition der Lösungen der Gleichung:

$$F(\tfrac{\partial g}{\partial y}) \cdot U_y + F(\tfrac{\partial g}{\partial x}) \cdot U_x = 0$$

die wegen der Teilerfremdheit von partiellen Ableitungen durch ein $\alpha \in A$ parametrisiert werden können:

$$U_x = \alpha \cdot F\left(\tfrac{\partial g}{\partial y}\right) \text{ und } U_y = -\alpha \cdot F\left(\tfrac{\partial g}{\partial x}\right)$$

Sei $(\breve{\psi}_x, \breve{\psi}_y)$ eine festgewählte Lösung der Basisgleichung von B und κ das Hindernis zur trivialen Liftung $\hat{F}_n$ von F_{n-1}. Die kleinen Liftungen von F_{n-1} sind nun parametrisiert durch:

$$F_n(x) := \hat{F}_n(x) + p^n * \left(\breve{\psi}_x \cdot \kappa + \alpha \cdot F(\tfrac{\partial g}{\partial y})\right)$$

$$F_n(y) := \hat{F}_n(y) + p^n * \left(\breve{\psi}_y \cdot \kappa - \alpha \cdot F(\tfrac{\partial g}{\partial x})\right).$$

Als nächstes erweitern wir diese Parametrisierung indem wir die Änderung der Liftungen der definierenden Gleichungen:

$$\tilde{g}_n = g_n + p^n * \mu \text{ und } \tilde{f}_n = f_n + p^n * \tau$$

in die Parametrisierung aufnehmen.

Theorem 3.2.6. *Alle kleine Liftungen von F_{n-1} sind parametrisiert durch α, μ und τ*

$$F_n(x) := \hat{F}_n(x) + p^n * \left(\breve{\psi}_x \cdot (\kappa + F(\mu) + \bar{\pi} \cdot \tau) + \alpha \cdot F(\tfrac{\partial g}{\partial y})\right)$$

$$F_n(y) := \hat{F}_n(y) + p^n * \left(\breve{\psi}_y \cdot (\kappa + F(\mu) + \bar{\pi} \cdot \tau) - \alpha \cdot F(\tfrac{\partial g}{\partial x})\right)$$

Dabei ist $\bar{\pi}$ wie in 3.1.8 definiert.

Beweis: folgt aus den Lemmas 3.1.7 und 3.1.8, sowie dem Theorem 3.2.2. □.

3.3 Berechnung der Liftungen: Algorithmus und Beispiele

In diesem Abschnitt skizzieren wir einen Liftungsalgorithmus für die Berechnung einer Liftung F_n von F und illustrieren es an einem konkreten Beispiel. Anschließend geben wir Beispiele der Liftungen auf singulären Kurven.

Liftungsalgorithmus:
Die Charakterisierung der Liftungen im Satz 3.2.2 ermöglicht die praktische Berechnung der kleinen Liftungen. Damit erhalten wir einen induktiven p-adischen Liftungsalgorithmus, mit dem man den Homomorphismus $F : B \to A$ zu einem Homomorphismus $F^\dagger : B^\dagger \to A^\dagger$ mit gewünschter Genauigkeit liften kann. Als Voraussetzung für die Durchführbarkeit des Algorithmus benötigen wir die Glattheit der Kurve C_B.

Im Rahmen der Vorberechnung wird bei dem Algorithmus eine Lösung $(\breve{\psi}_x, \breve{\psi}_y)$ der Basisgleichung von B berechnet:

$$F(\tfrac{\partial g}{\partial x}) \cdot \breve{\psi}_x + F(\tfrac{\partial g}{\partial y}) \cdot \breve{\psi}_y + 1 = 0$$

Wir skizzieren die Vorgehensweise im Liftungsschritt n, bei dem wir ausgehend von einer Liftung F_{n-1} eine kleine Liftung $F_n : B_n \to A_n$ berechnen:

1. *Berechnung des Hindernisses κ zur trivialen Liftung von F_{n-1}:*

   $$p^n \kappa := \hat{F}_n(g_n)$$

2. *Lösung der charakteristischen Gleichung von F_{n-1}:*

   $$(\psi_x := \breve{\psi}_x \cdot \kappa \,, \psi_y := \breve{\psi}_y \cdot \kappa)$$

3. *Berechnung der kleinen Liftung F_n von F_{n-1}:*

$$F_n(x) := \hat{F}_n(x) + p^n * \psi_x \text{ und } F_n(y) := \hat{F}_n(y) + p^n * \psi_y.$$

Die einzige rechnerisch aufwendige Operation dabei ist die Auswertung von $\hat{F}_n(g_n) \in A_n$ bei der Berechnung des Hindernisses. Diese Berechnung ist allerdings relativ schnell wegen der Tatsache, dass κ über k definiert ist. Die Komplexitätsfragen und erzielte Laufzeiten diskutieren wir in 4.5 für den implementierten Algorithmus zur Liftung des Frobeniusmorphismus.

Beispiel für die Durchführung des Algorithmus:
Den skizzierten Liftungsalgorithmus illustrieren wir nun an einem konkreten Beispiel. Betrachte eine über einen Körper $k \cong \mathbb{F}_p[t]/h(t)$ in Charakteristik 2 definierte Kurve C und die dazu isomorphe Kurve C^σ mit definierenden Gleichungen:

$$f = y^2 + xy + x^3 + t \text{ und } f^\sigma = y^2 + xy + x^3 + t^2.$$

sowie den zugehörigen Frobeniushomomorphismus:

$$F : A^\sigma = k[x,y]/(y^2 + xy + x^3 + t^2) \to A = k[x,y]/(y^2 + xy + x^3 + t)$$

Vorberechnung der Basisgleichung:
Betrachte die partiellen Ableitungen der definierenden Gleichung f^σ:

$$\frac{\partial f^\sigma}{\partial x} = y + x^2 \qquad \frac{\partial f^\sigma}{\partial y} = x$$

Die Basisgleichung der Kurve C ist nun gegeben durch

$$(y^2 + x^4) \cdot \breve{\psi}_x + x^2 \cdot \breve{\psi}_y + 1 = 0$$

Betrachte diese Gleichung modulo x^2. Wir erhalten die Kongruenz:

$$y^2 \cdot \breve{\psi}_x = (x^3 + xy + t) \cdot \breve{\psi}_x \equiv -1 \mod x^2$$

Ein Lösung dieser Kongruenz ist gegeben durch $\breve{\psi}_x = t^{-1} + t^{-2}xy$ und es gilt:

$$\begin{aligned}(y^2 + x^4) \cdot \breve{\psi}_x &= (x^4 + x^3 + xy + t^2) \cdot (t^{-1} + t^{-2}xy) \\ &= 1 + x^2 \cdot (t^{-1}(x^2 + x) + t^{-2}(x^3y + x^2y + x^2y^2))\end{aligned}$$

Setze $\breve{\psi}_y := t^{-1}(x^2+x)+t^{-2}(x^3y+x^2y+x^2y^2)$, dann ist $(\breve{\psi}_x, \breve{\psi}_y)$ eine Lösung der Basisgleichung.

1-er Liftungsschritt:
Wir wählen die triviale Liftung $\tilde{f}_1 = (y^2 + xy + x^3 + t)$ der definierenden Gleichung und erhalten folgende Liftungen der Koordinatenringe:

$$A_1 = R_1[x,y]/(y^2+xy+x^3+t) \qquad A_1^\sigma = R_1[x,y]/(y^2+xy+x^3+t^2)$$

Die triviale quasi-Liftung $\hat{F}_1$ von F_0 ist gegeben durch

$$\hat{F}_1(x) = x^2 \in A_1 \text{ und } \hat{F}_1(y) = y^2 \in A_1.$$

Betrachte den Term $\hat{F}_1(f_1^\sigma) \in A_1$. Es gilt:

$$\begin{aligned}\hat{F}_1(f_1^\sigma) &= y^4 + x^2y^2 + x^6 + t^2 \\ &= (xy+x^3+t)^2 + x^2y^2 + x^6 + t^2 \\ &= x^2y^2 + x^6 + t^2 + 2\cdot(x^4y + tx^3 + txy) + x^2y^2 + x^6 + t^2 \\ &= 2\cdot(x^6 + x^4y + tx^3 + x^2y^2 + txy + t^2) \neq 0 \text{ in } A_1\end{aligned}$$

Folglich ist $\kappa = x^6 + x^4y + tx^3 + x^2y^2 + txy + t^2 \in A$ das Hindernis zur trivialen Liftung von F_{n-1}. Damit ist $(\breve{\psi}_x \cdot \kappa, \breve{\psi}_y \cdot \kappa)$ eine Lösung der charakteristischen Gleichung von F_{n-1} und wir erhalten die Parametrisierung der kleinen Liftungen $F_1 : A_1^\sigma \to A_1$ von F_0 via:

$$F_1(x) = x^2 + 2\cdot(\breve{\psi}_x \cdot \kappa + x^2 \cdot \alpha)$$
$$F_1(y) = y^2 + 2\cdot(\breve{\psi}_y \cdot \kappa + (y^2+x^4) \cdot \alpha)$$

für alle $\alpha \in A$.

Größe der Liftung:
Die berechnete Lösung $(\breve{\psi}_x \cdot \kappa, \breve{\psi}_y \cdot \kappa)$ liefert eine relativ „große“ Liftung, gemessen an den Graden von $F_1(x)$ und $F_1(y)$, denn es existieren auch „kleinere“ Liftungen. Betrache die charakteristische Gleichung

$$(y^2+x^4)\cdot\psi(x) + x^2\cdot\psi(y) = x^6 + x^4y + tx^3 + x^2y^2 + txy + t^2$$

modulo x^2. Wir erhalten eine Kongruenz:

$$y^2\cdot\psi(x) = (x^3+xy+t)\cdot\psi(x) \equiv t^2 + txy \mod x^2$$

mit einer Lösung $\psi(x) = t$. Die entsprechende Lösung der charakteristischen Gleichung ist dann gegeben durch

$$\big(\psi(x) = t\,,\ \psi(y) = y^2 + x^4 + x^2y + tx^2\big)$$

2-er Liftungsschritt:
Möchte man F_0 über R_2 liften, so wiederholt man dieselben Berechnungen aufbauend auf einer berechneten Liftung F_1. Dabei ist es algorithmisch vorteilhaft die folgende „kleinere“ Liftung F_1 zu verwenden:

$$F_1(x) = x^2 + 2\cdot t \qquad F_1(y) = y^2 + 2\cdot(y^2 + x^4 + x^2y + tx^2)$$

Sei $f_2 = y^2+xy+x^3+t \in R_2[x,y]$ eine Liftung der definierenden Gleichung. Das Hindernis zu der trivialen quasi-Liftung berechnen wir durch:

$$\kappa(\hat{F}_2(x)) = \frac{\hat{F}_2(f_2^\sigma)}{4} = (t+1)x^2y^2 + x^5y + txy + x^8 + (t^2+t)x^4 + t^2$$

und erhalten automatisch eine Liftung:

$$F_2(x) = x^2 + 2\cdot t + 4\cdot(\breve{\psi}_x \cdot \kappa_2)$$
$$F_2(y) = y^2 + 2(y^2 + x^4 + x^2y + tx^2) + 4(\breve{\psi}_y \cdot \kappa_2)$$

wobei auch hier eine viel „kleinere“ Liftung existiert (die Bestimmung einer möglichst „kleinen“ Liftung diskutieren wir in 4.3):

$$F_2(x) = x^2 + 2\cdot t + 4\cdot t$$
$$F_2(y) = y^2+2\cdot(y^2+x^4+x^2y+tx^2)+4\cdot((t+1)y^2+x^3y+x^6+t^2x^2+tx)$$

Liftungen auf singulären Hyperflächen:
Zum Schluss des Abschnittes diskutieren wir die Liftungen im singulären Fall. Sei C eine singuläre affine Hyperfläche, dann haben die partiellen Ableitungen der definierenden Gleichungen einen gemeinsamen Teiler, s.d. die Basisgleichung von C keine Lösung besitzt. Die charakteristische Gleichung eines Morphismus kann trotzdem lösbar sein.

Beispiel 1:
Betrachte z.B. die Kurve $C : f := y^2 + x^5 + x^2 = 0$ in Charakteristik 3 und den Frobeniusmorphismus $F = F_0 : C^\sigma \to C$. Diese Kurve hat eine Singularität in $(0,0)$ und die Terme

$$(\frac{\partial f^\sigma}{\partial y})^p = 2y^3 = 2y(x^5+x^2)^2 = 2y(x^3+1)^2\cdot x^4$$
$$(\frac{\partial f^\sigma}{\partial x})^p = 5x^{12} + 2x^3$$

haben einen gemeinsamen Teiler x^3.

Wir wählen die triviale Liftung $f_1 = y^2 + x^5 + x^2$ über R_1 und berechnen das Hindernis zu $\hat{F}_0$:

$$\kappa = \frac{F_0(f_1)}{p} = x^{12} + x^9$$

Es ist auch teilbar durch x^3 und folglich ist die charakteristische Gleichung von F_0 lösbar. Wählt man dagegen die Liftung $\tilde{f}_1 = y^2 + x^5 + x^2 + 3$, dann gilt $\kappa = x^{12}+x^9+2$. Die charakteristische Gleichung hat in diesem Fall keine Lösung, da beide partielle Ableitungen einen gemeinsamen Teiler x haben. Also existiert keine Liftung des Frobenius auf der durch $\tilde{f}_1$ gegebener affinen

Kurve $\tilde{C}_1$.

Wir vermuten, dass für jede affine Hyperfläche C stets eine solche Liftung der definierenden Gleichung existiert, so dass auch der Frobeniusmorphismus darauf liftbar ist. In den meisten Fällen ist die Wahl der trivialen Liftung der definierenden Gleichung ausreichend (wie im obigen Beispiel), jedoch nicht immer:

Beispiel 2:
Betrachte die Kurve $C: f := y^2 + x^5 + x^2 = 0$ in Charakteristik 2 und deren triviale Liftung $C_1: f_1 := y^2 + x^5 + x^2 = 0$ über R_1. Das Hindernis zur trivialen Liftung ist gleich $\kappa = x^{10} + x^7 + x^4$ und die charakteristische Gleichung ist gegeben durch

$$0 \cdot \psi_y + x^8 \cdot \psi_x = x^{10} + x^7 + x^4$$

Diese Gleichung hat keine Lösung in $A = k[x, y]/(y^2 + x^5 + x^2)$. Aber auch in diesem Fall existiert eine Liftung der Kurve, für die eine Liftung des Frobenius existiert. Betrachte die Liftung $\tilde{f}_1 := y^2 + x^5 + x^2 + 2 \cdot xy = 0$ über R_1. Das Hindernis ist gleich

$$\kappa = x^{10} + x^7 + x^4 + x^2y^2 = x^{10} + x^7 + x^4 + x^2(x^5 + x^2) = x^{10}$$

und die Lösungen der charakteristischen Gleichung sind gegeben durch

$$(\psi_x = x^2, \psi_y = \alpha), \text{ für ein } \alpha \in A.$$

3.4 Verallgemeinerungen

Im vorigen Kapitel haben wir affine Hyperflächen betrachtet, deren Koordinatenringe nur eine definierende Gleichung hatten. Diese Einschränkung hatte keine fundamentalen Ursachen, so dass alle Ergebnisse sich für affine Varietäten mit mehreren definierenden Gleichungen auf eine natürliche Weise verallgemeinern lassen.

Seien $V_B = \mathbb{V}(\{f_i\}) \in \mathbb{A}^r$ und V_A affine Varietäten und

$$F: B := k[x_1, \ldots, x_r]/(g_1, \ldots g_m) \to A$$

ein Homomorphismus zwischen den Koordinatenringen. Wir betrachten eine Liftung $F_{n-1} : B_{n-1} \to A_{n-1}$ von F über R_{n-1} und zeigen, wie man alle kleine affine Liftungen von F_{n-1} parametrisieren und berechnen kann.

Unsere Vorgehensweise ist analog zu der im früheren Abschnitten. Wir betrachten die quasi-Liftungen auf Polynomringen und Hindernisse zu deren Einschränkung auf die Koordinatenringe. Die Deformation des Parameterraums der quasi-Liftungen, bei der die Hindernisse eliminiert werden, führen wir auf das Lösen eines linearen Gleichungssystems über den Koordinatenring A zurück.

Quasi-Liftungen und Hindernisse:
Sei $\hat{F}_n : R_n[x_1, \ldots, x_r] \to A_n$ eine quasi-Liftung von F_{n-1}, die wir als Liftung des von F_{n-1} induzierten Morphismus $\hat{F}_{n-1} : R_{n-1}[x_1, \ldots, x_r] \to A_{n-1}$ erhalten. Wir definieren das Hindernis zu der quasi-Liftung $\hat{F}_n$ auf A_n als ein m-Tupel $\{\kappa_j(\hat{F}_n) \in A\}$, definiert durch:

$$\{\hat{F}_n(g_j) = p^n * \kappa_j\}_{0<j\leq m} ,$$

wobei die Komponenten κ_j die Verträglichkeit mit der definierenden Gleichung $\tilde{g}_j$ indizieren. Dieses Hindernis verschwindet genau dann, wenn $\hat{F}_n$ eine echte Liftung von F_{n-1} ist.

Aus dem Korollar 2.3.4 folgt, dass jede weitere quasi-Liftung $\tilde{F}_n$ von F_{n-1} durch eine Derivation ψ aus $\mathrm{Der}_F(k[x_1, \ldots, x_r], A)$ via:

$$\tilde{F}_n := \hat{F}_n + p^n * \psi$$

eindeutig gegeben ist und dass jede Derivation aus $\mathrm{Der}_F(k[x_1, \ldots, x_r], A)$ auf diese Weise eine quasi-Liftung von F_{n-1} induziert.

Charakteristisches Gleichungssystem:
Dieselben Argumenten wie im Abschnitt 3.1 liefern die Bedingung dazu, dass eine durch die Derivation ψ induzierte quasi-Liftung eine echte Liftung ist. So ist eine quasi-Liftung $\tilde{F}_n = \hat{F}_n + p^n * \psi$ genau dann echt, wenn sie das folgende Gleichungssystem erfüllt:

$$\{\kappa_j(\hat{F}_n) + \psi(g_j) = 0\}_{0<j\leq m}$$

Der Ausdruck $\psi(g_j)$ läßt sich stets als eine Linearkombination der Bilder der Basisvariablen schreiben:

$$\psi(g_j) = \sum_{i=1}^{r} \psi(x_i) \cdot F(\tfrac{\partial g_j}{\partial x_i})$$

Auf diese Weise erhalten wir ein Analogon zu der charakteristischen Gleichung, das in dem allgemeinen Fall durch ein Gleichungssystem in A gegeben ist, das wir das *charakteristische Gleichungssystem von* F_{n-1} nennen. Die Ergebnisse fassen wir in dem folgenden Theorem zusammen:

Theorem 3.4.1. *Seien die Bezeichnungen wie oben, dann gibt es 1-zu-1 Korrespondenz zwischen dem Raum der kleinen Liftungen von F_{n-1} (für fixierte Liftungen der Varietäten), dem Derivationsmodul*

$$\mathcal{D}_{\{g_j\}}(\{\kappa_j\}) = \{\psi \in Der_F(k[x_1, \dots x_n], A) \mid \psi(g_j) = \kappa_j := \tfrac{\hat{F}_n(g_j)}{p^n}\}$$

und dem Lösungsraum des folgenden Gleichungssystems aus m Gleichungen in r Unbekannten $\{\psi_i \in A\}$:

$$\left\{ \sum_{i=1}^{r} F(\tfrac{\partial g_j}{\partial x_i}) \cdot \psi_i = \kappa_j \right\}_{1 \le j \le m}$$

gegeben durch die folgende Zuordnung:

$$\left\{ F_n(x_i) = \hat{F}_{n-1}(x_i) + p^n * \psi(x_i) = \hat{F}_{n-1}(x_i) + p^n * \psi_i \right\}_{1 \le i \le r}$$

Beweis: erfolgt genauso wie in 3.1.6 und 3.2.2. □.

Auch die Parametrisierung des Liftungsraumes, insbesondere mit Berücksichtigung der Liftungen der definierenden Gleichungen kann analog zu der Vorgehensweise in 3.2 erfolgen.

Berechnung der Liftungen
Die Idee des Liftungsalgorithmus lässt sich entsprechend verallgemeinern, wenn auch die praktische Umsetzung im allgemeinen Fall ziemlich aufwendig erscheint. Die Struktur des n-ten Liftungsschrittes des Algorithmen sieht genau so aus, wie im Fall der Hyperflächen:

1. *Berechnung der Hindernisse:*

$$\left\{ \kappa_j := \tfrac{\hat{F}_n(f_j^\sigma)}{p^n} \right\}_{1 \le j \le m}$$

2. *Lösung des charakteristischen Gleichungssystems:*

$$\left\{ \sum_{i=1}^{r} F(\tfrac{\partial g_j}{\partial x_i}) \cdot \psi_i = \kappa_j \right\}_{1 \le j \le m}$$

3. *Berechnung der kleinen Liftung:*

$$\left\{ F_n(x_i) := \hat{F}_{n-1}(x_i) + p^n * \psi_i \right\}_{1 \le i \le r}$$

Die Lösbarkeit des charakteristischen Gleichungssystems und damit die Durchführbarkeit des angegebenen Algorithmus kann wie in 3.2.4 aus dem Jacobi Glattheitskriterium gefolgert werden, falls die Varietät V_B glatt ist.

Liftungen auf singulären Varietäten
Die Parametrisierung der kleinen Liftungen durch Derivationen, bzw. Charakterisierung durch Lösungen der entsprechenden linearen Gleichungen gilt auch für die singulären Varietäten. Das charakteristische Gleichungssystem ist bei singulären Varietäten jedoch nicht notwendigerweise lösbar (s. Beispiele in 3.3).

Falls man jedoch bei der Liftung der Koordinatenringe die Hinzunahme der neuen Basisvariablen zulässt, dann kann man die Lösbarkeit des resultierenden charakteristischen Gleichung stets erzwingen und damit eine kleine Liftung der Kurve zusammen mit dem Morphismus finden. Insbesondere kann man dabei die bekannte Auflösung der Singularitäten verwenden.

3.5 Liftung auf lokalisierten Koordinatenringen

In diesem Abschnitt illustrieren wir die Verallgemeinerung auf mehrere definierende Gleichungen an dem Beispiel der lokalisierten Koordinatenringen der affinen Hyperflächen. Anschließend diskutieren wir den Zusammenhang zwischen den Liftungen auf Koordinatenringen und auf deren Lokalisierungen.

Lokalisierte Koordinatenringe:
Sei C eine affine Kurve mit dem Koordinatenring $B = k[s,t]/(g(s,t))$. In diesem Abschnitt betrachten wir die affine Kurve $C_{(t)}$, die man als Durchschnitt der Kurve C mit der offenen Umgebung $\{t \neq 0\}$ erhält. Den Koordinatenring dieses Durchschnittes erhalten wir dadurch, dass wir den Ring B nach der Variablen t lokalisieren. Den dadurch entstehenden Ring bezeichnen wir mit

$$B_{(t)} = k[s,t,t^{-1}]/(g(s,t))$$

Den t^{-1}-Grad eines Elementen $\bar{h}$ von $B_{(t)}$ definieren wir als minimalen t^{-1}-Grad aller Repräsentanten $h \in k[s,t,t^{-1}]$ der Restklasse von $\bar{h}$.

Die Kurve $C_{(t)}$ besitzt eine natürliche Einbettung $i_t : C_{(t)} \hookrightarrow C$. Diese Einbettung induziert einen injektiven Ringhomomorphismus $i_t : B \to B_{(t)}$ auf Koordinatenringen, definiert durch die Zuordnung

$$i_t(t) := t \text{ und } i_t(s) := s.$$

Das Bild der Abbildung i_t besteht genau aus solchen Elementen g des Quo-

tientenringes $B_{(t)}$, für die man t^{-1}-Terme eliminieren kann und folglich $\deg_{t^{-1}} g = 0$ gilt.

Betrachte nun einen Morphismus $F^t : B_{(t)} \to A_{(t)}$ zwischen den lokalisierten Koordinatenringen. Außer der induzierten definierenden Gleichung $g(s,t) = 0$ besitzt der lokale Ring $B_{(t)}$ eine zusätzliche definierende Gleichung:

$$t \cdot t^{-1} - 1 = 0 \text{ in } B_{(t)}$$

Folglich muss eine Liftung F^t_n von F^t mit den Liftungen beider Gleichungen verträglich sein, wobei wir die zweite Gleichung im Folgenden stets trivial liften:

$$t \cdot t^{-1} - 1 = 0 \text{ in } B_{(t),n} := R_n[s,t,t^{-1}]/(g_n(s,t))$$

Charakterisierung der kleinen Liftungen
Seien $F^t_{n-1} : B_{(t),n-1} \to A_{(t),n-1}$ eine Liftung des Frobenius über R_{n-1} und $\hat{F}^t_n : R_n[s,t,t^{-1}] \to A_{(t),n}$ eine quasi-Liftung von F^t_{n-1} auf den Ring $A_{(t),n} := R_n[s,t,t^{-1}]/(g_n)$. Das Hindernis zur Einschränkung von $\hat{F}^t_n$ ist gegeben durch das Paar $(\kappa_s \in A_{(t)}, \kappa_t \in A_{(t)})$, definiert via:

$$p^n * \kappa_s := \hat{F}^t_n(g_n)$$
$$p^n * \kappa_t := \hat{F}^t_n(t) \cdot \hat{F}^t_n(t^{-1}) - 1$$

Die Liftungen auf den lokalisierten Ringen sind dann parametrisiert durch den Derivationsmodul $\mathcal{D}_g(\kappa_s, \kappa_t) \subset \mathcal{D} := \mathrm{Der}(k[s,t,t^{-1}], A)$:

$$\mathcal{D}_g(\kappa_s, \kappa_t) := \{\xi |\ \xi(g) + \kappa_s = 0,\ \xi(t \cdot t^{-1} - 1) + \kappa_t = 0\}$$

Da die partiellen Ableitungen von $t \cdot t^{-1} - 1$ nach t, bzw. t^{-1} gleich t^{-1}, bzw. t sind, besteht das charakteristische Gleichungssystem über $A_{(t)}$ aus folgenden Gleichungen:

$$F(\tfrac{\partial g}{\partial s}) \cdot\ \xi_s + F(\tfrac{\partial g}{\partial t}) \cdot\ \xi_t = \kappa_s$$
$$F(t) \cdot\ \xi_{t^{-1}} + F(t^{-1}) \cdot\ \xi_t = \kappa_t$$

wobei die erste Gleichung, der charakteristischen Gleichung der kleinen Liftungen der Hyperfläche C entspricht.

Liftungen auf Koordinatenringen und deren Lokalisierungen:
Auf dem Koordinatenring $A_{(t)}$ hat man einen größeren Raum für Deformationen und dadurch mehr Liftungen der Morphismen als auf dem Ring A. Diese (intuitiv klare) Behauptung können wir nun auch formal beweisen.

Wir zeigen zunächst, dass die Einschränkung einer Derivation aus $\mathcal{D}_g(\kappa_s)$ zu einer Derivation $\psi_i := i_t(\psi) \in \mathcal{D}_g(\kappa_s, \kappa_t)$ wohldefiniert und eindeutig ist.

Lemma 3.5.1. *Für jede Derivation $\psi \in \mathcal{D}_g(\kappa_s)$ existiert stets eine eindeutige Derivation $\xi \in \mathcal{D}_g(\kappa_s, \kappa_t)$ für die*

$$\xi(t) = i_t(\psi(t)) \text{ und } \xi(s) = i_t(\psi(s)) \text{ gilt.}$$

Das Bild von t^{-1} ist dann gegeben durch:

$$\xi(t^{-1}) = -F(t^{-1}) \cdot \kappa_t - F(t^{-1})^2 \cdot \xi(t)$$

Beweis:
Da die Bilder $\xi(t)$ und $\xi(s)$ fest vorgegeben sind, ist die Derivation ξ durch die Wahl von $\xi(t^{-1})$ eindeutig bestimmt. Für jede solche Derivation verschwindet das Hindernis κ_s nach der Konstruktion. Also reicht es zu zeigen, dass es genau eine Wahl für $\xi(t^{-1})$ gibt, für die das Hindernis κ_t verschwindet. Das folgt unmittelbar aus der folgenden Umformung der ersten charakteristischen Gleichung:

$$\kappa_t = \xi(t \cdot t^{-1} - 1) \Leftrightarrow$$
$$\kappa_t = F(t^{-1}) \cdot \xi(t) + F(t) \cdot \xi(t^{-1}) \Leftrightarrow$$
$$\xi(t^{-1}) := -F(t^{-1}) \cdot \kappa_t - F(t^{-1})^2 \cdot \xi(s)$$

□.

Eine unmittelbare Folgerung aus dem Lemma ist die Existenz und Eindeutigkeit der Einschränkung der Liftung $F_n : B_n \to A_n$ zu einer Liftung F_n^t auf den lokalisierten Koordinatenringen:

Satz 3.5.2. *Sei $F_n : B_n \to A_n$ eine Liftung von F über R_n, dann existiert genau eine Liftung $F_n^t : B_{(t),n} \to A_{(t),n}$ von F^t über R_n für die*

$$F_n^t(s) = i_t(F_n(s)) \text{ und } F_n^t(t) = i_t(F_n(t)) \text{ gilt}$$

Beweis:
Wir führen den Beweis induktiv mit der Induktionsbasis für $n = 0$, gegeben durch $F^t(t^{-1}) := t^{-p}$. Der Induktionsschritt $n - 1 \mapsto n$ folgt aus der Parametrisierung der Liftungsräume durch Derivationen und deren eindeutigen Einschränkung (3.5.1). □.

Umgekehrt sind nur wenige Liftungen auf den lokalisierten Ringen $A_(t)$ durch die Einschränkungen der Liftungen auf A induziert. Solche Liftungen sind charakterisiert genau durch den verschwindenden t^{-1}-Grad der Bilder:

Lemma 3.5.3. *Sei F_n^t eine Liftung von F^t. Eine Liftung F_n von F, für die $i_t(F_n) = F_n^t$ gilt, existiert genau dann, wenn F_n^t folgende Bedingungen erfüllt:*

$$\deg_{t^{-1}} F_n^t(s) = 0, \qquad \deg_{t^{-1}} F_n^t(t) = 0$$

Beweis: folgt aus der Tatsache dass $i_t(F_n(t))$ und $i_t(F_n(s))$ nach Konstruktion keine t^{-1}-Terme enthalten. $\square$.

Die Liftungen auf den lokalisierten Koordinatenringen werden wir bei der Betrachtung der Liftungen des Frobenius aus dem Kedlaya Algorithmus in 4.4 sowie bei der Verklebung der projektiven Morphismen auf Durchschnitten der affinen Karten im Kapitel 5 weiterverwenden und expliziter ausführen.

Kapitel 4

Liftungen des Frobenius auf hyperelliptischen Kurven

Die Ergebnisse die wir für Morphismen zwischen den affinen Varietäten (und insbesondere Hyperflächen) erzielt haben, wenden wir in diesem Kapitel auf den Frobeniusmorphismus auf affinen hyperelliptischen Kurven in der ungeraden Charakteristik $p > 2$ an.

Die definierende Gleichung der hyperelliptischen Kurve besitzt eine für die Berechnungen besonders günstige Form, bei der man die Hindernisse zur trivialen Liftung, sowie die charakteristischen Gleichungen in einer Variablen auffassen kann. Wir zeigen wie die explizite Parametrisierung der kleinen Liftungen in diesem Fall aussieht und wie sie für die Berechnung der Liftungen mit gewünschten Eigenschaften (wie z.B. die Minimalität der Grade der Polynomen $F_n(x)$ oder $F_n(y)$) angewendet werden kann.

Anschließend disskutieren wir die Anwendungen auf das Punktezählproblem und insbesondere auf die Beschleunigung der Reduktion der Differentialformen durch eine geeignete Wahl der Liftung des Frobenius. Insbesondere gehen wir auf die Komplexität sowie die praktisch erzielten Laufzeiten des implementierten Algorithmus ein.

4.1 Hyperelliptische Liftungen

Dieser Abschnitt beginnt mit der Definition der hyperelliptischen Kurven und deren Liftungen sowie des Frobeniusmorphismus darauf. Anschließend betrachten wir die hyperelliptische Involution und definieren die hyperellip-

tischen Liftungen des Frobenius, die mit dieser Involution verträglich sind.

Hyperelliptischen Kurven und deren Liftungen

Definition 4.1.1. *Unter einer* ***hyperelliptischen Gleichung*** *(in einer ungeraden Charakteristik) verstehen wir eine Gleichung von der Form*

$$y^2 = f(x)$$

wobei $f \in k[x]$ *ein monisches Polynom ohne doppelte Nullstellen ist. Unter einer* ***affinen hyperelliptischen Kurve*** *vom Geschlecht* g *über einen Körper* k *verstehen wir eine affine Kurve* C*, die durch eine hyperelliptische Gleichung vom Grad* $2g+1$ *(oder* $2g+2$*) definiert ist.*

Bei der Liftung der hyperelliptischen Kurven soll die Form und Grad der definierenden Gleichung erhalten bleiben, also beschränken wir uns auf solche Liftungen der Kurve über den Quotientenringen R_n, die durch die hyperelliptischen Gleichungen von demselben x-Grad definiert sind.

Diese Liftungen haben ähnliche Eigenschaften wie die affinen hyperelliptischen Kurven über einem Körper. So sind sie auch glatt nach dem Jakobi Kriterium und insbesondere dadurch charakterisiert, dass es einen Morphismus $C_n \to \mathbb{A}^1_{R_n}$ vom Grad 2 gibt.

Für die Elemente der Koordinatenringe $A = k[x,y]/(y^2 - f(x))$ und dessen Liftungen $A_n = R_n[x,y]/(y^2 - f_n(x))$ benutzen wir im Folgenden eine normalisierte Form, die durch das Eliminieren der Variablen y entsteht. Also betrachten wir für jedes Element des Quotientenringes A_n denjenigen eindeutigen Vertreter $g \in R_n[x,y]$ der Restklasse, für den $\deg_y g < 2$ gilt. In dieser Form ist der x-Grad von $h \in A_n$ eindeutig definiert.

Betrachte den relativen Frobeniushomomorphismus zwischen diesen Koordinatenringen:

$$F : A^\sigma = k[x,y]/(y^2 - f^\sigma(x)) \to A = k[x,y]/(y^2 - f(x))$$

In dem Rest des Kapitels sei $F_{n-1} : A^\sigma_{n-1} \to A_{n-1}$ eine Liftung von F über R_{n-1}, deren kleine Liftungen

$$F_n : A^\sigma_n = R_n[x,y]/(y^2 - f^\sigma_n(x)) \to A_n = R_n[x,y]/(y^2 - f_n(x))$$

wir parametrisieren und berechnen werden.

Hyperelliptische Involution:
Unter einer *hyperelliptischen Involution* auf einer affinen hyperelliptischen Kurve C verstehen wir einen Automorphismus von C, der den Punkt (X, Y) auf $(X, -Y)$ abbildet. Diese Involution existiert stets und induziert eine Involution auf den Koordinatenringen:

$$i : A \to A$$
$$x \mapsto x,\ y \mapsto -y$$

Für die Liftungen A_n und A_n^σ der Koordinatenringen von C und C^σ definieren wir die hyperelliptishe Involution analog durch:

$$i : A_n \to A_n \qquad i^\sigma : A_n^\sigma \to A_n^\sigma$$
$$x \to x,\ y \to -y \qquad x \to x,\ y \to -y$$

Der Ring $A_n = R_n[x, y]/(y^2 - f(x))$ zerfällt unter der Involution i in eine direkte Summe

$$A_n = R_n[x, y]/(y^2 - f(x)) \equiv R_n[x] \oplus y \cdot R_n[x]$$

Die hyperelliptische Involution operiert dabei trivial auf dem Unterraum $R_n[x]$ und auf dem Unterraum $y \cdot R_n[x]$ ist diese Operation durch die Gleichung $i(h) = -h$ definiert. Die Elemente des Unterraums $R_n[x]$ bezeichnen wir im Folgenden als *x-Polynome*.

Hyperelliptischen Liftungen des Frobenius:
Als nächstes definieren wir eine spezielle Klasse der Liftungen des Frobenius, die wir in dem Rest des Kapitels betrachten:

Definition 4.1.2. *Wir nennen eine Liftung F_n eine **hyperelliptische Liftung des Frobenius**, wenn das Bild $F_n(x)$ ein x-Polynom ist.*

Diese Definition ist insbesondere dadurch motiviert, dass solche Liftung des Frobenius durch die Verträglichkeit mit der hyperelliptischen Involution charakterisiert sind, die wir im Rest des Abschnittes beweisen.

Zunächst zeigen wir, dass $F_n(y)$ stets durch ein x-Polynom eindeutig bestimmt ist:

Lemma 4.1.3. *Sei F_n eine hyperelliptische Liftung des Frobenius auf A_n, dann liegt $F_n(y)$ in $y \cdot R_n[x] \subset A_n$.*

Beweis:
Wir wenden den F_n auf die definierende Gleichung $y^2 - f_n(x)$ an:

$$F_n(y)^2 = F_n(y^2) = F_n(f_n(x)) = f_n(F_n(x))$$

Betrachte die normalisierte Darstellung von $F_n(y)$ und von $F_n(y)^2$

$$F_n(y) = h_x + y \cdot h_y$$
$$F_n(y)^2 = (h_x + y \cdot h_y)^2 = (h_x^2 + f(y)h_y^2) + y \cdot 2h_x h_y$$

wobei h_x,h_y in $R_n[x]$ liegen. Da $F_n(y)^2 = F_n(x)$ nach der Voraussetzung ein x-Polynom ist, verschwindet h_x oder h_y. Folglich liegt $F_n(y)$ entweder in $R_n[x]$ oder ganz in $y \cdot R_n[x]$. Da die Liftung des Frobenius F_n die Äquivalenz:

$$F_n(y) \equiv y^p = y \cdot f^{\frac{p-1}{2}} \bmod p$$

für ein ungerades p erfüllt, ist die Aussage des Lemmas bewiesen. □.

Nun betrachten wir die Verträglichkeit einer Liftung $F_n : A_n^\sigma \to A_n$ mit der hyperelliptischen Involution:

$$F_n \circ i_\sigma = i \circ F_n$$

wobei i die zu A und i_σ die zu A^σ zugehörigen hyperelliptischen Involutionen sind.

Satz 4.1.4. *Eine Liftung F_n ist genau dann mit der hyperelliptischen Involution verträglich, wenn F_n hyperelliptisch ist.*

Beweis:
$''\Rightarrow''$:
Sei F_n mit der hyperelliptischen Involution verträglich. Dann gilt:

$$F_n(x) = F_n(i_\sigma(x)) = i(F_n(x))$$

und folglich liegt $F_n(x)$ in dem i-invarianten Unterraum $R_n[x] \subset A_n$. □.

$''\Leftarrow''$:
Sei F_n eine hyperelliptische Liftung des Frobenius. Weiterhin sei $h \in A_n$, mit der normalisierten Form:

$$h = h_x + y \cdot h_y \text{ , wobei } h_x \text{ und } h_y \text{ } x\text{-Polynome sind.}$$

Dann gilt:

$$i(F_n(h)) = i(F_n(h_x)) + i(F_n(y)) \cdot i(F_n(h_y))$$

Nach der Voraussetzung liegen $F_n(h_x)$ und $F_n(h_y)$ in $R_n[x]$ und sind also i-invariant. Daraus folgt:

$$i(F_n(h)) = F_n(h_x) + i(F_n(y)) \cdot F_n(h_y)$$

Nach dem Lemma (4.1.3) liegt $F_n(y)$ in dem Unterraum $y \cdot R_n[x] \subset A_n$ und folglich gilt $i(F_n(y)) = -F_n(y)$. Damit folgt die gewünschte Verträglichkeit

wegen:

$$i(F_n(h)) = F_n(h_x) - F_n(y) \cdot F_n(h_y) = F_n(h_x - y \cdot h_y) = F_n(i_\sigma(h))$$

□.

4.2 Berechnung der kleinen hyperelliptischen Liftungen, Beispiele

In diesem Abschnitt beschreiben wir die Parametrisierung des Raumes der kleinen hyperelliptischen Liftungen des Frobenius und zeigen wie solche Liftungen praktisch berechnet werden.

Hindernisse zu den hyperelliptischen quasi-Liftungen
Sei F_{n-1} eine hyperelliptische Liftung von Frobenius über R_{n-1}. Eine quasi-Liftung $\hat{F_n} : R_n[x,y] \to A_n$ von F_{n-1}, die die Bedingung $\hat{F_n}(x) \in R_n[x]$ erfüllt nennen wir eine *hyperelliptische quasi-Liftung.*

Das Hindernis zu einer solchen quasi-Liftung ist immer ein x-Polynom. In der Tat liegen sowohl $\hat{F_n}(y)^2$ als auch $\hat{F_n}(f_n(x))$ in $R_n[x]$, so dass auch $\kappa(\hat{F_n})$, definiert durch:

$$p^n * \kappa(\hat{F_n}) := \hat{F_n}(y^2 - f_n(x)).$$

notwendigerweise in $k[x]$ liegt.

Charakteristische Gleichung der hyperelliptischen Liftungen:
Die charakteristische Gleichung der kleinen Liftungen von F_{n-1} auf A_n ist gegeben durch:

$$(\tfrac{\partial(y^2-f(x))}{\partial y})^p \cdot \psi_y + (\tfrac{\partial(y^2-f(x))}{\partial x})^p \cdot \psi_x + \kappa = 0 \text{ in } A,$$

Nach dem Berechnen der partiellen Ableitungen erhält man folgende Gleichung über A:

$$2y^p \cdot \psi_y - f'(x)^p \cdot \psi_x + \kappa = 0$$

Liegt ψ_y in $y \cdot k[x]$, dann kann man diese Gleichung zu einer äquivalenten Gleichung mit den Koeffizienten in $k[x]$ umformen:

$$2f^{\frac{p+1}{2}} \cdot \tfrac{\psi_y}{y} - f'(x)^p \cdot \psi_x + \kappa = 0$$

Die gesuchte Parametrisierung der hyperelliptischen Liftungen entspricht nun genau den Lösungen dieser Gleichung über $k[x]$, die wir im Folgenden *hyperelliptische charakteristische Gleichung* nennen.

Satz 4.2.1. *Seien die Bezeichnungen wie oben. Dann gibt es eine 1-zu-1 Korrespondenz zwischen den hyperelliptischen Liftungen von F_{n-1} auf A_n und den Lösungen (U_x, U_y) der linearen Gleichung*

$$2 \cdot f^{\frac{p+1}{2}} \cdot U_y - f'(x)^p \cdot U_x + \kappa = 0 \quad in \quad k[x]$$

Beweis:
Die Lösung (U_x, U_y) der hyperelliptischen charakteristischen Gleichung über $k[x]$ induziert eine Lösung (ψ_x, ψ_y) der charakteristischen Gleichung über A durch

$$\psi_x := U_x,\ \psi_y := y \cdot U_y$$

Die, auf diese Weise entstehenden Liftungen sind offensichtlich hyperelliptisch, da $F_n := \hat{F}_n + p^n * U_x$ ein x-Polynom ist.

Wir müssen noch zeigen, dass alle hyperelliptischen Liftungen durch die obige Zuordnung getroffen werden. Sei (ψ_x, ψ_y) eine Lösung der charakteristischen Gleichung die eine hyperelliptische Liftung induziert. Dann liegen ψ_x in $k[x]$ und ψ_y in $y \cdot k[x]$, also ist

$$\left(U_x := \psi_x\ , U_y := \tfrac{\psi_y}{y} \in k[x]\right)$$

eine Lösung der hyperelliptischen charakteristischen Gleichung. □.

Lösung der Basisgleichung:
Als nächstes zeigen wir, wie man eine hyperelliptische Liftung praktisch berechnen kann. Betrachte die hyperelliptische Basisgleichung der Liftungen des Frobenius auf der hyperelliptischen Kurve C, die analog zu der charakteristischen Gleichung über $k[x]$ definiert ist:

$$2 \cdot f^{\frac{p+1}{2}} \cdot \breve{\psi}_y - f'(x)^p \cdot \breve{\psi}_x + 1 = 0$$

Diese Gleichung ist immer lösbar in $k[x]$ wegen der Teilerfremdheit der x-Polynomen f und f'. Betrachte die Kongruenz:

$$-f'(x)^p \cdot \breve{\psi}_x + 1 \equiv \mod f^{\frac{p+1}{2}}$$

Eine Lösung $\breve{\psi}_x$ dieser Kongruenz erhält man durch einen Koeffizientenvergleich in $k[x]$ bis zum Grad $\frac{(2g+1)(p+1)}{2} = \deg_x(f^{\frac{p+1}{2}})$. Hat man eine solche Lösung $\breve{\psi}_x$ gefunden, so erhält man die gesuchte Lösung der Basisgleichung durch

$$\left(\breve{\psi}_x,\ \breve{\psi}_y := \tfrac{1 - f'(x)^p \cdot \breve{\psi}_x}{2 \cdot f^{\frac{p+1}{2}}}\right)$$

für die $\deg_x \breve{\psi}_x < \frac{(2g+1)(p+1)}{2}$ gilt.

Die Auflösung der Kongruenz kann man deutlich verbessern durch eine Zerlegung in $\frac{p+1}{2}$ sukzessive Schritte. In dem Schritt i berechnen wir dabei die Reduktion der Lösung $\breve{\psi}_x$ modulo f^i durch einen Koeffizientenvergleich bis zum Grad $2g+1$.

Parametrisierung der hyperelliptischen Liftungen:
Wir wählen nun eine hyperelliptische Liftung (A_n, F_n) von (A_{n-1}, F_{n-1}) als Basis der Parametrisierung und beschreiben den Parameterraum der kleinen Liftungen des Frobenius auf hyperelliptischen Kurven, sowie den Unterraum der hyperelliptischen Liftungen.

Satz 4.2.2. *Sei $(\breve{\psi}_x, \breve{\psi}_y) \in k[x]$ eine Lösung der hyperelliptischen Basisgleichung. Dann ist jede weitere Liftung $(\tilde{A}_n, \tilde{F}_n)$ parametrisiert durch ein Paar $(\alpha \in A, \mu \in A)_{F_n}$:*

$$\tilde{F}_n(x) = F_n(x) + p^n * \Delta_x(\alpha, \mu) = p^n * \left(2y^p \cdot \alpha + \mu^p \breve{\psi}_x\right)$$

$$\tilde{F}_n(y) = F_n(y) + p^n * \Delta_y(\alpha, \mu) = p^n * \left((f'(x))^p \cdot \alpha + \mu^p \, y \, \breve{\psi}_y\right)$$

Diese Liftung ist genau dann hyperelliptisch, wenn α in $y \cdot k[x]$ liegt.

Beweis: folgt aus der Parametrisierung der kleinen affinen Liftungen in 3.2, dem Satz 3.1.9 und der Definition der hyperelliptischen Liftungen. □.

In der obigen Parametrisierung entspricht μ der Differenz der definierenden Gleichungen von A_n und $\tilde{A}_n$, während α die Liftungen des Frobenius auf einer festgelegten Liftung der Kurve parametrisiert. So sind die kleinen Liftungen des Frobenius auf demselben Koordinatenring A_n durch die Parameterpaare $\{(\alpha, 0)\}$ gegeben.

Beispiel:
Die Durchführung des Liftungsalgorithmus aus 3.3 zeigen wir nun an einem Beispiel. Betrachte eine affine elliptische Kurve $E : y^2 = x^3 + x$ über einen Körper k in Charakteristik 5. Die Basisgleichung dieser Kurve ist gegeben durch:

$$2(x^3 + x)^3 \cdot \breve{\psi}_y - (3x^{10} + 1) \cdot \breve{\psi}_x + 1 = 0$$

Eine Lösung dieser Gleichung in $k[x]$ erhält man z.B. durch einen Koeffizientenvergleich bis zum Grad $\frac{(2g+1)(p+1)}{2} = 9$:

$$(\breve{\psi}_y = 2x^9 + x^7 + 3x,\ \breve{\psi}_x = 3x^8 + 3x^6 + x^4 + 1)$$

Wir wählen die triviale Liftung der definierenden Gleichung $y^2 - x^3 - x$ und die triviale quasi-Liftung $\hat{F}_1$ über R_1:

$$\hat{F}_1(x) = x^5 \qquad \hat{F}_1(y) = y^5$$

Das Hindernis $\kappa(\hat{F}_1)$ ist gleich $4x^{13} + 3x^{11} + 3x^9 + 4x^7$ wegen

$$\begin{aligned}\hat{F}_1(y^2 - f^\sigma) &= y^{10} - x^{15} - x^5 = (x^3 + x)^5 - x^{15} - x^5 \\ &= 5 \cdot (4x^{13} + 3x^{11} + 3x^9 + 4x^7) \in R_1[x]\end{aligned}$$

So erhält man eine hyperelliptische Liftung F_1 durch

$$\begin{aligned}F_1(x) &= x^5 + 5 \cdot \big((3x^8 + 3x^6 + x^4 + 1) \cdot (4x^{13} + 3x^{11} + 3x^9 + 4x^7)\big) \\ F_1(y) &= y^5 + 5 \cdot \big((2x^9 + x^7 + 3x) \cdot (4x^{13} + 3x^{11} + 3x^9 + 4x^7)\big)\end{aligned}$$

Die Parametrisierung der kleinen Liftungen von F_0 ist nun gegeben durch:

$$\Big\{\tilde{F}_1(x) := F_1(x) + 10y^5 \cdot \alpha,\ \ \tilde{F}_1(y) := F_1(y) + 5 \cdot (3x^{10} + 1) \cdot \alpha\Big\}$$

für ein beliebiges $\alpha \in A$, wobei die kleinen Liftungen genau dann hyperelliptische Liftungen sind, wenn α in $y \cdot k[x]$ liegt.

Die Grade der soeben berechneten Liftung F_1 sind viel höher als die Grade von F_0. Es existieren jedoch Liftungen, deren Grade nicht so hoch sind. Betrachte z.B. eine weitere Liftung $\tilde{F}_1$:

$$\tilde{F}_1(x) := x^5 + 5 \cdot (x^7 - x^3) \qquad \tilde{F}_1(y) := y^5 + 5y \cdot (x^8 + 2x^6 + x^2 + 3)$$

Diese Liftung liegt im Raum der kleinen Liftungen von F_0 und ist durch

$$\alpha = x^{12} + 3x^8 + 2x^6 + 2x^4 + x^2 + 3$$

parametrisiert. Die Möglichkeit den Grad der Liftung möglichst klein zu halten diskutieren wir im nächsten Abschnitt.

4.3 Minimale Liftungen

In den Beispielen aus den Abschnitten (4.2) und (3.3) haben wir gesehen, dass die berechneten Liftungen oft ziemlich hohe Grade haben und dass es in dieser Hinsicht viel „kleinere“ Liftungen gibt. Möchte man allerdings die p-adischen Liftungen über R_n durch die Zerlegung in kleine Liftungsschritte (wie in 3.3 beschrieben) bestimmen, so hängt die Komplexität der Berechnungen sehr stark von den Graden der gewählten Liftungen ab. Also kann

man den Algorithmus erheblich verbessern, indem man in jedem Liftungsschritt eine Liftung mit möglichst kleinen Graden wählt.

In diesem Abschnitt beschreiben wir eine solche kleine hyperelliptische Liftung F_n für die der Grad $\deg F_n(x)$ minimal unter allen kleinen Liftungen ist. Wir zeigen Existenz und Eindeutigkeit dieser Liftung und geben Schranken für die x-Grade von $F_n(x)$ und $F_n(y)$.

***x*-Minimale hyperelliptische Liftung:**
Wir konstruieren eine Liftung des Frobenius über R_n, indem wir in jedem Liftungsschritt die induzierende Derivation ψ mit möglichst kleinen x-Grad von $\psi(x)$ wählen:

Lemma 4.3.1. *Sei $\hat{F}_n$ eine quasi-Liftung von F_{n-1}. Dann existiert ein eindeutiges $\psi_x \in k[x]$ mit*

$$\deg_x(\psi_x) < deg_x(f^{\frac{p+1}{2}}) = \tfrac{(2g+1)(p+1)}{2},$$

so daß es eine kleine Liftung F_n von F_{n-1} existiert, für die

$$F_n(x) = \hat{F}_n(x) + p^n * \psi_x \quad \textit{gilt.}$$

Beweis:
Betrachte die charakteristische Gleichung der hyperelliptischen Liftungen von F_{n-1}:

$$2f^{\frac{p+1}{2}} \cdot \psi_y - (f')^p \cdot \psi_x + \kappa(F_{n-1}) = 0$$

Für jede Lösung (ψ_x, ψ_y) dieser Gleichung ist ψ_x eine Lösung der folgenden Kongruenz:

$$(f')^p \cdot \psi_x \equiv \kappa(F_{n-1}) \mod 2f^{\frac{p+1}{2}}$$

Die Aussage des Lemmas ist äquivalent dazu, dass diese Kongruenz eine eindeutige Lösung ψ_x mit $\deg_x(\psi_x) < \frac{(2g+1)(p+1)}{2}$ besitzt.

Nach der Voraussetzung wissen wir, daß f keine mehrfache Nullstellen hat. Foglich sind die Polynome f und f' teilerfremd. Da $k[x]$ ein euklidisches Ring ist, folgt die Aussage des Lemmas aus der Teilerfremdheit von $f^{\frac{p+1}{2}}$ und $(f')^p$. $\square$.

Korollar 4.3.2. *Es existiert eine eindeutige Liftung F_n des Frobeniushomomorphismus F, für die*

$$\deg_x F_n(x) < \tfrac{(2g+1)(p+1)}{2} \quad \textit{gilt.}$$

Beweis:
Nach dem Lemma 4.3.1 kann man F über R_n so liften, dass in jedem Liftungsschritt i stets eine parametrisierende Derivation ψ_i mit der folgenden Eigenschaft gewählt wird:

$$\deg_x \psi_i(x) < \tfrac{(2g+1)(p+1)}{2} \text{ ist.}$$

Die resultierende Liftung F_n erfüllt die gewünschte Bedingung wegen:

$$\deg F_n(x) = \deg_x \left[\sum_i^n p^n * \psi_i(x) \right] = \max\{\deg_x \psi_i(x)\} \leq \tfrac{(2g+1)(p+1)}{2}$$

Diese Liftung ist unter der Einhaltung dieser Schranke eindeutig wegen der Eindeutigkeit von ψ_i. $\square$.

Definition 4.3.3. *Die eindeutige Liftung F_n aus dem Korollar 4.3.2 nennen wir im Folgenden* ***die x-minimale hyperelliptische Liftung*** *von F auf A_n.*

Berechnung der x-minimalen Liftung:
Die Berechnung der x-minimalen hyperelliptischen Liftung erfolgt durch eine leichte Modifikation des Algorithmus aus (3.3). In jedem Liftungsschritt lösen wir die charakteristische Gleichung wie im ursprünglichen Algorithmus und deformieren diese Lösung entlang des Parameterraumes so, dass sie x-minimal wird.

Sind $\breve{\psi}_x$ und $\breve{\psi}_y$ die Lösungen der Basisgleichung und κ das Hindernis, so erhält man den Parameter α für die x-minimale Lösung durch:

$$\alpha := \kappa \cdot \breve{\psi}_x \ div \ f^{\frac{p+1}{2}}$$

Einen Beispiel für die x-minimale Liftung, sowie den zugehörigen Parameter α haben wir bereits im Beispiel aus dem vorigen Abschnitt angegeben.

Die entsprechende Lösung (ψ_x, ψ_y) der charakteristischen Gleichung ist nun gegeben durch:

$$\psi_x = \kappa \cdot \breve{\psi}_x + \alpha \cdot f^{\frac{p+1}{2}} = \kappa \cdot \psi_x \mod f^{\frac{p+1}{2}}$$
$$\psi_y = \kappa \cdot y \cdot \breve{\psi}_y + \alpha \cdot y \cdot (f')^p$$

Minimalität der Liftungen:
Die Wahl den x-Grad von $F_n(x)$ zu minimieren war durch die Beschleunigung der Berechnung der Hindernisse motiviert. Bei der Berechnung des Terms $\kappa := F_n(y)^2 - f_n(F_n(x))$ fällt $F_n(x)$ mehr ins Gewicht, also erscheint

es für die Laufzeit vorteilhafter den $\deg_x F_n(x)$ zu minimieren. Mit derselben Methode können wir allerdings auch den Grad von $F_n(y)$ minimal halten, so dass $\deg_x F_n(y) < \deg(f')^p = 2gp$ gilt. Es ist auch möglich eine gewisse Balance zwischen den Graden von $F_n(x)$ und $F_n(y)$ zu halten, so dass man eine geeignete Minimalitätsfunktion in Abhängigkeit von F_n optimiert.

Im allgemeinen hilft die Parametrisierung der Liftungen die für konkrete Anwendungen geeigneten Liftungen zu finden. So diskutieren wir im Abschnitt 6.4 die Wahl solcher Liftungen, für die die Reduktion der Differentiale bei der Berechnung der induzierten Operation des Frobenius möglichst einfach wird.

Auf einigen Kurven können auch Liftungen existieren, bei denen sowohl $\deg F_n(x)$ als auch $\deg F_n(y)$ nicht mehr von n abhängen. Ein Beispiel dafür ist gegeben durch die affine Einschränkung einer projektiven Liftung nach Charakteristik 0, bzw. von deren Reduktionen modulo p. Diesen Fall diskutieren wir im Kapiteln 5 und 6 für die kanonische Liftung elliptischer Kurven.

Größe der x-minimalen Liftung:
Die hyperelliptische minimale Liftung wurde so konstruiert, so dass $\deg_x F_n(x)$ minimal wird, $\deg_x F_n(y)$ wächst jedoch zusammen mit n und ist für steigendes n unbeschränkt. Dieses Wachstum ist allerdings linear mit einer kleinen Konstante:

Satz 4.3.4. *Sei F_n eine hyperelliptische minimale Liftung des Frobenius über R_n, dann gilt*

$$\deg F_n(y) < 2pg + (n-1)\tfrac{(2g-1)(p+1)}{2} = \tfrac{p+1}{2} - g + n\tfrac{(2g-1)(p+1)}{2}$$

Beweis:
den Beweis führen wir induktiv, mit $n = 0$ als Induktionsbasis, wobei der Induktionschritt $n-1 \to n$ im Lemma 4.3.7. am Ende des Abschnittes bewiesen wird. □.

Die Vorbereitung für das Lemma 4.3.7 beginnen wir mit einem Hilfssatz, der die Abhängigkeit des Grades des $F_n(y)$ von dem Grad des Hindernisses $\kappa(\hat{F}_n)$ zeigt:

Lemma 4.3.5. *Sei F_{n-1} die x-minimale Liftung von Frobenius über R_{n-1}, κ das Hindernis zur trivialen Liftung von F_{n-1}. Weiterhin sei F_n die x-minimale Liftung von Frobenius über R_n, die von F_{n-1} durch die Derivation ψ_n induziert ist. Dann gilt*

$$\deg \psi_n(y) \leq \max\left\{2pg-1,\ \deg\kappa - \tfrac{(2g+1)(p+1)}{2}\right\}$$

Beweis:
Die Bilder $\psi_n(x)$ und $\psi_n(y)$ liefern eine Lösung der charakteristischen Gleichung von F_{n-1}. Ein Auflösung dieser Gleichung nach $\psi_n(y)$ liefert:

$$\psi_n(y) = (f'(x)^p\ \psi_n(x) - \kappa)\ /(2f^{\frac{p+1}{2}})\ \text{ in } k[x]$$

Also ist Grad von $\psi_n(y)$ beschränkt durch

$$\begin{aligned}\deg \psi_n(y) &\leq \max\{\deg f'(x)^p\ \psi_n(x),\ \deg \kappa\} - \deg(2 \cdot f^{\frac{p+1}{2}}) \\ &\leq \max\{2pg + \tfrac{(2g+1)(p+1)}{2} - 1,\ \deg \kappa\} - \tfrac{(2g+1)(p+1)}{2}\end{aligned}$$

da $\deg \psi_n(x) < \frac{(2g+1)(p+1)}{2}$ nach der Konstruktion gilt. $\square$.

Wir betrachten nun den Grad des Hindernisses κ:

Lemma 4.3.6. *Sei $F_{n-1} = F_0 + \sum p^i * \psi_i$ die p-adische Darstellung der Liftung F_{n-1}. Angenommen jede Derivation ψ_i erfüllt die Ungleichung*

$$\deg \psi_i(y) \leq 2pg - 1 + (i-1)\tfrac{(2g-1)(p+1)}{2}$$

dann gilt:

$$\deg \kappa(F_{n-1}) \leq (2g+1) + (4pg-2) + (n-1)\tfrac{(2g-1)(p+1)}{2}$$

Beweis:
Wir zerlegen den Beweis in 2 Teile in denen wir die angegebene κ Schranke für $\deg_x \hat{F}_n(y)$ und für $\deg_x F_n(f_n^\sigma)$ zeigen. Damit werden wir die Aussage des Lemmas aus der Definition des Hindernisses schließen.

1) Betrachte den Term $\frac{\hat{F_n}(y)}{y} = \sum p^i * \frac{\psi_i(y)}{y} \in R_n[x]$. Nach dem Lemma A.4 gilt:

$$\deg_x(F_n(y)/y)^2 \leq 2pg - 1 + 2pg - 1 + (n-2)\tfrac{(2g-1)(p+1)}{2}$$

wegen der vorausgesetzten Schranken von $\deg_x \psi_i(y)$.

Die gewünschte Schranke für $\hat{F_n}(y)^2 = f_n(x) \cdot (F_n(y)/y)^2$ erhalten wir aus der obigen Schranke für $\deg_x(F_n(y)/y)^2$ durch Addition von $\deg f = 2g+1$. $\square$.

2) Der Term $\deg_x F_n(f_n^\sigma)$ ist offensichtlich beschränkt durch

$$\deg F_n(x) \cdot \deg(f_n^\sigma) \leq \left(\tfrac{(2g+1)(p+1)}{2} - 1\right)(2g+1)$$

da $\deg F_n(x) < \frac{(2g+1)(p+1)}{2}$ und $\deg f_n(x) < 2g+1$ gilt. Deswegen ist die Schranke für $n \geq 2g+1$ erfüllt wegen:

$$
\begin{aligned}
2g+1+4pg-2+(n-1)\tfrac{(2g-1)(p+1)}{2} &\geq 2g+4pg-1+\tfrac{(2g-1)^2(p+1)}{2} \\
&= 2g+4pg-1+\tfrac{p+1}{2}\left((2g+1)^2-8g\right) \\
&= -2g-1+\tfrac{(2g+1)^2(p+1)}{2} \\
&= (2g+1)\left(\tfrac{(2g+1)(p+1)}{2}-1\right)
\end{aligned}
$$

Weiterhin für $n < 2g+1$ liefert das Lemma A.4 folgende Schranke:

$$\deg_x F_n(f_n^\sigma) \leq \left(\tfrac{(2g+1)(p+1)}{2}-1\right)\cdot n\ ,$$

da wir höchstens n Terme der p-adischen Darstellung von $F_n(x)$ multiplizieren können, ohne das Produkt modulo p^n verschwindet. Damit folgt die Behauptung wegen :

$$
\begin{aligned}
&2g+1+4pg-2+(n-1)\tfrac{(2g-1)(p+1)}{2} > \\
&g+3pg-1+n\tfrac{(2g-1)(p+1)}{2} = g+3pg-1-n(p+1)+n\tfrac{(2g+1)(p+1)}{2} \geq \\
&g+3pg-1-2g(p+1)+n\tfrac{(2g+1)(p+1)}{2} \geq n\tfrac{(2g+1)(p+1)}{2}
\end{aligned}
$$

□.

Mit diesem Lemma können wir die Schranke für den Grad von $\psi_n(y)$ und damit auch für $F_n(y)$ beweisen:

Lemma 4.3.7. *Sei $F_{n-1} = F_0 + \sum p^i * \psi_i$ die p-adische Darstellung der x-minimalen Liftung F_{n-1}. Weiterhin sei ψ_n eine Derivation, die x-minimale Liftung F_n über R_n induziert. Angenommen für jedes $i < n$ erfüllt jede Derivation ψ_i die Ungleichung*

$$\deg_x \psi_i(y) < 2pg + (i-1)\tfrac{(2g-1)(p+1)}{2}$$

dann gilt:

$$\deg_x \psi_n(y) \leq (2pg-1) + (n-2)\tfrac{(2g-1)(p+1)}{2}$$

Beweis:
Nach dem Lemma (4.3.5) erhalten wir eine Schranke für $\deg_x \psi_n(y)$ durch:

$$\deg \psi_n(y) < \deg \kappa - \tfrac{(2g-1)(p+1)}{2}$$

Nach dem Lemma (4.3.6) kennen wir eine Schranke für $\deg_x \kappa$:

$$\deg \kappa < (2g+1) + (4pg-2) + (n-2)\cdot(2g-1)\cdot\tfrac{p+1}{2}.$$

Also reicht es folgende Ungleichung zu zeigen:

$$(2g+1) + (4pg-2) + (n-2)\tfrac{(2g-1)(p+1)}{2} - \tfrac{(2g+1)(p+1)}{2} \leq$$
$$2pg - 1 + (n-1)\tfrac{(2g-1)(p+1)}{2}$$

Durch das Umformen erhalten wir eine äquivalente Ungleichung :

$$2g + 1 + 2pg - 1 \leq \tfrac{(2g-1)(p+1)}{2} + \tfrac{(2g+1)(p+1)}{2} \Leftrightarrow$$
$$2g + 2pg \leq 2g(p+1)$$

die Trivialerweise erfüllt ist. Damit haben wir gezeigt, dass Grad von $\psi_n(y)$ die angegebene Schranke nicht überschreitet. □.

4.4 Liftungen auf den "Kedlaya" Kurven

In diesem Abschnitt betrachten wir die Liftungen des Frobenius auf den affinen (hyperelliptischen) Kurven, die Kedlaya in seinem Algorithmus verwendet. Wir betrachten die, in diesem Algorithmus berechnete Liftung im Rahmen der Parametrisierung der kleinen Liftungen, beweisen dadurch die Schranken für die Größe dieser Liftung und vergleichen sie mit denen der Einschränkung der x-minimalen Liftung auf den lokalisierten Koordinatenring.

Sei $A = k[x,y]/(y^2 - f(x))$ der Koordinatenring einer affinen hyperelliptischen Kurve. Wir betrachten die Lokalisierung von A nach y und bezeichnen diesen Ring mit $A_{(y)} = k[x,y,y^{-1}]/(y^2 - f(x))$. Der Ring $A_{(y)}$ ist der Koordinatenring der affinen Kurve C_y, die man aus der projektiven hyperelliptischen Kurve durch den Schnitt mit der affinen Ebene $\{(y \neq 0)\}$ erhält. Die Kurven C_y bezeichnen wir als *Kedlaya Kurven.*

Elemente dieser Koordinatenringe betrachten wir in der normalisierten Form, bei der x eliminiert wird, so dass der x-Grad aller Elemente von $A_{(y),n}$ stets kleiner als $2g+1$ ist. Beachte, dass in dieser Normalform der y^{-1}-Grad stets minimal unter allen möglichen Darstellungen der Elemente des Quotientenringes ist.

Parametrisierung des Liftungsraumes auf Kedlaya-Kurven:
Wir wissen bereits, dass es mehr "Raum" und dadurch mehr Liftungen des Frobenius auf den lokalisierten Kurven gibt. Bei der Liftung des Frobenius auf affinen Kurven mit einer definierenden Gleichung müssen wir die Bilder $F(x)$ und $F(y)$ stets gleichzeitig liften, damit die Verträglichkeit mit der definierenden Gleichung erhalten bleibt. Bei den lokalisierten hyperellipti-

schen Kurven kann man das Liften der Bilder der Variablen aufspalten. In dem folgenden Satz zeigen wir, dass man das Bild $F_n(x)$ frei wählen und anschließend $F(y)$ liften kann:

Satz 4.4.1. *Sei F_{n-1} eine Liftung von F über R_n und $\gamma = \hat{F}_n(x) + p^n * \gamma_n \in B_n$ eine beliebige Liftung des Polynoms $F_{n-1}(x)$. Dann existiert genau eine Liftung F_n von F_{n-1} für die $F_n(x) = \gamma$ gilt.*

Beweis:
Die Liftungen von F_{n-1} über F_n entsprechen den Lösungen des Gleichungssystems:

$$f'(x)^p \cdot \psi_x + 2y^p \cdot \psi_y = \kappa_x := \frac{\hat{F}_n(y^2 - f_n)}{p^n}$$

$$y^p \cdot \psi_y + y^{-p} \cdot \psi_{y^{-1}} = \kappa_y := \frac{\hat{F}_n(y \cdot y^{-1} - 1)}{p^n}$$

dabei entsprechen diejenigen mit der zusätzlichen Eigenschaft $F_n(x) = \gamma$ genau solchen Lösungen, für die $\psi_x = \gamma_n$ gilt. In diesem Fall hat die erste Gleichung stets eine eindeutige Lösung:

$$\psi_y := \tfrac{1}{2} y^{-p} \cdot (f'(x)^p \cdot \gamma_n + \kappa_x)$$

Nach dem Lemma 3.5.1 existiert genau ein $\psi_{y^{-1}}$, so dass die zweite Gleichung für die gegebene ψ_y erfüllt ist. Damit ist der Satz bewiesen. □.

Aus diesem Satz folgt insbesondere die Existenz und Eindeutigkeit der Liftungen des Frobenius die im Kedlaya Algorithmus verwendet wird und durch $\gamma_i = 0$ für alle $i > 0$ definiert ist:

Korollar 4.4.2. *Seien die Bezeichnungen wie oben. Dann existiert genau eine Liftung des Frobenius F_n^B auf B_n, für die $F_n(x) = x^p$ gilt.*

Größe der Kedlaya Liftungen:
Bei der Liftung aus dem Kedlaya-Algorithmus ist der Grad von $F_n(x)$ minimal, dafür der y^{-1}-Grad von $F_n(y^{-1})$ ziemlich groß. Die in der Originalarbeit angegebene Schranke für $\deg_{y^{-1}} F_n(y^{-1})$ zeigen wir mit den entwickleten deformationstheoretischen Methoden. Zunächst beweisen wir einen zu 4.3.5 ähnlichen Hilfsatz:

Lemma 4.4.3. *Seien die wie oben und $F_n := (F_{n-1})_n + p^n * \psi_n$ eine kleine Liftung des Frobenius auf $A_{(y),n}$ für die $F_n(x) = x^p$ gilt, dann gilt:*

Bezeichnungen $\deg_{y^{-1}} \psi_n(y^{-1}) \leq \max\{\deg_{y^{-1}}(\kappa) + p,\ 2p + \deg_{y^{-1}}(\psi_y)\}$

Beweis:
Die Behauptung des Lemmas folgt unmittelbar aus der Auflösung der zweiten charakteristischen Gleichung nach y^{-1}:

$$\psi_n(y^{-1}) = -y^{-p} \cdot \kappa - y^{-2p} \cdot \psi_n(y)$$

□.

Satz 4.4.4. *Sei F_n die Kedlaya Liftung auf $A_{(y),n}$. Dann gilt*

$$\deg_{y^{-1}} F_n^B(y) < (2n-1)p$$

$$\deg_{y^{-1}} F_n^B(y^{-1}) < (2n+1)p$$

Beweis:
Den Beweis führen induktiv mit der Basis $n = 0$. Betrachte der Induktionsschritt $n-1 \mapsto n$. Wegen der Definition der Hindernisse und den vorausgesetzten Schranken folgern wir aus dem Lemma A.4:

$$\deg_{y^{-1}} \kappa_y = \max\{(2i+1)p + (2(n-1-i)+1)p\}_{i<n} = 2np$$

$$\deg_{y^{-1}} \kappa_x = \max\{(2i-1)p + (2(n-1-i)+1)p\}_{i<n} = 2(n-1)p$$

Da $\psi_n(x) = 0$ nach Konstruktion der Liftung gilt, erhalten wir

$$\deg_{y^{-1}} \psi_n(y) = \deg_{y^{-1}} \kappa_x + p = (2n-1)p$$

aus der Betrachtung y^{-1}-Grades in der ersten charakteristischen Gleichung. Die zweite Behauptung des Satzes folgt nach dem Lemma 4.4.3 wegen:

$$\deg_{y^{-1}} \psi_n(y^{-1}) \leq \max\{2np + p, (2n-1)p + 2p)\} = (2n+1)p$$

□.

Beachte, dass diese Schranke in meisten Fällen genau erreicht wird.

Einschränkung der x-minimalen Liftung:
Als nächstes betrachten wir die in (4.3) definierte x-minimale Liftung und deren Einschränkung auf den lokalisierten Koordinatenring.

Satz 4.4.5. *Seien F_n die x-minimale Liftung auf der Kurve C und F_n^t die Einschränkung auf C_y. Dann gilt*

$$\deg_{y^{-1}} F_n^t(y^{-1}) < pn$$

Beweis:
Den Beweis führen induktiv mit der Basis $n = 0$. Betrachte der Induktionsschritt $n-1 \mapsto n$. Die y^{-1}-Grade von $F_n(y)$ und $F_n(x)$ verschwinden nach Konstruktion der Liftung, also gilt:

$$\deg_{y^{-1}} \kappa_x = 0$$

Aus dem Lemma A.4 und der Definition des Hindernisses folgt

$$\deg_{y^{-1}} \kappa_y = \max\{ip + (n-1-i)p\}_{i<n} = np - p$$

Die Behauptung des Satzes folgt nun aus dem Lemma 4.4.3 wegen:

$$\deg_{y^{-1}} \psi_n(y^{-1}) = \max\{np - p + p,\, 2p\} = np$$

□

Damit haben wir eine kleine Liftung, bei der y^{-1}-Grad von $F_n^t(y^{-1})$ doppelt so klein ist wie bei der Kedlaya Liftung. Der Gesamtgrad dieser Liftung ist allerdings nur ein wenig kleiner als bei Kedlaya:

Lemma 4.4.6. *Sei F_n^t die x-minimale Liftung des Frobenius, dann gilt*

$$\deg_y F_n^t(y^{-1}) + \deg_{y^{-1}} F_n^t(y^{-1}) < n\left(p + (p+1)\tfrac{2g-1}{2g+1}\right)$$

Beweis:
Die in (4.3.4) angegebene Schranken für den x-Grad liefern:

$$\deg_y F_n(y) \leq (2pg - 1 + (n-1)\tfrac{(2g-1)(p+1)}{2}) \cdot \tfrac{2}{2g+1} \leq n \cdot (p+1)\tfrac{2g-1}{2g+1}$$

Die Aussage des Lemmas folgt damit aus dem Satz 4.4.5. □.

4.5 Anwendung das Punktezählproblem

In diesem Abschnitt beschreiben wir die Anwendung der x-minimalen Liftung auf das Punktezählproblem auf hyperelliptischen Kurven. Wir zeigen, dass die Anwendung dieser Liftung eine schnelle Berechnung der induzierten Operation des Frobenius auf der MW-Kohomologie ermöglicht und eine deutliche Komplexitätsverbesserung gegenüber dem Originalalgorithmus von Kedlaya bringt.

Anschließend diskutieren wir die geschätzte Komplexität und erzielten Laufzeiten des implementierten Liftungsalgorithmus, sowie die Auswirkungen auf das gesamte Punktezählalgorithmus.

MW-Kohomologie auf affinen hyperelliptischen Kurven:
Die Wahl der affinen Kurven beim Kedlaya Algorithmus (die durch das Wegnahme der Weierstrasspunkte aus der projektiven hyperelliptischen Kurve entstehen) war ausschließlich durch den verwendeten Liftungsalgorithmus motiviert. Die Idee des Punktezählens durch die Betrachtung der Monsky-Washnitzer Kohomologie kann für beliebige glatte affine Varietäten eingesetzt werden.

Die Dimension der Monsky-Washnitzer Kohomologie eine glatten affinen Kurve C_A vom Geschlecht g ist gleich $2g + m - 1$, wobei m die Anzahl der zum projektiven Abschluss von C_A notwendigen Punkte. Die in diesem Kapitel betrachteten affinen hyperelliptischen Kurven vom Geschlecht g entstehen aus der projektiven Kurve durch das Wegnahme des unendlich fernen Punktes und folglich ist die MW-Kohomologie einer solchen Kurve $2g$-dimensional, wobei eine Basis durch folgende Differentiale gegeben ist:

$$\{y \cdot x^i dx\}_{0 \leq i \leq 2g-1}$$

Die induzierte Operation des Frobenius darauf ist gegeben durch

$$F_n^*(y \cdot x^i dx) = F_n(y)F_n(x)^i \cdot DF_n(x)dx$$

wobei $DF_n(x) := \frac{\partial \tilde{F}(x)}{\partial x}dx + \frac{\partial \tilde{F}(x)}{\partial y}dy$ den totalen Differential von F_n bezeichnet. Um die Matrix dieser Operation zu berechnen, müssen diese Differentiale modulo den exakten Differentialen reduziert werden.

Für alle geschlossenen Differentiale betrachten wir eine eindeutige Darstellung als y-Potenzreihe, die man durch die Anwendung der definierenden Gleichung erhält:

$$h(x,y)dx = \left(\sum_{i=1}^{n} h_i(x) \cdot y^i \right) dx \text{ , wobei } \; deg_x(h_i) < 2g + 1 \; \text{ gilt.}$$

Wie im Kedlaya Algorithmus kann man die Relation $2y\,dy = f'(x)dx$ ausnutzen um den y-Grad von h schrittweise zu reduzieren, wobei dieser Grad in jedem Schritt um 2 verringert wird (s. [Gerk], Kap. 5). Daraus folgt, dass die Anzahl der notwendigen Reduktionsschritten gleich $n/2$, wobei n der y-Grad von g ist.

Anwendung der x-minimalen Liftung:
Betrachte nun die x-minimale hyperelliptische Liftung. In diesem Fall ist $F_n(x)$ ein x-Polynom, und es gilt

$$DF_n(x) = F_n'(x)dx \;\; \text{für die Ableitung } F_n'(x) \text{ von } F_n(x) \in R_n[x]$$

Die, aus der Konstruktion der Liftung und dem Satz 3.3.4 folgenden, Schranken für den x Grad von $F_n(y)$ und $F_n(x)$ führen zu der folgenden Schranke für den x-Grad des Polynoms $F_n(y)F_n(x)^i F_n'(x)$:

$$\deg_x(F_n(y)F_n(x)^i F_n'(x)) < \tfrac{(2g+1)(p+1)(i+1)}{2} + 2pg + (n-1)\tfrac{(2g-1)(p+1)}{2}$$

Diese Schranke für den x-Grad liefert folgende Schranke für den y-Grad:

$$\deg_y(F_n(y)F_n(x)^iF_n'(x)) < (i+1)(p+1) + \tfrac{4pg}{2g+1} + (n-1)\tfrac{(2g-1)(p+1)}{2g+1}$$
$$< (2g+3)(p+1) + (n-1)\tfrac{(2g-1)(p+1)}{(2g+1)}$$

Folglich ist die Anzahl der notwendigen Reduktionsschritte linear in n mit der Konstante $\frac{(2g-1)(p+1)}{2(2g+1)}$.

Zum Vergleich beachte, dass beim Kedlaya Algorithmus diese Konstante gleich p (s. 4.5.4) und damit mehr als doppelt so hoch ist. Da die bewiesene Zeitkomplexität des Reduktionsschrittes im Originalalgorithmus $\mathbb{O}(n^{3+\epsilon})$ beträgt, erhält man eine Beschleunigung um Faktor > 8, und insbesondere um Faktor $> 17{,}5$ für Geschlecht 2.

Laufzeitdiskussion
Wir haben gesehen, dass die x-minimale Liftung des Frobenius eine deutlich schnellere Berechnung der induzierten Operation ermöglicht. Es bleibt allerdings die Frage, wie schnell die Berechnung dieser Liftungen ist und wie sich die Laufzeiten des gesamten Punktezählalgorithmus ändern.

In dem Schritt n des Liftungsalgorithmus wird eine Auswertung der berechneten Liftung des F_{n-1} in $\mathbb{Z}_q/p^n\,[x]$ für die Berechnung des Hindernisses und die modulare Reduktion der Polynome in $k[x]$ für die Lösung der charakteristischen Gleichung durchgeführt.

Wir vermuten, dass die Durchführung dieses Schrittes die Zeitkomplexität $\mathbb{O}(n^{2+\epsilon}g^{3+\epsilon})$ hat, wobei n die gewünschte p-adische Genauigkeit n und g das Geschlecht der Kurve bezeichnen. Folglich hätte Liftungsalgorithmus dieselbe Zeitkomplexität $\mathbb{O}(n^{3+\epsilon}g^{3+\epsilon})$ wie bei Kedlaya.

Setzen nun voraus, dass die Laufzeit der beiden Liftungsalgorithmen gleich L ist und die Laufzeit des Reduktionsschrittes bei Kedlaya (entsprechend den Komplexitätsabschätzungen) $g \cdot L$ beträgt. In diesem Fall würde die Beschleunigung des Reduktionschrittes um Faktor λ, eine Beschleunigung des gesamten Algorithmus um den Faktor

$$\tfrac{L+g\cdot L}{L+g\cdot L/\lambda} = \tfrac{\lambda\cdot g+\lambda}{\lambda+g} > \min\{g,\lambda\}$$

nach sich ziehen, wobei wir folgendes λ wegen der oben gegebenen Abschätzung der y-Gesamtgrade:

$$\lambda \approx (2\tfrac{2g+1}{2g-1})^3 \text{ vermuten.}$$

Damit hätte man eine Beschleunigung um Faktor g für Kurven mit kleineren Geschlechtern und Beschleunigung um Faktor > 8 für Kurven mit $g \geq 9$.

Empirische Komplexitätsanalyse
Die aufgestellte Vermutung haben wir durch viele Beispiele bestätigt, einige davon in den unten aufgeführten Tabellen zusammengefasst sind. Der Algorithmus wurde in MAGMA 2.11 implementiert (nicht optimiert) und auf einem Windows-XP Rechner mit dem Intel Core 2 Prozessor (1,66 / 0,89 GHz) ausgeführt.

Wir haben die Berechnung der Liftung für affine hyperelliptische Kurven vom Geschlecht g über den Körper $\mathbb{F}_5^{50}$ mit unterschiedlicher p-adischen Genauigkeit n durchgeführt und folgende Laufzeiten (in Sekunden) erhalten:

n	6	12	18	24
$g = 1$	0,4	2,1	6,0	11,1
$g = 2$	1,9	10,6	29,3	53,8
$g = 3$	6,1	33,8	88,3	154,6

An diesen Zahlen (sowie an vielen weiteren Beispielen) sieht man, dass die in der Praxis auftretenden Abhängigkeiten der Laufzeit von g und n deutlich unter den n^3, bzw. g^3 liegen.

Als nächstes beschreiben wir die Abhängigkeit der Laufzeiten von p. Dabei haben wir den Frobeniushomorhismus mit einer (für das Punktezählen) ausreichenden p-adischen Genauigkeit für unterschiedliche Grundkörper $\mathbb{F}_p^d$ geliftet, wobei wir eine vergleichbare (für kryptographische Anwendungen geeignete) Größe dieser Körper $\mathbb{F}_p^d$ gesetzt haben.

Die folgenden Laufzeiten haben wir für die Kurve $C : y^2 = x^5 + 2x^2 + t$ erhalten:

p	3	5	7	11	13	17	29	37	59
$[\mathbb{F}_p : \mathbb{F}_q]$	50	34	28	23	21	19	16	15	13
n	27	19	16	13	12	11	9	8	7
Laufzeit	35,8	33,1	38,6	60,5	64,3	89,3	149,1	205,0	341,2

Diese Ergebnisse lassen vermuten, dass die Berechnungslaufzeit (ab einem gewissen p) linear in p ist.

Kapitel 5

Projektive Liftungen des Frobenius auf elliptischen Kurven

Dieses Kapitel beschreibt die Anwendung der in den Kapiteln 3 und 4 hergeleiteten Parametrisierung aller affinen Liftungen des Frobeniusmorphismus für die Berechnung der projektiven Liftungen. Die Idee besteht darin, den Frobeniusmorphismus auf affinen Karten beliebig zu liften, die Hindernisse zur Verklebung auf den Durchschnitten zu bestimmen und anschließend die affinen Liftungen entlang der Parameterräumen so zu deformieren, dass diese Hindernisse verschwinden.

Im affinen Fall existiert eine Liftung des Frobeniusmorphismus auf jeder beliebigen Liftung einer glatten Kurve, im projektiven Fall treten gewisse Obstruktionen zur Liftbarkeit auf (s. 2.2.1), so dass es im Allgemeinen überhaupt keine Liftung des projektiven Frobeniusmorphismus gibt. Deswegen konzentrieren wir uns auf den Fall der ordinären elliptischen Kurven, in dem eine kanonische Liftung des Frobeniusmorphismus stets existiert. Die möglichen Verallgemeinerungen diskutieren wir im Abschnitt 6.4.

5.1 Liftungen elliptischer Kurven, kanonische Liftung

Nach einer kurzen Einführung der elliptischen Kurven und deren kanonischen Liftung, betrachten wir (projektive) elliptische Kurven als affine Über-

deckung durch zwei affine hyperelliptische Kurven und betrachten Liftungen des Frobeniusmorphismus darauf.

Definition 5.1.1. *Unter einer **elliptischen Kurve** über dem Körper k verstehen wir eine glatte Kurve E von Geschlecht 1 zusammen mit einem ausgezeichneten k-rationalen Punkt $O \in E(k)$.*

Für eine ausfühliche Einführung in die elliptische Kurven siehe [Silv1] und [Silv2].

Im Folgenden konzentrieren wir uns auf ungerade Charakteristik ($p > 2$). In diesem Fall ist eine elliptische Kurve affin gegeben durch die Gleichung $E_A : y^2 = x^3 + ax + b$, wobei die entsprechende affine Kurve durch das Wegnahme des unendlich fernen Punkt entsteht. Die Isomorphieklassen der elliptischen Kurven über den Körper k sind beschrieben durch die j-Invariante der Kurve und einem quadratischen Twist.

Kanonische Liftung:
Das folgende Theorem sichert die Existenz der projektiven Liftungen des Frobenius auf elliptischen Kurven unter einer zusätzlichen Bedingung:

Theorem 5.1.2. *Sei E eine ordinäre elliptische Kurve, dann existiert eine (bis auf Isomorphie) eindeutige Liftung $\tilde{F} : \tilde{E}^\sigma \to \tilde{E}$ des Frobeniusmorphismus $F : E^\sigma \to E$ nach Charakteristik 0.*

Beweis: s. [LST]

Insbesondere existiert eine Liftung $F_n : E_n^\sigma \to E_n$ über R_n, gegeben durch die Reduktion des Paares $(\tilde{E}, \tilde{F})$ modulo p^n.

Die Bedingung der Ordinarität ist dabei leicht überprüfbar:

Definition 5.1.3. *Eine elliptische Kurve ist genau dann **ordinär**, wenn deren Hasse-Invariante nicht verschwindet. Die **Hasse-Invariante** einer elliptischen Kurve $E : y^2 = f(x)$ ist dabei definiert als der Koeffizient von x^{p-1} in $f^{\frac{p-1}{2}}$, den wir im folgenden mit $C_{x^{p-1}}(f^{\frac{p-1}{2}})$ bezeichnen.*

Die Isomorphieklassen der elliptischen Kurve $\tilde{E}$ sind eindeutig bestimmt durch die j-Invariante von E. Daraus folgt insbesondere, dass die kanonische Liftung $\tilde{E}$ allein durch die Wahl der Liftung $\tilde{b}$ des Koeffizienten b eindeutig bestimmt ist.

Auch die Kurven E_n, die durch Reduktionen $\tilde{E}$ modulo p^n entstehen sind

eindeutig bestimmt durch die Reduktion von $\tilde{b}$. Deswegen liften wir den Koeffizient a stets trivial und betrachten die Liftungen der definierenden Gleichung die durch $y^2 = x^3 + ax + b_n$ für ein $b_n \in R_n$ ($a \in k$) gegeben sind.

Affine Überdeckung:
Die elliptische Kurve E über den Körper k, sowie deren Liftungen über den p-adischen Ringen R_n betrachten wir im Folgenden als Vereinigung von zwei folgenden affinen (hyper)elliptischen Kurven:

$$C_A : \{(x,y)|y^2 = f_n(x) := x^3 + ax + b_n\} \subset \mathbb{A}^2_{R_n}$$
$$C_B : \{(s,t)|s^2 = h_n(t) := b_n t^4 + at^3 + t\} \subset \mathbb{A}^2_{R_n}$$

Diese affine Karten verkleben sich dabei entlang der offenen Mengen

$$C_{AB} := D(x) = \{x \neq 0\} \subset C_A \text{ und } C_{BA} := D(t) = \{t \neq 0\} \subset C_B$$

mit dem Verklebungsisomorphismus $\phi : C_{AB} \to C_{BA}$, gegeben durch

$$\phi(x) = t^{-1},\ \phi(y) = s \cdot t^{-2} \text{ und } \phi(x^{-1}) = t$$

Die Gleichungen f_n und h_n werden durch die Relation

$$h_n(t) := f_n(t^{-1}) \cdot t^4$$

verklebt, so dass ϕ wohldefiniert ist:

$$\begin{aligned}\phi(0) = \phi(y^2 - f_n(x)) &= s^2 \cdot t^{-4} - f_n(t^{-1}) \\ &= t^{-4}\left(s^2 - t^4\, f_n(t^{-1})\right) = t^{-4}\left(s^2 - h_n(t)\right) = 0\end{aligned}$$

Dieselbe Überdeckung wird in [LIU] für hyperelliptische Kurven verwendet, wobei $\phi(y) = s \cdot t^{-g-1}$ gilt.

Die Koordinatenringe der affinen Kurven C_A und C_B bezeichnen wir im Folgenden mit

$$A := R_n[x,y]/(y^2 - f_n(x)) \text{ und } B := R_n[s,t]/(s^2 - h_n(t))$$

und Koordinatenringe der Durchschnitte C_{AB} und C_{BA} (die aus A und B durch das Lokalisieren nach x, bzw. t entstehen) mit

$$A_B := R_n[x,y,x^{-1}]/(y^2 - f_n(x)) \text{ und } B_A := R_n[s,t,t^{-1}]/(s^2 - h_n(t)).$$

Elemente der Koordinatenringe betrachten wir stets in der normalisierten Form, die wir bereits in 4.1 für affine hyperelliptische Kurven definiert haben (diese ist gegeben durch minimale Grade von y bzw. s).

Mit i_x, bzw. i_t bezeichnen wir (wie in 3.5) die Einschränkungsabbildun-

gen $A \to A_B$ und $B \to B_A$, wenn auch wir gelegentlich A als Unterring von A_B auffassen und insbesondere F_A für den Morphismus $i_x(F_A)$ schreiben. Im Folgenden werden wir uns hauptsächlich auf den Durchschnitt B_A konzentrieren, deswegen, aus Übersichtlichkeitsgründen, bezeichnen wir das Bild $\phi(g) \in B_A$ eines Polynoms $g \in A_B$ oft einfach mit g.

Projektive Liftungen des Frobeniusmorphismus:
Ein projektiver Morphismus ist eindeutig bestimmt durch seine Einschränkungen auf affine Karten, die sich auf den Durchschnitten verkleben müssen. Die affine Einschränkungen des projektiven Frobeniusmorphismus induzieren Liftungen des Frobeniushomomorphismus auf den Koordinatenringen der affinen Karten.

Im Folgenden betrachten wir projektive Liftungen des Frobenius auf elliptischen Kurven als ein Paar der affinen Liftungen des Frobenius und bezeichnen sie mit $(\tilde{E}, \tilde{F}_A, \tilde{F}_B)$:

$$\tilde{F}_A : \tilde{A}^\sigma \to \tilde{A} \text{ und } \tilde{F}_B : \tilde{B}^\sigma \to \tilde{B}$$

wobei die Einschränkungen $\tilde{F}_{AB}$ und $\tilde{F}_{BA}$ dieser Homomorphismen auf die Durchschnitte die folgende Verklebungsbedingung erfüllen:

$$\tilde{F}_{BA} = \phi \circ \tilde{F}_{AB} \circ \phi^{-1},$$

Die Differenz $\tilde{F}_{AB} - \phi \circ \tilde{F}_{BA} \circ \phi^{-1}$ kann man dabei als Hindernis zur Verklebung der affinen Karten auffassen, denn es verschwindet genau dann, wenn die affinen Morphismen auf den Durchschnitten übereinstimmen.

Die projektiven Liftungen des Frobenius sind immer verträglich mit der hyperelliptischen Involution. Die affinen Einschränkungen des projektiven Frobeniusmorphismus sind folglich stets die hyperelliptischen Liftungen (s. 4.1). Also können wir die Berechnung der Liftungen auf den Durchschnitten (analog zu 4.2) in einer Variablen durchführen.

Anders als in bisherigen Kapiteln, verzichten wir bei der Notation der Liftungen auf den Index, der die p-adische Genauigkeit anzeigt. In dem Rest des Kapitels sei $(E_{n-1}, F_A : A^\sigma \to A, F_B : B^\sigma \to B)$ eine Liftung des Frobenius auf E über R_{n-1}.

5.2 Verklebbungsbedingung an die Parameterräume

In diesem Abschnitt leiten wir die explizite Verklebungsbedingung an die Parameterräume der kleinen affinen Liftungen her.

Hindernisse zu Verklebung der affinen Liftungen:
Seien $(\tilde{A}, \tilde{F}_A)$ und $(\tilde{B}, \tilde{F}_B)$ kleine affine Liftungen von (A, F_A), bzw. (B, F_B) über R_n. Wir zeigen, dass man Hindernis zur Verklebung als eine Derivation auf Koordinatenringen über k definieren kann:

Lemma 5.2.1. *Seien die Bezeichnungen wie oben. Dann existiert eine eindeutige Derivation $\eta \in Der_\sigma(B_A^\sigma, B_A)$ definiert durch:*

$$p^n * \eta := \tilde{F}_{BA} - \phi \circ \tilde{F}_{AB} \circ \phi^{-1}$$

Beweis: folgt aus 2.3.2 angewendet auf die zwei kleine Liftungen von F_{AB}, gegeben durch $\tilde{F}_{AB}$ und $\phi \circ \tilde{F}_{BA} \circ \phi^{-1}$. $\square$.

Definition 5.2.2. *Die Derivation η aus dem Lemma 5.2.1 nennen wir im Folgenden* ***das Hindernis zur Verklebung von $\tilde{F}_A$ und $\tilde{F}_B$.***

Das Hindernis η ist bestimmt durch die Bilder der Basisvariablen t und s. Insbesondere ist $\eta(t^{-1})$ gegeben durch $\eta(t^{-1}) = -t^{-2p} \cdot \eta(t)$. Also können wir die Verklebungsbedingung von zwei kleinen affinen Liftungen als zwei Gleichungen in dem Koordinatenring des Durchschnittes angeben:

Satz 5.2.3. *Seien die Bezeichnungen wie oben. Die Liftungen $\tilde{F}_A$ und $\tilde{F}_B$ sind genau durch den Isomorphismus ϕ auf den Durchschnitten verklebbar, wenn folgende Gleichungen (genannt Verklebungsbedingungen) erfüllt sind:*

$$0 = \eta(t) = \tilde{F}_B(t) \cdot \tilde{F}_A(x) - 1$$

$$0 = \eta(s) = \tilde{F}_B(s) - \frac{\tilde{F}_A(y)}{\tilde{F}_A(x)^2}$$

Beweis:
Die Verklebungsbedingungen sind äquivalent zu

$$0 = \eta(s) = \tilde{F}_{BA}(s) - \phi(\tilde{F}_{AB}(y\, x^{-2})) = \tilde{F}_{BA}(s) - \phi(\tilde{F}_{AB}(\phi^{-1}(s)))$$

und

$$0 = \eta(t) = \tilde{F}_{BA}(t) \cdot \tilde{F}_{AB}(x) - 1 = \tilde{F}_{AB}(x) \left(\tilde{F}_{BA}(t) - \tilde{F}_{AB}(x^{-1}) \right)$$

$$= t^{-p} \left(\tilde{F}_{BA}(t) - \phi(\tilde{F}_{AB}(\phi^{-1}(t))) \right)$$

Die letzte Gleichheit gilt, denn $\tilde{F}_{BA}(t) - \tilde{F}_{AB}(x^{-1})$ verschwindet modulo p^{n-1} wegen der Verklebbarkeit von F_A und F_B. $\square$.

Wegen der Verträglichkeit mit der hyperelliptischen Involution sind die affine Liftungen $\tilde{F}_A$ und $\tilde{F}_B$ notwendigerweise hyperelliptisch, und mit dem folgenden Lemma können wir die Verklebungsbedingungen als Gleichungen über $k(t)$ auffassen:

Lemma 5.2.4. *Sei η das Hindernis zur Verklebung von affinen hyperelliptischen Liftungen $\tilde{F}_A$ und $\tilde{F}_B$, dann liegt $\eta(t)$ stets in $k(t)$ und $\eta(s)$ in $s \cdot k(t)$.*

Beweis:
Die Behauptung des Lemmas folgt aus der Definition der hyperelliptischen Liftungen, wegen:

$\tilde{F}_{BA}(t) \in R_n[t]$ und $\tilde{F}_{BA}(s) \in s \cdot R_n[t]$, sowie

$\phi(\tilde{F}_{AB}(x)) \in \phi(R_n[x]) \subset R_n(t)$ und $\phi(\tilde{F}_{AB}(y)) \in \phi(y \cdot R_n[x]) \subset s \cdot R_n(t)$
$\square$.

Verklebung der parametrisierten affinen Liftungen:
Betrachte die durch $(\hat{A}, \hat{F}_A)$, bzw. $(\hat{B}, \hat{F}_B)$ induzierten Parametrisierungen kleiner Liftungen auf affinen Karten. Nach dem Lemma 4.2.2 sind alle kleinen Liftungen von (A, F_A), bzw. (B, F_B) parametrisiert durch $(\alpha, \mu_A \in k[x])_{\hat{F}_A}$, bzw. $(\beta, \mu_B \in k[t])_{\hat{F}_B}$:

$$\tilde{F}_A(x) \in \{\hat{F}_A(x) + p^n * \Delta_x(\alpha, \mu_A)\}, \quad \tilde{F}_A(y) \in \{\hat{F}_A(x) + p^n * \Delta_y(\alpha, \mu_A)\}$$
$$\tilde{F}_B(t) \in \{\hat{F}_B(t) + p^n * \Delta_t(\beta, \mu_B)\}, \quad \tilde{F}_B(s) \in \{\hat{F}_B(s) + p^n * \Delta_s(\beta, \mu_B)\}$$

Die Parameter μ_A und μ_B beschreiben die Liftungen der definierenden Gleichungen der affinen Kurven, während α und β die affine Liftungen des Frobenius auf den gegebenen Liftungen der Kurven parametrisieren.

Nun formulieren wir die Verklebungsbedingung an die Parameterfunktionen Δ_x, Δ_y, Δ_t und Δ_s, die anschließend auf die Parameter α, β, μ_A und μ_B zurückführbar sind:

Theorem 5.2.5. *Sei η das Hindernis zur Verklebung von $(\hat{A}, \hat{F}_A)$ und $(\hat{B}, \hat{F}_B)$. Die durch $(\alpha, \mu_A)_{\hat{F}_A}$ und $(\beta, \mu_B)_{\hat{F}_B}$ parametrisierten kleinen affinen Liftungen $(\tilde{A}, \tilde{F}_A)$ und $(\tilde{B}, \tilde{F}_B)$ verkleben sich genau dann, auf den Durchschnitten, wenn die folgenden Gleichungen in B_A erfüllt sind:*

$$0 = t^{-p}\eta(t) + t^p \Delta_x(\alpha, \mu_A) + t^{-p}\Delta_t(\beta, \mu_B)$$

$$0 = \eta(s) + t^{2p}\Delta_y(\alpha, \mu_A) + 2t^{-p}s^p\Delta_t(\beta, \mu_B) - \Delta_s(\beta, \mu_B)$$

Beweis:
Betrachte das Hindernis $\tilde{\eta}$ zur Verklebung von $(\tilde{A}, \tilde{F}_A)$ und $(\tilde{B}, \tilde{F}_B)$ auf dem Durchschnitt, gegeben durch

$$t^p\,\tilde{\eta}(t) := \tilde{F}(t)\tilde{F}(x) - 1 \text{ und } \tilde{\eta}(s) := \tilde{F}(y)\tilde{F}(t)^2 - \tilde{F}(s)$$

Der Term $\tilde{\eta}(t)$ verschwindet genau dann, wenn:

$$\begin{aligned}
0 &= \tilde{F}(t)\tilde{F}(x) - 1 = (\hat{F}(t) + p^n * \Delta_t)(\hat{F}(x) + p^n * \Delta_x) - 1 \\
&= (\hat{F}(t)\hat{F}(x) - 1) + p^n * (\Delta_t\,\hat{F}(x) + \Delta_x\,\hat{F}(t)) \\
&= p^n * (\eta(t)\,t^{-p} + x^p\,\Delta_t + t^p\,\Delta_x) \\
&= p^n * (\eta(t)\,t^{-p} + t^{-p}\,\Delta_t + t^p\,\Delta_x)
\end{aligned}$$

und folglich ist die erste Gleichung der Verklebungsbedingung äquivalent zum Verschwinden von $\eta(t)$.

Analog formen den Term $\eta(s)$ um:

$$\begin{aligned}
0 &= \tilde{F}(y)\tilde{F}(t)^2 - \tilde{F}(s) \\
&= (\hat{F}(y) + p^n * \Delta_y)(\hat{F}(t) + p^n * \Delta_t)^2 - (\hat{F}(s) + p^n * \Delta_s) \\
&= \hat{F}(y)\hat{F}(t)^2 - \hat{F}(s) + p^n * \Big(\hat{F}(t)^2\,\Delta_y + 2\,\hat{F}(y)\hat{F}(t)\,\Delta_t - \Delta_s\Big) \\
&= p^n * \big(\eta(s) + t^{2p}\,\Delta_y + 2\,t^p y^p\,\Delta_t - \Delta_s\big) \\
&= p^n * \big(\eta(s) + t^{2p}\,\Delta_y + 2\,t^{-p}s^p\,\Delta_t - \Delta_s\big)
\end{aligned}$$

Also ist die zweite Gleichung der Verklebungsbedingung äquivalent zum Verschwinden von $\eta(s)$ und damit ist der Satz bewiesen. □

Beachte, dass diese Verklebungsbedingung die konkrete Gestalt des Parameterraums nicht verwendet. So könnte man diesen Satz für die Verklebung des Frobenius (oder auch weiteren Morphismen) auf andere affine Varietäten verallgemeinern, wobei man es für den entsprechenden Verklebungsmorphismus ϕ anpassen sollte.

Bei einer solchen Verallgemeinerung müsste man sich allerdings mit der Lösbarkeit des Verklebungssystems auseinandersetzen, während das für elliptische Kurven angegebene Gleichungssystem im ordinären Fall wegen der Existenz der kanonischen Liftung immer lösbar ist. Insbesondere ist diese Lösung immer eindeutig für ein μ aus k, denn diese Wahl entspricht der

gewählten Liftungsform der definierenden Gleichung (Liftung des Koeffizienten b).

Verklebungsbedingung als Gleichungssystem:
Durch auflösen der Parameterfunktionen erhalten wir unmittelbar ein lineares Gleichungssystem mit 2 Gleichungen in B_A und 4 Unbekannten: α, β, μ_A und μ_B. Wegen der Verklebbarkeit der definierenden Gleichung kann man allerdings einen der beiden μ-Parameter eliminieren durch

$$\mu_B(t) = \mu_A(t^{-1})t^{4p}$$

Eine weitere Bemerkung besteht darin, dass man beide Gleichung über $k(t)$ auffassen kann. In der Tat liegen Parameterfunktionen und die Hindernisse in $k(t)$, bzw. $s \cdot k(t)$ (s. 4.2.2 und 5.2.4), also ist die erste Verklebungsbedingung in $k(t)$ und die zweite in $s \cdot k(t)$ definiert.

Im nächsten Abschnitt zeigen wir, wie man das zu lösende Gleichungssystem erheblich vereinfachen und insbesondere durch die Betrachtung der projektiven Fortsetzbarkeit einer affinen Liftung nur auf die Variablen α und μ reduzieren kann.

5.3 Projektive Forsetzbarkeit einer affinen Liftung

Eine projektive Liftung des Frobenius ist eindeutig bestimmt durch die Einschränkung auf eine der affinen Karten wegen der Verklebbarkeit. In der Tat induziert die Einschränkung $\tilde{F}_{AB}$ einer affinen Liftung $\tilde{F}_A$ auf den Durchschnitt A_B stets den damit verklebbaren Homomorphismus $\tilde{F}_{BA}$ auf dem Durchschnitt B_A via

$$\tilde{F}_{BA} := \phi \circ \tilde{F}_{AB} \circ \phi^{-1}$$

Dieser induzierte Homomorphismus $\tilde{F}_{BA}$ zwischen den lokalisierten Ringen ist allerdings nicht immer fortsetzbar zu einer Liftung $\tilde{F}_B$ auf $\tilde{B}$, wobei die Eindeutigkeit einer solchen Fortsetzbarkeit in 3.5.2 bewiesen wurde. Falls diese Fortsetzung existiert, nennen wir die Liftung F_A *projektiv fortsetzbar*.

In diesem Abschnitt sei $(\tilde{A},\ \tilde{F}_A)$ eine kleine affine Liftung von (A, F_A) und $\tilde{F}_{AB}$ die Einschränkung von $\tilde{F}_A$ auf den Durchschnitt $\tilde{A}_B$

Lemma 5.3.1. *Eine affine Liftung $(\tilde{A},\ \tilde{F}_A)$ ist genau dann projektiv fortsetzbar, wenn folgende Bedingungen erfüllt sind:*

$$\deg_{t^{-1}} \phi\left(\tilde{F}_{AB}(x^{-1})\right) = 0$$

$$\deg_{t^{-1}} \phi \left(\tilde{F}_{AB}(y) \cdot \tilde{F}_{AB}(x^{-1})^2 \right) = 0$$

Beweis:
" $\Rightarrow$ ":
Nach der Voraussetzung existiert eine affine Liftung $\tilde{F}_B$, deren Einschränkung $\tilde{F}_{BA}$ sich mit $\tilde{F}_{AB}$ verklebt:

$$\tilde{F}_{BA} = \phi \circ \tilde{F}_{AB} \circ \phi^{-1}$$

Nach dem Lemma 3.5.3 gilt $\tilde{F}_{BA}(i_t(g)) = i_t(\tilde{F}_B(g))$ für jedes $g \in B$. Also erfüllt $\tilde{F}_{BA}$ die Bedingungen:

$$\deg_{t^{-1}} \tilde{F}_{BA}(t) = 0 \text{ und } \deg_{t^{-1}} \tilde{F}_{BA}(s) = 0$$

Die Anwendung von ϕ^{-1} auf diese beide Bedingungen beweist die Aussage des Satzes.

" $\Leftarrow$ ":
Betrachte den Homomorphismus $\hat{F}_{BA} := \phi \circ \hat{F}_{AB} \circ \phi^{-1} : B_A^\sigma \to B_A$, sowie seine Bilder:

$$\hat{F}_{BA}(t) := \phi(\hat{F}_{AB}(x^{-1})) \text{ und } \hat{F}_{BA}(s) := \phi(\hat{F}_{AB}(y \cdot x^{-2}))$$

Dieser Homomorphismus verklebt sich mit $\hat{F}_{AB}$ nach der Konstruktion und ist fortsetzbar zu einem Homomorphismus auf B nach dem Lemma 3.5.3, da es nach der Voraussetzung keine t^{-1} Terme enthält. □.

Als eine unmittelbare Folgerung aus diesem Satz erhalten wir zwei notwendige Bedingungen an eine fortsetzbare Liftung $(\tilde{A}_B, \tilde{F}_{AB})$, bzw. an $(\tilde{A}, \tilde{F}_A)$. Dieses Erkenntnis kombinieren wir mit der Verklebungsbedingung (5.2.5) an die Parameterräume und erhalten ein Kriterium dafür, wann eine affine Liftung sich projektiv fortsetzen läßt:

Theorem 5.3.2. *Seien $(\hat{A}, \hat{F}_A)$ und $(\hat{B}, \hat{F}_B)$ kleine affine Liftungen von (A, F_A), bzw. (B, F_B) und η das Hindernis zu der Verklebung dieser Liftungen. Eine durch $(\alpha, \mu)_{\hat{F}_A}$ parametrisierte affine Liftung $(\tilde{A}, \tilde{F}_A)$ ist genau dann projektiv fortsetzbar, wenn die folgenden (Fortsetzbarkeits-)Bedingungen erfüllt sind:*

$$\deg_{t^{-1}} \left[-\eta(t) - t^{2p} \Delta_x(\alpha, \mu) \right] = 0$$
$$\deg_{t^{-1}} \left[\eta(s) + t^{2p} \Delta_y(\alpha, \mu) + 2t^{-p} s^p \cdot \left(-\eta_t - t^{2p} \Delta_x(\alpha, \mu) \right) \right] = 0$$

Beweis:
" $\Rightarrow$ ":

Nach den Voraussetzungen existiert eine mit $(\tilde{A}, \tilde{F}_A)$ verklebbare Liftung $(\tilde{B}, \tilde{F}_B)$, parametrisiert durch $(\beta, \mu_B)_{\hat{F}_B}$. Betrachte die Verklebungsbedingung aufgelöst nach Δ_t und Δ_s:

$$\Delta_t = -\eta(t) - t^{2p}\Delta_x$$
$$\Delta_s = \eta(s) + t^{2p}\Delta_y + 2t^{-p}s^p(\eta(t) + t^{2p}\Delta_x)$$

Die t^{-1}-Grade von Δ_t und Δ_s verschwinden, weil beide Terme als Bilder des B-Homomorphismus $\frac{\tilde{F}_B - \hat{F}_B}{p^n} : B^\sigma \to B$ definiert sind. Damit ist die "⇒"-Richtung bewiesen.

" ⇐ ":
Sei $(\breve{A}, \breve{F})$ eine durch $(\alpha,\ \mu)$ parametrisierte Liftung. Betrachte die mit $\breve{A}$ verklebbare Liftung des Koordinatenringes $\breve{B}$, sowie den $\tilde{B}_A$ Homomorphismus $\phi \circ \breve{F}_{AB} \circ \phi^{-1}$ auf dem Durchschnitt $\breve{B}_A$, der im Raum der kleinen Liftungen von F_{BA} liegt.

Die Aussage des Theorems folgt nun aus dem Lemma 5.3.2, da nach der Voraussetzung:

$$\deg_{t^{-1}} \Delta_t := \deg_{t^{-1}} \left[-\eta(t) - t^{2p}\Delta_x\right] = 0$$
$$\deg_{t^{-1}} \Delta_s := \deg_{t^{-1}} \left[\eta(s) + t^{2p}\Delta_y + 2t^{-p}s^p\left(-\eta(t) - t^{2p}\Delta_x\right)\right] = 0$$

gilt und damit die Polynome

$$\breve{F}_{BA}(t) = \hat{F}_{BA}(t) + p^n * \Delta_t \text{ und } \breve{F}_{BA}(s) = \hat{F}_{BA}(s) + p^n * \Delta_s$$

in $i_t(\breve{B}) \subset B_A$ liegen. □.

Nach dem Satz können wir die Grade der Parameterfunktionen Δ_x und Δ_y, die eine projektiv fortsetzbare Liftung induzieren, genau bestimmen:

Korollar 5.3.3. *Seien die Bezeichnungen wie im Satz. Dann gilt:*

$$\deg_{t^{-1}} \Delta_x = \deg_{t^{-1}} \eta(t) + 2p$$
$$\deg_{t^{-1}} \Delta_y = \max\left\{\tfrac{p+1}{2} + \deg_{t^{-1}} \eta(t), \deg_{t^{-1}} \eta(s)\right\} + 2p$$

Beweis:
Die erste Gleichung folgt unmittelbar aus dem Theorem 5.3.2, nach dem t^{-i}- Koeffizientenvergleich. Weil $h(t)$ nach der Konstruktion immer durch t teilbar ist, gilt:

$$\tfrac{p+1}{2} \geq \deg_{t^{-1}}(t^{-p}s^p) = \deg_{t^{-1}}(t^{-p}s \cdot h^{\frac{p-1}{2}}(t))$$

Also erhalten wir folgende Schranke:

$$\deg_{t^{-1}}(\eta(s) + 2t^{-p}s^p\eta(t)) \leq \max\left\{\tfrac{p+1}{2} + \deg_{t^{-1}}\eta(t), \deg_{t^{-1}}\eta(s)\right\}$$

und damit auch die Behauptung des Korollars. □.

Auflösen der Fortsetzbarkeitsbedingungen

Eine effiziente Lösung des obigen Bedingungssystems findet man durch die Beobachtungen, dass die erste Fortsetzbarkeitsbedingung nur von dem Parameter α abhängt, und dass α aus dieser Gleichung zum großen Teil bestimmt ist:

Lemma 5.3.4. *Seien die Bezeichungen wie im Theorem. Die erste Fortsetzbarkeitsbedingung ist äquivalent zu:*

$$\deg_{t^{-1}}\left[\eta(t) + t^{2p}\alpha \cdot 2f^{\frac{p+1}{2}}\right] = 0$$

und insbesondere gilt:

$$\deg_{t^{-1}}\alpha = \deg_{t^{-1}}\eta(t) + 2p - 3\tfrac{p+1}{2} = \deg_{t^{-1}}\eta(t) + \tfrac{p-3}{2}$$

Beweis:

Wegen der Wahl von $\mu \in k$ und der Konstruktion der Basisliftung $\breve{\psi}$ (s. 4.2) gilt:

$$\deg_x \mu^p \cdot \breve{\psi}(x) < \tfrac{3(p+1)}{2} < 2p$$

und folglich ist der x-Grad von $\Delta_x(\alpha, \mu)$ unabhängig von μ:

$$\deg_x \Delta_x(\alpha, \mu) = \deg_x(\alpha \cdot 2f^{\frac{p+1}{2}}).$$

Damit ist die erste Behauptung des Lemmas bewiesen. Die zweite Behauptung folgt aus dem Korollar 5.3.3. □.

Hat man eine Lösung $\breve{\alpha}$ der ersten Fortsetzbarkeitsbedingung gefunden, so ist das gesuchte α ab einem gewissen Grad eindeutig bestimmt:

Lemma 5.3.5. *Seien α_1 und α_2 zwei Lösungen der ersten Fortsetzbarkeitsbedingung, dann gilt*

$$\deg_x[\alpha_1 - \alpha_2] < \tfrac{p-3}{2}$$

Beweis:

Setze beide Lösungen in die erste Fortsetzbarkeitsbedingung ein und subtrahiere die resultierenden Gleichungen voneinander. Wir erhalten:

$$\deg_x\left[t^{2p} \cdot (\alpha_1 - \alpha_2) \cdot 2f(x)^{\frac{p+1}{2}}\right] < 0$$

Das Polynom $t^{2p} \cdot 2f(x)^{\frac{p+1}{2}}$ liegt in $t^{\frac{p-3}{2}}k[t]$ wegen:

$$\deg_x[2f(x)^{\frac{p+1}{2}}] = 3\tfrac{p+1}{2} = 2p - \tfrac{p-3}{2}.$$

Folglich ist $(\alpha_1 - \alpha_2)$ stets durch $x^{\frac{p-3}{2}}$ in $k[x]$ teilbar. Damit ist die Aussage des Lemmas bewiesen. $\square$.

Nach diesem Lemma können wir das Auflösen der Fortsetzbarkeitsbedingungen in zwei Schritte zerlegen. Im ersten Schritt wird ein $\hat{\alpha}$ aus der ersten Fortsetzbarkeitsbedingung bestimmt (z. B. durch einen Koeffizientenvergleich bis zum Grad $\deg_{t^{-1}} \eta(t)$). Anschließend setzen wir dieses $\hat{\alpha}$ in die zweite Fortsetzbarkeitsbedingung und erhalten eine modifizierte Gleichung mit den Unbekannten $\mu^p \in k$ und $\breve{\alpha} := \alpha - \hat{\alpha}$.

Wegen der Bedingung $\deg_x \breve{\alpha} < \frac{p-3}{2}$ kann diese Gleichung durch einen Koeffizientenvergleich bis zum Grad

$$\deg_{t^{-1}} s^p t^{-p} = p - \tfrac{p-1}{2} = \tfrac{p+1}{2} \text{ gelöst werden.}$$

5.4 Berechnung der Liftungen: Algorithmus und Beispiele

Dieses Kapitel beginnt mit der Beschreibung eines induktiven Algorithmus zur Berechnung der projektiven Liftung der Frobenius auf elliptischen Kurven, der auf den Ergebnissen des letzten Kapitels basiert. Ausgehend von einer projektiven Liftung (E_{n-1}, F_A, F_B) des Frobeniusmorphismus über R_{n-1} berechnen wir im n-ten Schritt eine Liftung $(E_n, \tilde{F}_A, \tilde{F}_B)$. Dieser Schritt ist immer durchführbar, falls E ordinär ist.

Algorithmus

1) *Hindernisse zur Verklebung:*
Berechne zwei beliebige Liftungen $(\tilde{A}, \tilde{F}_A)$ und $(\tilde{B}, \tilde{F}_B)$ auf den affinen Karten, sowie das Hindernis $\eta = (\eta(t), \eta(s))$ zur Verklebung auf den Durchschnitten.

2) *Auflösen der Fortsetzbarkeitsbedingung:*
Finde zunächst eine Lösung $\hat{\alpha}$ der ersten Fortsetzbarkeitsbedingung und setze $\alpha := \breve{\alpha} + \hat{\alpha}$ in die zweite Fortsetzbarkeitsbedingung ein. Dadurch erhalten wir eine modifizierte Bedingung mit einem beschränkten $\hat{\alpha}$, deren Lösung $(\breve{\alpha}, \mu)$ das gesuchte Paar (α, μ) liefert.

3) *Liftungen des Frobenius*
Berechne die, durch (α, μ) parametrisierte Liftung $(\breve{A}, \breve{F}_A)$. Anschließend berechne Δ_t und Δ_s aus der Verklebungsbedingung und damit auch die affine

Liftung auf der Karte B.

Den skizzierten Algorithmus illustrieren wir nun am Beispiel der elliptischen Kurve $E : y^2 = x^3 + x + 2$ über k. Die Koordinatenringe der affinen Karten von E sind gegeben durch:

$$A := k[x, y]/(y^2 - x^3 - x - 2) \text{ und } B := k[s, t,]/(s^2 - 2t^4 - t^3 - t)$$

Beispiel: Hindernisse zur Verklebung
Betrachte die triviale Liftung der definierenden Gleichung ($y^2 = x^3 + x + 2$) über $\mathbb{Z}_q/p^2$ sowie die zugehörigen Liftungen der beiden affinen Karten. Seien $\hat{F}_A$ und $\hat{F}_B$ kleine affine Liftungen auf beiden Karten, induziert durch folgende Derivationen ψ_A und ψ_B:

$$\begin{aligned}
\psi_A(x) &= 4x^{11} + 3x^9 + 3x^8 + 2x^7 + 3x^6 + 3x^4 + 3x + 3 \\
\psi_A(y) &= y \cdot (x^{12} + 4x^{10} + x^9 + 3x^8 + 3x^7 + 3x^5 + 4x^4 + 4x^2 + 4x + 2) \\
\psi_B(t) &= 2t^{11} + 3t^{10} + 3t^9 + 4t^7 + 4t^5 + 3t^4 + 3t^3 \\
\psi_B(s) &= s \cdot (t^{14} + 2t^{12} + t^{11} + t^9 + 3t^7 + 2t^5 + 3t^4 + 4t^3 + 4t + 4)
\end{aligned}$$

Das Hindernis zur Verklebung von $\hat{F}_A$ und $\hat{F}_A$ ist gegeben durch die Derivation η:

$$\begin{aligned}
\eta(t) &:= ((x^p + p * \psi_A(x))(t^p + p * \psi_B(t)) - 1) \cdot t^{-p} \\
&= 2t^{11} + t^{10} + t^9 + 4t^7 + 3t^6 + 4t^5 + t^4 + 3t^2 + 3t + 4t^{-1} \\
\eta(s) &:= (y^p + p * \psi_A(y))(t^p + p * \psi_B(t))^2 - (s^p + p * \psi_A(s)) \\
&= s \cdot (2t^9 + 3t^8 + 2t^6 + t^{-1} + 4t^{-2} + t^{-4})
\end{aligned}$$

Beispiel: Fortsetzbarkeitsbedingungen
Für die Betrachtung des Fortsetzbarkeitskriteriums benötigen wir die Lösung $(\breve{\psi}_x, \breve{\psi}_y)$ der Basisgleichung von A^σ (s. 4.2):

$$\begin{aligned}
\breve{\psi}(x) &= (x^8 + 2x^7 + x^6 + x^4 + 2x^3 + 4x^2 + x + 2) \\
\breve{\psi}(y) &= y \cdot (4x^9 + 3x^8 + 2x^7 + 2x^6 + 3x^5 + 3x^4 + x^3 + 4x^2 + 2x + 1)
\end{aligned}$$

Betrachte zunächst die erste Fortsetzbarkeitsbedingung:

$$\begin{aligned}
&\deg_{t^{-1}} \left[-\eta(t) - t^{2p} \cdot \Delta_x(\alpha, \mu)\right] = 0 \Leftrightarrow \\
&\deg_{t^{-1}} \left[-4t^{-1} - t^{2p} \cdot 2f(x)^3 \cdot \alpha\right] = 0
\end{aligned}$$

Eine Lösung $\breve{\alpha} := 3x^2$ dieser Bedingung finden wir durch den Koeffizienten-

vergleich in t^{-1}.

Betrache nun die zweite Fortsetzbarkeitsbedingung:

$$\deg_{t^{-1}} \left[\eta(s) + t^{2p}\Delta_y(\alpha,\mu) + 2t^{-p}s^p\left(-\eta(t) - t^{2p}\cdot\Delta_x(\alpha,\mu)\right)\right] = 0$$

Wir setzen $\alpha := \breve{\alpha} + \tilde{\alpha}$ und μ in diese Gleichung ein und erhalten

$$\begin{aligned}\deg_{t^{-1}} \Big[\eta(s) + t^{2p}\cdot\Big(y\cdot f'(x)^p\cdot(\tilde{\alpha}+3x^2) + \mu^p\cdot\breve{\psi}_y\Big) + \\ 2t^p s^p\cdot\Big(-t^{-2p}\eta(t) - 2f(x)^{\frac{p+1}{2}}\cdot(\tilde{\alpha}+3x^2) - \mu^p\cdot\breve{\psi}_x\Big)\Big] = 0\end{aligned}$$

wobei μ im Körper k nach Konstruktion liegt und für $\tilde{\alpha}\in k[x]$ die Schranke $\deg_x\tilde{\alpha}\leq 1$ wegen 5.3.5 gilt.

Wir vereinfachen die Bedingung dadurch, dass wir alle Terme, die nicht zu dem t^{-1}-Grad beitragen, eliminieren:

$$\begin{aligned}&\deg_{t^{-1}}\Big[s\cdot(t^{-4}+4t^{-2}+t^{-1}) + 3t^{-2}s\cdot\tilde{\alpha} + 4t^{-4}s + 4t^{-1}s\cdot\mu^p + \\ &\qquad s\cdot(2t^{-4}+3t^{-2}+2t^{-1}) + t^{-2}s\cdot\tilde{\alpha} + 3t^{-4}s + 3t^{-1}s\cdot\mu^p\Big] = 0\end{aligned}$$

$\Leftrightarrow$

$$\deg_{t^{-1}}\left[s\cdot\left(2t^2+3t^{-1}+4t^{-2}\cdot\tilde{\alpha}+2t^{-1}\cdot\mu^p\right)\right]$$

Durch den Koeffizientvergleich in t^{-2} und t^{-1} erhalten wir $\tilde{\alpha}=2$ und $\mu=1$ und damit auch das gesuchte Paar ($\alpha := 3x^3+2$, $\mu := 1$).

Beispiel: Liftungen des Frobenius
Aus den berechneten α und μ erhalten wir nun eine affine projektiv fortsetzbare Liftung $(\tilde{A},\tilde{F}_A)$:

$$\begin{aligned}\tilde{A} &:= R_1[x,y]/(y^2-x^3-x-2+5) = R_1[x,y]/(y^2-x^3-x-22)\\ \tilde{F}_A(x) &:= x^5+5\cdot(\psi_A(x)+2f(x)^3\cdot\alpha)+\mu^p\cdot\breve{\psi}_x\\ &= x^5+5\cdot(4x^7+3x^4+x^3+x^2+2x+2)\\ \tilde{F}_A(y) &:= y^5+5\cdot(\psi_A(y)+y\cdot f'(x)^5\cdot\alpha+\mu^p\cdot\breve{\psi}_y\\ &= y\cdot f(x)^2+5\cdot y\cdot(x^8+2x^6+x^5+2x^4+x^3+x^2+x)\end{aligned}$$

Die Terme Δ_t und Δ_s erhalten wir aus den Verklebungsbedingungen (5.3.1). Die Liftung auf Karte B ist gegeben durch $(\tilde{B},F_B)$:

$$\begin{aligned}\tilde{B} &:= R_1[s,t]/(s^2-22t^4-t^3-t)\\ \tilde{F}_B(t) &:= t^5+5\cdot(3t^{10}+3t^9+4t^8+4t^7+2t^6+t^3)\end{aligned}$$

$$\tilde{F}_B(t) := s^5 + 5 \cdot s \cdot (4t^{13} + 3t^{12} + 2t^{11} + 4t^{10} + 2t^9 + 3t^8 + 4t^7 + 2t^6 + 2t^4 + 3t^3 + t^2 + 3)$$

Durch die Betrachtung der Fortsetzbarkeit des induzierten Homomorphismus auf den Durchschnitten anstelle der Verklebungsbedingung haben wir ein viel einfacheres Gleichungssystem erhalten und insbesondere mussten wir den Parameter β nicht bestimmen. Das zu der obigen Liftung gehöriges β wäre gegeben durch:

$$\beta = 4t^{20} + t^{18} + t^{17} + 4t^{16} + t^{15} + 3t^{14} + 3t^{13} + 2t^{12} + 2t^{11} + 3t^{10} + 4t^9 + 2t^8 + 4t^7 + 3t^6 + 2t^5 + t^4 + t^3 + 4t^2 + 4t + 1$$

Kapitel 6

Operation des Frobenius auf Differentialräumen

In diesem Abschnitt zeigen wir wie man die deformationstheoretische Liftungsmethoden auf die Räume der Differentiale und die induzierte Operation des Frobenius fortsetzen kann. Dabei beschränken wir uns auf die elliptischen Kurven und deren holomorphen Differentiale.

Der Raum der holomorphen Differentialen der kanonischen Liftung einer elliptischen Kurve ist ein eindimensionaler $W(k)$-Modul mit dem erzeugenden Element $\{\frac{dx}{y}\}$. In diesem Kapitel betrachten wir die Module $R_n\{\frac{dx}{y}\}$ und solche affine Liftungen des Frobenius auf elliptischen Kurven, die eine lineare Operation auf diesen Moduln induzieren. Einen Beispiel für solche induzierten Operation liefern die affine Einschränkungen der kanonischen Liftung des Frobenius auf die affine Karte $A : y^2 = x^3 + ax + b$.

Wir beschreiben eine explizite Parametrierung sowie die Berechnungsmethoden für solche Liftungen. Anschließend zeigen wie diese Ergebnisse für eine schnellere Berechnung der kanonischen Liftung des Frobenius eingesetzt werden können und geben eine gute Schätzung für die Grade dieser Liftung.

Die Verallgemeinerungsmöglichkeiten auf andere Differentialräume, sowie einige weitere Anwendungsideen diskutieren wir im letzten Abschnitt.

6.1 Affine Ω-Liftungen des Frobenius

Die durch einen projektiven Morphismus induzierte Operation auf holomorphen Differentialen, ist eindeutig bestimmt durch die Einschränkung dieses Morphismus auf die geeignete affine Umgebung. In diesem Abschnitt beschreiben wir solche affine hyperelliptische Liftungen des Frobenius auf elliptischen Kurven, die eine lineare Operation auf dem von $\frac{dx}{y}$ erzeugten Modul induzieren.

Lineare Operation auf $R_n\{\frac{dx}{y}\}$***:***

Eine hyperelliptische affine Liftung des Frobeniushomomorphismus F_n nennen wir eine Ω-*Liftung des Frobenius*, falls F_n eine lineare Operation auf dem Modul $R_n\{\frac{dx}{y}\}$ induziert:

$$F_n^*(\{\tfrac{dx}{y}\}) = \tfrac{DF_n(x)dx}{F_n(y)} = \Lambda_n \tfrac{dx}{y} \text{ für einen Eigewert } \Lambda_n \in R_n,$$

wobei $DF_n(x) := \frac{\partial F_n(x)}{\partial x}dx + \frac{\partial F_n(x)}{\partial y}dy$ der totale Differential von F_n ist. Wegen der Definition der affinen hyperelliptischen Liftungen liegt $F_n(x)$ in $R_n[x]$ und folglich gilt:

$$DF_n(x) = F_n'(x)dx \ \in \ R_n[x]dx,$$

wobei $F_n'(x)$ die übliche Ableitung eines x-Polynoms bezeichnet. Also ist eine affine Liftung des Frobenius genau dann eine Ω-Liftung, wenn sie die folgende Ω-*Verträglichkeitsbedingung* für einen Eigenwert $\Lambda_n \ \in R_n[x]$ erfüllt:

$$F_n'(x) = \tfrac{F_n(y)}{y}\Lambda_n = \tfrac{(F_{n-1}(y))_n}{y}\Lambda_n \ \text{ in } R_n[x]$$

Die letzte Gleichung gilt für jede Liftung des Frobenius, denn der Frobeniushomomorphismus $F : A^\sigma \to A$ induziert die Nullabbildung

$$F^*(\tfrac{dx}{y}) = \tfrac{DF(x)}{F(y)} = \tfrac{px^{p-1}dx}{y^p} = 0 \ \text{ auf dem Modul } k\{\tfrac{dx}{y}\}$$

und folglich $\bar{\Lambda}_n \equiv 0 \bmod p$ stets erfüllt ist.

Aus Übersichtlichkeitsgründen werden wir für die triviale Liftungen $(F_{n-1}(y))_n$, bzw. $(\Lambda_{n-1})_n$ im Folgenden oft $F_{n-1}(y)$, bzw. Λ_{n-1} schreiben.

Hindernisse zur Ω-Liftung des Frobenius

Im Folgenden sei F_{n-1} eine Ω-Liftung des Frobenius über R_{n-1}, mit dem Eigenwert Λ_{n-1}. Für eine kleine affine Liftung F_n von F_{n-1} definieren wir *das Hindernis* $\delta(F_n, \Lambda_n)$ *zur* Ω-*Verträglichkeit in Abhängigkeit von dem Ei-*

genwert Λ_n durch:

$$p^n * \delta(F_n, \Lambda_n) := \Lambda_n \frac{F_{n-1}(y)}{y} - F_n'(x) \ \in p^n R_n[x]$$

wobei die Wohldefiniertheit wegen der Ω-Verträglichkeit von F_{n-1} und dem Lemma A.3 folgt.

In diesem Abschnitt betrachten wir den Parameterraum der kleinen affinen Liftungen von F_{n-1} mit einer fixierten Liftung $\hat{F}_n$ als Basis. Der folgende Satz liefert eine Bedingung der Ω-Verträglichkeit an diesen Parameterraum für den vorgegebenen Eigenwert:

Satz 6.1.1. *Sei F_n eine weitere kleine affine Liftung von F_{n-1}, parametrisiert durch $(\alpha, \mu)_{\hat{F}_n}$. Diese Liftung induziert genau dann eine Ω-Operation mit dem Eigenwert $\Lambda_n := \Lambda_{n-1} + p^n * \lambda_n$, wenn die Ableitung der Parameterfunktion $\Delta_x(\alpha, \mu) \in k[x]$ folgende Gleichung erfüllt:*

$$\Delta_x'(\alpha, \mu) = \delta(\hat{F}_n, \Lambda_{n-1}) + \lambda_n \cdot f^{(p-1)/2}$$

Beweis:
Betrachte die Ω -Verträglichkeitsbedingung:

$$\begin{aligned}
0 &= \Lambda_n \tfrac{F_{n-1}(y)}{y} \ - F_n'(x) \\
&= (\Lambda_{n-1} + p^n * \lambda_n) \left(\tfrac{\hat{F}_{n-1}(y) + p^n * \Delta_y(\alpha,\mu)}{y} \right) - \left(\hat{F}_n'(x) + p^n * \Delta_x'(\alpha, \mu) \right) \\
&= p^n * \left(\delta(\hat{F}_n, \Lambda_{n-1}) + \lambda_n \tfrac{\bar{F}_{n-1}(y)}{y} + \bar{\Lambda}_{n-1} \tfrac{\Delta_y(\alpha,\mu)}{y} - \Delta_x'(\alpha, \mu) \right) \\
&= p^n * \left(\delta(\hat{F}_n, \Lambda_{n-1}) + \lambda_n f^{\frac{p-1}{2}} - \Delta_x'(\alpha, \mu) \right)
\end{aligned}$$

wobei die letzte Gleichheit gilt, da die Reduktion $\bar{\Lambda}_{n-1}$ modulo p verschwindet und $\bar{F}_n(y) = y^p = y f^{\frac{p-1}{2}}$ gilt. $\square$

Mit dieser Bedingung können wir die Eindeutigkeit der induzierten linearen Operation für den Fall der ordinären elliptischen Kurven beweisen:

Satz 6.1.2. *Sei F_{n-1} eine affine Liftung des Frobenius auf einer elliptischen Kurve E und F_n eine kleine Ω-Liftung von F_{n-1}. Dann erfüllt der Eigenwert $\Lambda_n := \Lambda_{n-1} + p^n * \lambda_n$ von F_n die folgende Gleichung:*

$$\lambda_n \cdot H(E) + C_{x^{p-1}} \left(\delta(\hat{F}_n, \Lambda_{n-1}) \right) = 0,$$

wobei $H(E)$ die Hasse-Invariante der Kurve E ist und $C_{x^{p-1}}(g)$ den x^{p-1}-Koeffizienten für ein $g \in k[x]$ bezeichnen.

Beweis:
Betrachte die Ω -Verträglichkeitsbedingung:

$$\Delta'_x(\alpha, \mu) = \delta(\hat{F}_n, \Lambda_{n-1}) + \lambda_n \cdot f^{\frac{p-1}{2}}$$

und insbesondere den Koeffizient von x^{p-1} auf beiden Seiten der Gleichung. Auf der linken Seite verschwindet dieser Koeffizient, da er wegen der Ableitungsdefinition durch p teilbar ist. Für die rechte Seite folgern wir daraus:

$$C_{x^{p-1}}\left(\delta(\hat{F}_n, \Lambda_{n-1})\right) + \lambda_n \cdot H(E) = 0$$

da die Hasse-Invariante $H(E)$ genau als der x^{p-1}-Koeffizient in $f^{\frac{p-1}{2}}$ definiert ist. $\square$.

Lemma 6.1.3. *Sei $F_1 := F + p * \psi$ eine Ω-Liftung des Frobenius über R_1, dann ist der Eigenwert von F_1 gegeben durch $p \cdot \frac{1}{H(E)}$ in R_1.*

Beweis:
Betrachte das Hindernis

$$\delta(F_1, 0) = 0 \cdot \psi(y) - (x^p)' - p * \psi'(x) = p * (-x^{p-1} - \psi'(x))$$

und den x^{p-1}-Koeffizient $C_{x^{p-1}}(\delta(F_1, 0)) = -1$. Die Behauptung des Lemmas folgt nun aus dem Satz 6.1.2. $\square$.

An den obigen Ergebnissen sieht man insbesondere, wieso man die Ordinarität der elliptischen Kurven ($H(E) \neq 0$) für die projektive Liftung benötigt:

Korollar 6.1.4. *Es existieren keine projektiven Liftungen des Frobenius über p-adische Quotientenringe auf supersingulären elliptischen Kurven.*

Beweis:
Eine projektive Liftung des Frobenius würde eine lineare Operation auf den holomorphen Differentialen induzieren. Nach dem Lemma 6.1.3 ist der Eigenwert dieser Operation gleich $p/H(E)$ modulo p^2, was zum Widerspruch zu der Supersingularität der Kurve führt. $\square$.

Im Folgenden beschränken wir uns auf die ordinären elliptischen Kurven. In diesem Fall ist das Eigenwert $\Lambda_n := \Lambda_{n-1} + p^n * \lambda_n$ einer Ω-Liftung von F_{n-1} eindeutig bestimmt durch

$$\lambda_n = -\frac{C_{x^{p-1}}\left(\delta(\hat{F}_n, \Lambda_{n-1})\right)}{H(E)}$$

Definition 6.1.5. *Sei $\lambda_n \in k[x]$ wie oben. Den Ω-**Hindernis zu** F_n definieren dann wir durch:*

$$\delta(F_n) := \delta(\hat{F}_n, \Lambda_{n-1} + \lambda_n f^{\frac{p-1}{2}})$$

Theorem 6.1.6. *Eine durch $(\alpha, \mu)_{\hat{F}_n}$ parametrisiere kleine affine Liftung F_n von F_{n-1} ist genau dann eine Ω-Liftung, wenn die Ableitung der x-Parameterfunktion gleich dem zugehörigen Ω-Hindernis ist:*

$$\Delta'_x(\alpha, \mu) = \delta(F_n)$$

Beweis: folgt aus 6.1.1 und 6.1.2. □.

Parametrisierung der Ω-Liftungen

Zum Schluss des Abschnittes geben wir eine Parametrisierung der kleinen Ω-Liftungen von F_{n-1}. Im Folgenden wählen wir eine Ω-Liftung $\hat{F}_n$ als Basis der Parametrisierung aller kleinen Liftungen.

Lemma 6.1.7. *Sei F_n eine weitere Ω-Liftung von F_{n-1}, parametrisiert durch $(\alpha, \mu)_{\hat{F}_n}$, dann gilt:*

$$\Delta_x(\alpha, \mu) = \gamma^p \quad \textit{für ein eindeutiges } \gamma \in k[x]$$

Beweis:
Die Anwendung des Theorems 6.1.5 auf die Ω-Liftungen F_n und $\hat{F}_n$ liefert:

$$\Delta'_x(\alpha, \mu) = \delta(\breve{F}_A) = 0$$

und beweist die Aussage des Lemmas. □.

Für die Parametrisierung des Raumes aller kleinen Ω-Liftungen müssen wir eine Lösung der Basisgleichung fixieren:

Lemma 6.1.8. *Es existiert eine solche Lösung $(\breve{\psi}_x, \breve{\psi}_y)$ der Basisgleichung von A:*

$$\breve{\psi}_x \cdot (f')^p + \breve{\psi}_y \cdot f^p + 1 = 0\,,$$

bei der $\breve{\psi}_x = \tau^p$ für ein $\tau \in k[x]$ gilt.

Beweis:
Wegen der Teilerfremdheit von f und f' existieren solche u und v, die folgende Gleichung erfüllen:

$$v \cdot (f^\sigma)' + u \cdot f^\sigma + 1 = 0 \Leftrightarrow$$
$$v^p \cdot ((f^\sigma)')^p + u^p \cdot (f^\sigma)^p + 1 = 0 \Leftrightarrow$$
$$v^p \cdot (f')^p + u^p \cdot f^p + 1 = 0$$

Daraus erhält man folgende Lösung der Basisgleichung:

$$\left(\breve{\psi}_x := v^p, \;\; \breve{\psi}_x := \tfrac{1}{2} u^p f^{\frac{p-1}{2}}\right)$$

□.

Im Folgenden verwenden wir die oben angegebene Lösung der Basisgleichung und schreiben τ^p für $\breve{\psi}(x)$.

Die kleinen Ω-Liftungen bilden eine Untermenge von kleinen affinen Liftungen, die durch den folgenden Satz eindeutig parametrisiert ist:

Satz 6.1.9. *Eine durch $(\alpha, \mu)_{\hat{F}_n}$ parametrisierte Liftung F_n ist genau dann eine Ω-Liftung, wenn*

$$\alpha = f^{\frac{p-1}{2}} \nu^p \text{ für ein } \nu \in k[x] \text{ gilt.}$$

Beweis:
"⇒":
Nach dem Lemma 6.1.6 existiert ein $\gamma \in k[x]$, das die folgende Gleichung erfüllt:

$$\gamma^p = \Delta_x(\alpha, \mu) = 2f^{\frac{p+1}{2}} \cdot \alpha + \mu^p \tau^p$$

wobei $\tau^p := \breve{\psi}_x$ der Lösung der Basisgleichung aus dem Lemma 6.1.7 entspricht. Die Behauptung des Satzes folgt nun aus der Tatsache, dass $2f^{\frac{p+1}{2}} \cdot \alpha$ eine p-Potenz in $k[x]$ sein muss. □.

"⇐":
Setze $\gamma := 2f \cdot \nu + \mu \cdot \tau$, dann gilt $\gamma^p = \Delta_x(\alpha, \mu)$ und die Behauptung des Lemmas folgt aus dem Theorem 6.1.5. □.

6.2 Existenz und Berechnung der Ω-Liftungen

Die hergeleitete Parametrisierung der kleinen Ω-Liftungen basiert auf einer existierenden kleiner Ω-Liftung F_n von F_{n-1}. In diesem Abschnitt untersuchen wir die Existenz einer solchen Liftung und beschreiben eine einfache Berechnungsmethode.

Existenz der Ω-Liftungen

Definition 6.2.1. *Eine Ω-Liftung F_{n-1}, für die eine kleine Ω-Liftung F_n existiert, nennen wir im Folgenden eine* ***erweiterbare Ω-Liftung****.*

Eine notwendige Bedingung an eine erweiterbare Liftung ist gegeben durch:

Satz 6.2.2. *Sei F_n eine erweiterbare Ω-Liftung, dann erfüllt der Term $\delta_0(F_n) \in k[x]$, definiert durch:*

$$p^{n+1} * \delta_0(F_n) := \Lambda_n \tfrac{(F_n(y))_{n+1}}{y} - (F_n)'_{n+1}(x) \ \in p^n R_n[x]$$

die folgende Bedingung:

$$C_{x^{jp-1}}\left(\delta_0(F_n)\right) = 0 \ \textit{ für alle } j > 1$$

Beweis:
Betrachte die Ω-Verträglichkeitsbedingung an eine Ω-Liftung F_{n+1} von F_n über R_{n+1} induziert durch $F_{n+1} := F_n + p^{n+1} * \psi$

$$\begin{aligned} 0 &= -F'_{n+1}(x) + \Lambda_{n+1}\tfrac{F_{n+1}(y)}{y} \\ &= -F'_n(x) - p^{n+1} * \psi'(x) + \Lambda_{n+1}\tfrac{F_n(y)}{y} \\ &= p^{n+1} * (-\psi'(x) + \delta_0(F_n) + \lambda_{n+1} f^{\frac{p-1}{2}}) \end{aligned}$$

Die Behauptung des Satzes folgt aus dem Koeffizientenvergleich von x^{jp-1} in der obigen Gleichung für ein $j > 1$ wegen:

$$C_{x^{jp-1}}(\psi'(x)) = 0 \text{ und } \deg_x f^{\frac{p-1}{2}} < 2p$$

□.

Als nächstes definieren wir ein Analogon zu der Stammfunktion in $k[x]$ und leiten ein Existenzkriterium her. Für ein Polynom $g = \sum g_i x^i \in k[x]$ definieren wir eine Abbildung $\int$ via:

$$\int g := \int(g) := \sum_{i+1 \notin p\mathbb{N}} \tfrac{g_i}{i+1} x^{i+1} \ \in k[x]$$

Diese Abbildung hat die folgende Eigenschaft:

$$\int g' = \int \sum g_i \cdot i \cdot x^{i-1} = \int \sum_{i \notin p\mathbb{N}} g_i \cdot i \cdot x^{i-1} = g$$

und liefert eine Stammfunktion $\int a$ von $a = \sum a_i x^i \in k[x]$ genau dann, wenn a_{jp+1} für alle $j \in N$ verschwinden.

Satz 6.2.3. *Sei $\hat{F}_n$ eine kleine affine Liftung von F_{n-1}, mit dem Ω-Hindernis $\delta := \delta(\hat{F}_n)$, das die Bedingung*

$$C_{x^{jp-1}}(\delta) = 0 \ \textit{ für alle } j > 1 \textit{ erfüllt}$$

Die Ω-Liftung F_{n-1} ist genau dann erweiterbar, wenn

$$\textstyle\int(\delta) \equiv \xi^p \ \ mod\ f^{\frac{p+1}{2}}$$

für ein $\xi \in k[x]$*, mit* $\deg_x(\xi) < 3$ *gilt.*

Beweis:
"$\Rightarrow$":
Sei F_n eine kleine Ω-Liftung von F_{n-1}, parametrisiert durch $(\alpha, \mu)_{\hat{F}_n}$. Nach dem Theorem 6.1.6 gilt

$$\Delta'_x(\alpha, \mu) = \delta \;\Leftrightarrow \text{ (wegen der Bedingung an } \delta)$$
$$2f^{\frac{p+1}{2}} \cdot \alpha + \mu^p \tau^p = \int \delta + \gamma^p \;\text{ für ein } \gamma \in k[x]$$

Betrachte diese Gleichung modulo $f^{\frac{p+1}{2}}$:

$$\mu^p \tau^p - \gamma^p \equiv \int \delta \mod f^{\frac{p+1}{2}}$$

und den Term $\mu\tau - \gamma$ modulo f:

$$\mu\tau - \gamma = uf + v \text{ , wobei } \deg_x v < \deg_x f = 3 \text{ gilt.}$$

Die Wahl $\xi := v$ erfüllt die Bedingungen des Satzes, wegen

$$\xi^p = \mu^p \tau^p - \gamma^p - u^p f^p \equiv \int \delta \mod f^{\frac{p+1}{2}} \;\square.$$

"$\Leftarrow$":
Sei $\xi \in k[x]$ ein Polynom, das die Bedingungen des Satzes erfüllt:

$$\xi^p + wf^{\frac{p+1}{2}} = \int \delta$$

Eine Ω-affine Liftung $(\tilde{A}, \tilde{F}_A)$ erhält man z.B. durch die Parameterwahl: $\alpha := \frac{w}{2}$, denn in diesem Fall gilt:

$$\Delta_x(\alpha, \mu) = f^{\frac{p+1}{2}} \cdot w + \mu^p \cdot \tau^p = \int \delta - \xi^p + \mu^p \cdot \tau^p = \int \delta + \gamma^p$$

für $\gamma := \mu \cdot \tau - \xi$. Die Aussage des Satzes folgt damit aus dem Theorem 6.1.6. $\square$.

Berechnung einer affinen Ω-Liftung
Als eine unmittelbare Folgerung aus dem Satz 6.2.3 erhalten wir eine einfache konstruktive Methode für die Berechnung einer kleinen Ω-Liftung. Dabei wählen wir eine beliebige kleine Liftung $\hat{F}_n$, berechnen ein ξ wie in 6.2.3 durch einen Koeffizientenvergleich in drei Unbekannten und wählen

$$\alpha := \frac{\int \delta - \xi^p}{2f^{\frac{p+1}{2}}}$$

Für jede Liftung der Kurve und das zugehörige Parameter μ ist die durch das Parameterpaar (α, μ) parametrisierte Liftung F_n ist ein Ω-Liftung nach dem Satz 6.1.6 wegen

$$\Delta'_x(\alpha,\mu) = (2f^{\frac{p+1}{2}} \cdot \alpha + \mu^p \tau^p)' = (\int(\delta) - \xi^p \mu^p \tau^p)' = \delta$$

Beispiel: Ω-Hindernis
Diese Berechnung illustrieren wir a Beispiel der Kurve $E : y^2 = x^3 + x + 2$ in Charakteristik 5 (s. auch Beispiel 5.4). Betrachte eine kleine affine Liftung des Frobenius (A_1, F_1) gegeben durch die triviale Liftung der definierenden Gleichung und die induzierende Derivation ψ:

$$\psi(x) = 4x^{11} + 3x^9 + 3x^8 + 2x^7 + 3x^6 + 3x^4 + 3x + 3$$
$$\psi(y) = y \cdot (x^{12} + 4x^{10} + x^9 + 3x^8 + 3x^7 + 3x^5 + 4x^4 + 4x^2 + 4x + 2)$$

Das Hindernis $\delta(F_1, 0)$ zu der Ω-Verträglichkeit von F_1 mit dem Eigenwert $\Lambda = 0 \in R_1$ ergibt sich aus

$$\begin{aligned} 5 * \delta(F_1, 0) &= \Lambda_1 \cdot F_1(y) - F_1(x) = -(x^5)' - \psi'(x) \\ &= 5 \cdot (4x^4 + x^{10} + 3x^8 + x^7 + x^6 + 2x^5 + 3x^3 + 2) \end{aligned}$$

weil Λ_1 modulo p verschwindet. Den Eigenwert $\Lambda_1 := 5 \cdot \lambda_1 \in R_1$ erhält man durch:

$$\lambda_1 := -\frac{C_{x^4}(\delta(F_1,0))}{H(E)} = -\frac{4}{2} = 3$$

Das Ω-Hindernis ist damit gegeben durch:

$$\begin{aligned} \delta := \delta(F_1) &= \delta(F_1, 0) + \lambda_1 \cdot f^{\frac{p-1}{2}} \\ &= x^{10} + 3x^8 + x^7 + 4x^6 + 2x^5 + 3x^2 + 2x + 4 \end{aligned}$$

Beispiel: Berechnung einer Ω-Liftung
Eine Stammfunktion von $\delta(F_1)$ ist wohldefiniert:

$$\int \delta = x^{11} + 2x^9 + 2x^8 + 2x^7 + 2x^6 + x^3 + x^2 + 4x$$

Betrachte nun die Äquivalenz aus dem Existenzkriterium einer Ω-Liftung:

$$\int \delta \equiv \xi^p \mod f^{\frac{p+1}{2}}$$

Durch den Koeffizientenvergleich bis zum Grad $\deg_x f^{\frac{p+1}{2}} = 3\frac{p+1}{2}$ finden wir eine Lösung: $\xi = 3x^2 + x + 3$. Damit haben wir die Existenz einer kleinen Ω-Liftung des Frobenius über R_1 bewiesen.

Wir wählen das Parameterpaar:

$$\left(\alpha := \frac{\int \delta(F_1) - \xi^p}{2f^{\frac{p+1}{2}}} = 3x^2 + x + 2,\ \mu := 0\right)$$

und erhalten damit wir eine Ω-Liftung $\tilde{F}_1$:

$$\begin{aligned}\tilde{F}_1(x) &= x^5 + 5 * (\psi(x) + 2f^{\frac{p+1}{2}} \cdot \alpha) \\ &= x^5 + 5 \cdot (2x^{10} + 4x^7 + 4x^5 + 3x^4 + x^3 + x^2 + 2x) \\ \tilde{F}_1(y) &= y^5 + 5 * (\psi(y) + y \cdot f' \cdot \alpha) \\ &= y^5 + 5 \cdot y \cdot (3x^{11} + x^9 + 3x^8 + 3x^7 + 3x^5 + 4x^4 + 2x^2 + 4)\end{aligned}$$

auf den Koordinatenring $A_1 := R_1[x, y]/(y^2 - x^3 - x - 2)$, die eine lineare Operation auf $R_1\{\frac{dx}{y}\}$ mit dem Eigenwert 15 induziert.

Die Liftung $\tilde{F}_1$ ist nicht erweiterbar nach dem Satz 6.2.2, wegen dem nicht verschwindenden Koeffizient von $x^{2p-1} = x^9$ in

$$\delta_0(\tilde{F}_1) := \frac{-F_1'(x)+\Lambda_1 F_1(y)/y}{p^2} \text{ nicht verschwindet}$$

Beispiel: Parametrisierung aller kleinen Ω-Liftungen
Alle weiteren kleinen Ω-Liftungen von F erhält man für beliebige $\mu, \nu \in k[x]$ durch:

$$\begin{aligned}F_1(x) &:= \tilde{F}_1(x) + 5 \cdot f^p \cdot \nu^p + \mu^p \breve{\psi}_x \\ F_1(y) &:= \tilde{F}_1(x) + 5 \cdot y \cdot f'(p) \cdot \nu^p + \mu^p \breve{\psi}_y\end{aligned}$$

wobei μ der kleinen Liftung der definierenden Gleichung von A entspricht und $(\breve{\psi}_x, \breve{\psi}_y)$ folgende Lösung der Basisgleichung (s. 6.1.8) ist:

$$\begin{aligned}\breve{\psi}_x &:= (3x^2 + x + 2)^5 \\ \breve{\psi}_x &:= y \cdot (2x^{11} + 4x^9 + 3x^8 + 2x^7 + 2x^6 + 3x^5 + 3x^4 + x^3 + 4x^2 + x + 1)\end{aligned}$$

Die in 5.4 über R_1 berechnete kanonische Liftung des Frobenius wird in diesem Raum durch das Paar $(\nu := 0,\ \mu := 1)$ parametrisiert und ist nach der Definition erweiterbar.

6.3 Grade der Ω-Liftungen und Anwendungen

In diesem Abschnitt beweisen wir die Schranken für die Grade der erweiterbaren Ω-Liftungen und zeigen wie man mit den erzielten Ergebnissen über Ω-Liftungen eine Verbesserung des projektiven Liftungsalgorithmus erhält.

Grade der erweiterbaren Ω-Liftungen
Die Ω-Verträglichkeitsbedingung engt den Raum der Ω-Liftungen stark ein; so erfüllten die Grade $\deg_x F_n(x)$ und $\deg_x F_n(y)$ einer erweiterbaren Ω-Liftung F_n folgende, sehr restriktive Schranken:

Theorem 6.3.1. *Sei F_n eine erweiterbare Ω-Liftung des Frobenius über R_n, dann gilt:*

$$\deg_x F_n(x) \leq p + n\tfrac{p-1}{2}$$
$$\deg_x F_n(y) \leq 3\tfrac{p-1}{2} + n\tfrac{p-1}{2}$$

Beweis:
Wir führen einen induktiven Beweis, mit der Basis für $n = 0$

$$\deg_x x^p = p \text{ und } \deg_x y^p = \deg_x y f^{\frac{p-1}{2}} = 3\tfrac{p-1}{2}$$

Betrachte die Ω-Verträglichkeitsbedingung an F_n:

$$0 = \Lambda_n \tfrac{F_n(y)}{y} - F_n'(x) \Rightarrow \deg_x F_n(x)' = \deg_x F_{n-1}(y)$$

Den weiteren Beweis zerlegen wir in 2 folgende Fälle:

1. $\deg_x F_n(x) = \deg_x F_{n-1}(y) + 1$
2. $\deg_x F_n(x) > \deg_x F_{n-1}(y) + 1$

und zeigen dass im ersten Fall die angegebenen Schranken erfüllt sind, und der zweite Fall zum Widerspruch mit der Erweiterbarkeit von F_n führt.

Fall 1:
Nach der Induktionsvoraussetzung erhalten wir unmittelbar:

$$\deg_x F_n(x) = \deg_x F_{n-1}(y) + 1 \leq 3\tfrac{p-1}{2} + (n-1)\tfrac{p-1}{2} + 1 = p + n\tfrac{p-1}{2}$$

Betrachte die induzierende Derivation ψ_n mit $F_n := F_{n-1} + p^n * \psi_n$ und nehme an, dass

$$\deg \psi_n(y) > 3\tfrac{p-1}{2} + n\tfrac{p-1}{2} \text{ gilt.}$$

Daraus folgt:

$$\begin{aligned}\deg_x F_n(y^2) &= \deg_x \left[F_{n-1}^2(y) + p^n * (y^p \psi_n(y))\right] = \deg_x y^p \psi_n(y) \\ &= \deg_x f^{\frac{p+1}{2}} \tfrac{\psi_n(y)}{y} > 3\tfrac{p+1}{2} + 3\tfrac{p-1}{2} + n\tfrac{p-1}{2} = 3p + n\tfrac{p-1}{2},\end{aligned}$$

wobei die zweite Gleichung nach den Voraussetzungen über die Grade und dem Lemma A.4 gilt:

$$\begin{aligned}\deg_x F_{n-1}(y)^2 &= \deg_x f \left(\tfrac{F_{n-1}(y)}{y}\right)^2 \\ &\leq 3 + 3\tfrac{p-1}{2} + (n-1)\tfrac{p-1}{2} + 3\tfrac{p-1}{2} = 3p + (n-1)\tfrac{p-1}{2} \\ &\leq \deg_x y^p \psi_n(y)\end{aligned}$$

Auf der anderen Seite folgt aus dem Lemma A.4 und den Induktionsvoraussetzungen die Schranke:

$$\deg_x F_n(x^3) = 3p + n\tfrac{p-1}{2}$$

Dies führt allerdings zum Widerspruch mit der Verträglichkeit der Liftung mit der definierenden Gleichung, wegen

$$F_n(y^2 - \tilde{f}(x)) = 0 \Rightarrow \deg_x F_n(y^2) = \deg_x F_n(x^3)$$

Damit ist der erste Fall bewiesen. □.

Fall 2:
In diesem Fall existiert ein $\gamma \in k[x]$ mit $p \cdot \deg_x(\gamma) > \deg_x F_{n-1}(y)$, das folgende Bedingungen erfüllt:

$$F_n(x) = p^n * \gamma^p + \int F_{n-1}(y)$$

Der Koeffizient von $x^{p \deg_x \gamma - 1}$ in $\delta_0(F_n)$ ist dann ungleich 0 nach dem folgenden Lemma 6.3.2. Daraus folgern wir mit dem Satz 6.2.2, dass F_n nicht erweiterbar ist, was im Widerspruch zu den Voraussetzungen steht. □.

Lemma 6.3.2. *Seien F_n und $\tilde{F}_n$ zwei kleine Ω-Liftungen von F_{n-1}, wobei $\tilde{F}_n$ durch $(\alpha, \mu)_{F_n}$ parametrisiert ist. Die zugehörigen Parameterfunktion erfüllen dann folgende Bedingung:*

$$C_{px^{\varpi-1}}(\Delta'_x(\alpha,\mu)) \neq C_{px^{\varpi-1}}\left(\Lambda_1 \tfrac{\Delta_y(\alpha,\mu)}{y}\right) \text{ für } \varpi := \deg_x \Delta_x(\alpha,\mu),$$

wobei $\Lambda_1 \in R_1$ die Reduktion des Eigenwerts Λ_n modulo p^2 ist.

Beweis:
Nach dem Lemma 6.1.7 ist $\Delta_x(\alpha,\mu) = \gamma^p$ eine p-Potenz in $k[x]$ und folglich ist ϖ durch p teilbar. Es gilt:

$$C_{px^{\varpi-1}}(\Delta'_x(\alpha,\mu)) = \tfrac{\varpi}{p} C_{x^{\varpi}}(\Delta_x(\alpha,\mu) =: K_x$$

wobei K_x der leitende Koeffizient von $\Delta_x(\alpha,\mu)$ ist. In diesem Fall ist der leitende Koeffizient des Parameters α gleich $\frac{H(E)}{2} \cdot K_x$ wegen:

$$\alpha = \frac{\Delta_x(\alpha,0)}{2f^{\frac{p+1}{2}}} = \frac{f^{\frac{p-1}{2}}\Delta_x(\alpha,0)}{2f^p}$$

Auf der anderen Seite gilt:

$$\begin{aligned} C_{px^{\varpi-1}}\left(\Lambda_1 \tfrac{\Delta_y(\alpha,\mu)}{y}\right) &= C_{px^{\varpi-1}}\left(p \cdot \lambda_1 \cdot f'(x) \cdot \alpha\right) \\ &= \lambda_1 \cdot 3^p \cdot K_x \cdot \tfrac{H(E)}{2} = \tfrac{3}{2} K_x \end{aligned}$$

wobei die letzte Gleichheit aus 6.1.3 folgt. Die Behauptung des Satzes folgt

nun wegen $\frac{3}{2} \neq 1$ $\square$.

Nach dem Theorem 6.2.4 wissen wir, dass es nur wenige (und auf jedem Fall endlich viele) erweiterbare Ω-Liftungen des Frobenius über einem Ring R_n gibt. Eine davon ist auf jedem Fall die Reduktion der kanonischen Liftung des Frobenius modulo p^n.

Die kanonische Liftung des Frobenius nach Charakteristik 0 ist algebraisch und folglich wird es bei der induktiven Berechnung dieser Liftung einen „terminalen“ Schritt geben, ab dem die Liftung sich nicht mehr ändert. Dieser Schritt, tritt allerdings i.A. bei einer sehr hohen p-adische Genauigkeit, die z.B. die für das Punktezählen notwendige Genauigkeit deutlich übersteigt.

Bis zu diesem „terminalen“ Schritt entsprechen die x-Grade der Bilder der kanonischen Liftung des Frobenius oft genau den angegebenen Schranken. z.B. bei der Liftung der Kurve $E : y^2 = x^3 + x + 2/F_5^{10}$ über R_{60} wird die Schranke für $\deg_x F_n(x)$ in 48 und die $\deg_x F_n(x)$ in 36 Schritten genau erreicht, wobei die Abweichung des x-Grades von der Schranke stets $\leq 5 = p$ ist.

Verbesserung des projektiven Liftungsalgorithmus
In dem kleinen Schritt des Liftungsalgorithmus (aus 5.4) haben wir zufällige affinen Liftungen als Basis der Parametrisierungen gewählt. Als nächstes wählen wir eine Ω-Liftung auf der Karte A als Basis und zeigen wie man dadurch den Algorithmus beschleunigen kann.

Lemma 6.3.3. *Sei (E_{n-1}, F_A, F_B) die kanonische Liftung des Frobenius auf einer ordinären elliptischen Kurve E über R_{n-1}. Weiterhin seien $(\hat{A}, \hat{F}_A)$ eine Ω-affine Liftung von (A, F_A), $(\tilde{B}, \tilde{F}_B)$ eine affine Liftung von (B, F_B) und η das Hindernis zu deren Verklebung. Dann existiert ein $u \in k[t^{-1}]$, für die*

$$\deg_{t^{-1}} \eta(t) = \deg_{t^{-1}} u^p \quad \textit{gilt.}$$

Beweis:
Sei (α, μ) das Paar, das die kanonische Liftung $(E_n, \tilde{F}_A, \tilde{F}_B)$ auf der Karte A parametrisiert. Die Liftung $\tilde{F}_A$ ist Ω-verträglich und folglich existiert ein solches $\gamma \in k[x]$, dass $\Delta_x(\alpha, \mu) = \gamma^p$ gilt. Die Behauptung des Lemmas folgt nun wegen der ersten Fortsetzbarkeitsbedingung an (α, μ):

$$\deg_{t^{-1}} \left[-\eta(t) - t^{2p}\Delta_x(\alpha, \mu)\right] = \deg_{t^{-1}} \left[-\eta(t) - (t^2\gamma)^p\right] = 0$$

$\square$.

Nach diesem Lemma können wir die Auflösung der ersten Fortsetzungsbedingung um den Faktor p beschleunigen. In der Tat, bei der Wahl einer Ω-verträglichen Liftungen als Basis der Parametrisierung auf A, muss man den Koeffizientenvergleich nur noch über die p-Potenzen durchführen. Diese Verbesserung illustrieren wir am Beispiel des 60-ten kleinen Liftungsschrittes zur Berechnung der kanonischen Liftung für die elliptische Kurve $E:\ y^2 = x^3 + x + 2$ über R_{61}:

Wählt man auf beiden Karten die x-minimalen affinen Liftungen (s. 4.3), dann ist der Grad des entstehenden Hindernisses $\eta(t)$ gleich 126. Also muss man in diesem Fall ein $\alpha \in k[x]$ mit $\deg \alpha = 129$ aus der ersten Fortsetzbarkeitsbedingung (z.B. durch einen Koeffizientenvegleich bis zum Grad 129) berechnen. Wählt man jedoch eine Ω-affine Liftung auf der Karte A, dann ist der Grad von $\eta(t)$ zwar mit 125 ähnlich hoch, wir müssen jedoch den Koeffizientenvergleich nur über die p-Potenzen führen, um ein γ vom Grad 25 zu finden.

6.4 Ausblick

Dieser Abschnitt skizziert weitere Anwendungsmöglichkeiten der entwickelten Methoden. Wir diskutierten die Möglichkeiten der weiteren Optimierung affiner Liftungen des Frobenius für den Reduktionsschritt auf der MW-Kohomologie, die Verallgemeinerung der projektiven Liftungsmethoden, sowie die Verklebung der Differentialen auf den Durchschnitten affiner Karten.

Optimierung der Liftung für das Punktezählalgorithmen
Im Kapitel 4 haben wir die x-minimale Liftung durch die Minimierung des x-Grades von $F_n(x)$ konstruiert und deren Anwendung für die Beschleunigung des Reduktionsschrittes auf der MW-Kohomologie gezeigt. Man könnte allerdings bei jedem Liftungsschritt, eine solche kleine Liftung suchen, bei der die Anzahl der notwendigen Reduktionsschritte minimal wird.

Es stellt sich die Frage insbesondere die Frage, wie weit man die Anzahl der Reduktionsschritten minimieren kann. Die Antwort darauf hängt stark ab von dem Darstellungsraum des Frobenius. So induziert die kanonische Liftung des Frobenius auf elliptischen Kurven eine Operation auf holomorphen Differentialen bei der man keine Reduktion benötigt.

Bei den hyperelliptischen Kurven ($g > 1$) hat man allerdings keine projektiven Liftungen des Frobeniusmorphismus (s. 6.4.1). Bei der Wahl der Basis $\{\frac{x^i dx}{y}\}$ der MW-Kohomologie auf affinen Kurven hängt die Anzahl der notwendigen Reduktionen von den y-Gesamtgraden der Terme:

$$\frac{F_n(x)^i DF_n(x)}{F_n(y)} \text{ für } 0 \leq i \leq 2g,$$

die nicht gleichzeitig verschwinden können. In Analogie zu elliptischen Kurven könnte man jedoch versuchen, solche Liftungen F_n zu finden, so dass diese Brüche teilweise oder für einige i vollständig gekürzt werden und dadurch der Gesamtgrad dieser Brüche möglichst klein wird. Wir vermuten, dass man auf diese Weise die Berechnung der Operation auf den Differentialen weiter beschleunigen könnte.

Liftungen der projektiven Morphismen:
Im Kapitel 5 haben wir eine Überdeckung durch zwei affine Karten betrachtet, die entwickelten Methoden sind allerdings auf beliebige Überdeckungen leicht verallgemeinerbar. Also ist es möglich die Liftungen des Frobenius auf allgemeineren projektiven Varietäten zu betrachten. Das Problem besteht allerdings darin, solche Varietäten zu finden, auf denen die in 2.2.1 angegebenen Obstruktionen zur Liftbarkeit verschwinden.

Satz 6.4.1. *Sei C eine projektive Kurven vom Geschlecht g>1, dann existiert keine Liftung des Frobeniusmorphismus auf C über einem Quotientenring R_n.*

Beweis:
Angenommen es existiert eine Liftung $F_1 : C_1^\sigma \to C_1$ von F über R_1, dann verschwinden die kleinen Obstruktionsräume zur Liftbarkeit (s. 2.1) und folglich kann man eine formale Liftung $\tilde{F}$ von F nach Charakteristik 0 induktiv konstruieren. Diese formale Liftung wäre aber algebraisch wegen der Kompaktheit der projektiven Räume (s. [GAGA])

Die Behauptung des Lemmas folgt nun aus der Hurwitz-Formel angewendet auf die Liftung $\tilde{F} : \tilde{C}^\sigma \to \tilde{C}$

$$2g - 2 = p(2g - 2) + \deg R, \text{ wobei } \deg R \geq 0 \text{ gilt.}$$

□.

Bei ordinären abelschen (bzw. jakobischen) Varietäten existiert stets eine kanonische Liftung der Varietät und eine eindeutige Liftung des Frobeniusmorphismus darauf. Es ist möglich, die deformationstheoretischen Liftungs-

methoden zur Berechung der kanonischen Liftung solcher abelschen Varietäten zu verwenden, für die eine explizite affine Überdeckung bekannt ist. Allerdings gibt es inzwischen viel geeigneter Methoden dazu, wie z.B. die Liftung der Theta-Funktionen in [Carls].

Weiterhin ist es wie im affinen Fall möglich, andere Morphismen als den Frobeniusmorphismus zu betrachten, denn die verwendeten Methoden nutzen keine besonderen Eigenschaften des Frobeniusmorphismus.

Verklebbarkeit der Differentialen:
Die Liftungen des Frobeniusmorphismus auf einer elliptischen Kurve induzieren Endomorphismen auf den holomorphen Differentialen. Dabei induzieren die affinen Liftungen $\tilde{F}_A$ und $\tilde{F}_B$ auf der Karten A und B lineare Operation auf den Moduln $R_n\{\frac{dx}{y}\}$, bzw. $R_n\{\frac{dt}{s}\}$, deren Eigenwerte sich verkleben.

Betrachte zunächst die Verklebung der Basisdifferentialen:

$$\phi(\tfrac{dx}{y}) = \tfrac{d\phi(t)}{\phi(y)} = \tfrac{dt^{-1}}{st^{-2}} = -\tfrac{dt}{s}$$

Die Verklebung der Differentialen erfolgt durch:

$$\phi(\tilde{F}_A^*(\tfrac{dx}{y})) = \phi\left(\tfrac{\tilde{F}'_A(x)dx}{\tilde{F}_A(y)}\right) = \phi(\Lambda_A \tfrac{dx}{y}) = -\Lambda_B \tfrac{dt}{s} = \tfrac{\tilde{F}'_B(t)dt}{\tilde{F}_B(s)} = \tilde{F}_B^*(\tfrac{ds}{t})$$

Diese Verklebbarkeit der Differentiale und der induzierten Operation kann man auch auf andere Varietäten verallgemeinern, für die es keine projektiven Liftungen des Frobenius gibt, z.B. auf hyperelliptische Kurven (g>1).

Betrachte eine affine Überdeckung der (projektiven) hyperelliptischen Kurve C (wie in 5.1) durch

$$C_A := \{(x,y)|y^2 = f_n(x)\} \text{ und } C_B := \{(s,t)|s^2 = h_n(t)\}$$

die sich auf den Durchschnitten mit dem Isomorphismus ϕ verkleben:

$$\phi(x) := t^{-1} \text{ und } \phi(y) := s \cdot t^{-g-1}$$

Die Basisvektoren der Differentialen verkleben sich dann durch:

$$\phi(\tfrac{x^i dx}{y}) = \tfrac{t^{-i}d\phi(t)}{\phi(y)} = \tfrac{t^{-i}dt^{-1}}{st^{-g-1}} = -\tfrac{t^{g-1-i}dt}{s} \text{ für alle } 0 \leq i \leq g-1.$$

Wir vermuten, dass es solche affine Liftungen F_A und F_B gibt, die folgende Verklebungsbedindung an Differentiale für jedes $0 \leq i \leq g-1$ erfüllen:

$$\phi\left(\tfrac{\tilde{F}_A(x^i)\tilde{F}'_A(x)dx}{\tilde{F}_A(y)}\right) = \tfrac{\tilde{F}_B(t^{g-1-i})\tilde{F}'_B(t)dt}{\tilde{F}_B(s)},$$

Für den elliptischen Fall $g = 1$ sind solche Liftungen durch die Einschränkungen der kanonischen Liftung des Frobenius gegeben.

Eine solche Liftung des Frobenius auf den affinen Karten könnte man dann anwenden, um eine Operation des Frobenius auf den holomorphen Differentialen der hyperelliptischen Kurve, bzw. auf den dazu isomorphen holomorphen Differentialen der jakobischen Varietät zu bestimmen.

Anhang A

p-adische Ringe

In diesem Anhang geben wir eine kurze Einführung in die p-adischen Zahlen und deren Erweiterungen, und fassen anschließend einige Eigenschaften der p-adischen Quotientenringe zusammen. Für eine ausführliche Beschreibung der p-adischen Zahlen verweisen wir auf [Kobl], sowie auf [FC$^+$] für die algorithmische Komponente.

Konstruktion der p-adischen Ringe:
Die Konstruktion der p-adischen Ringe beginnen wir mit der Definition einer, für eine festgewählte Primzahl $p \in N$, definierten *nichtarchimedischen* Norm auf $\mathbb{Q}$. Eine solche Norm soll die Ungleichung:

$$|a + b| \geq \max\{|a|, |b|\}$$

anstelle der üblichen Dreiecksungleichung erfüllen.

Die Abbildung $\mathrm{ord}_p : \mathbb{Z} \to \mathbb{N}$ definieren wir durch:

$$\mathrm{ord}_p(a) := \max\{i \in \mathbb{N} |\ \ a \equiv 0 \bmod p^i\} \text{ für ein } p \neq a \in \mathbb{Z}$$

und erweitern es auf $\mathbb{Q}$ durch:

$$\mathrm{ord}_p(\tfrac{a}{b}) := \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$$

Mit der zusätzlichen Eigenschaft $\mathrm{ord}_p(0) := \infty$ definiert die Abbildung

$$|c|_p := p^{-\mathrm{ord}_p(c)}$$

eine nichtarhimedische Norm auf $\mathbb{Q}$.

Unter dem *Körper $\mathbb{Q}_p$ der p-adischen Zahlen* verstehen wir die Komplettierung von $\mathbb{Q}$ bezüglich der p-adischen Norm $|.|_p$. Den Ganzheitsring dieses

Körpers bezeichnen wir mit $\mathbb{Z}_p$ und nennen den *Ring der ganzen p-adischen Zahlen*. Dieser Ring $\mathbb{Z}_p$ ist ein lokaler diskreter Bewertungsring mit dem maximalen Ideal $M = \{x \in \mathbb{Z}_p | \ \text{ord}_p(x) > 0\}$, der Bewertung ord_p und dem Residuenkörper $\mathbb{Z}_p/M \cong \mathbb{F}_p$.

Für jedes $a \in \mathbb{F}_p$ existiert eine eindeutige *p-adische Entwicklung*:

$$a = \sum_{i=\text{ord}_p(a)}^{\infty} p^i a_i,$$

wobei $\{a_i\}$ ganze Zahlen mit $0 \leq a_i \leq p-1$ sind. Also entsprechen die p-adischen Zahlen den formalen Potenzreihen in p.

Als nächstes betrachten wir die (eindeutige) unverzweigte endliche Körpererweiterung des Körpers $\mathbb{Q}_p$ von Grad d, die wir mit $\mathbb{Q}_q$ für $q := p^d$ bezeichnen. Betrachte die Dastellung des endlichen Körper $\mathbb{F}_q := \mathbb{F}_p[x]/(f)$ als Quotient des Polynomrings modulo einem irreduziblen monischen Polynom vom Grad d. Einen ähnlichen Isomorphismus gibt es auch für den Körper $\mathbb{Q}_q$:

$$\mathbb{Q}_q \cong \mathbb{Q}_p[t]/\tilde{f}$$

dabei ist $\tilde{f}$ ein monisches Polynom, deren Reduktion modulo p gleich f ist. Folglich hat jedes $h \in \mathbb{Z}_q$ eine eindeutige Zerlegung:

$$h = \sum_{i=0}^{d-1} a_i x^i \ \text{ für bestimmte } p\text{-adische Zahlen } a_i,$$

die eine Erweiterung der p-adischen Bewertung auf $\mathbb{Q}_q$ ermöglicht:

$$\text{ord}_p(h) := \max\{\text{ord}_p(a_i)\}$$

Den diskreten Bewertungsring von $\mathbb{Q}_q$ bezeichnen wir mit $\mathbb{Z}_q$. Dieser Ring $\mathbb{Z}_q$ ist isomorph zu dem Wittvektorenring $W(\mathbb{F}_q)$. Insbesondere impliziert die Unverzweigheit des Körpers $\mathbb{Q}_q$ eine Isomorphie zwischen dem Residuenkörper $\mathbb{Z}_q/(M := \mathbb{Z}_q \setminus pZ_q)$ und dem endlichen Körper $\mathbb{F}_q$.

p-adische Quotientenringe:
In der Praxis werden die Berechnungen in den p-adischen Ringen mit einer endlichen p-adischen Genauigkeit durchgeführt. Deswegen betrachten wir in der Arbeit die Quotienten $R_n := W(k)/(p^{n+1})$ des Wittvektorenringes über einen perfekten Körper in positiver Charakteristik, die wir als *p-adische Quotientenringe* referenzieren. In dem (für diese Arbeit wichtigsten) Fall eines endlichen Körpers, sind diese Ringe isomorph zu den Ringen $\mathbb{Z}_q/(p^{n+1})$.

Die Zerlegung der Elemente aus $\mathbb{Q}_q$ in eine $\mathbb{Q}_p$-lineare Kombination, zusammen mir der p-adischen Darstellung für Elemente aus $\mathbb{Q}_p$ induziert folgende eindeutige *p-adische Darstellung* für ein $h \in \mathbb{Z}_q/(p^{n+1})$

$$h = \sum_{i=0}^{d-1} \left(\sum_{j=0}^{n} p^j a_{ij} \right) \cdot x^i = \sum_{j=0}^{n} p^j \cdot \left(\sum_{i=0}^{d-1} a_{ij} x^i \right)$$

für bestimmte $\{0 \leq a_{ij} \leq p-1 \in \mathbb{Z}\}$. Die Terme $\sum_{i=0}^{d-1} a_{ij} x^i$ entsprechen dabei eineindeutig den Elementen

$$\sum_{i=0}^{d-1} a_{ij} \cdot 1_{\mathbb{F}_p} \cdot x^i \quad \text{von } \mathbb{F}_q := \mathbb{F}_p[x]/(f)$$

Also ist jedes $h \in \mathbb{Z}_q/(p^{n+1})$ eindeutig bestimmt durch einen n-Tupel der $\mathbb{F}_q$-Elemente und umgekehrt liefert jedes solches Tupel $\{h_j\}_{0<j<n}$ einen Element von $\mathbb{Z}_q/(p^{n+1})$, den wir mit

$$\sum_{j=0}^{n} p^j * h_j \quad \text{bezeichnen,}$$

wobei der Ausdruck $p^j * h_j$ in $p^n\mathbb{Z}_q/(p^{n+1}) \subset \mathbb{Z}_q/(p^{n+1})$ definiert ist. Für die Elemente der Quotientenringe R_n verwenden wir eine ähnliche p-adische Darstellung durch einen Tupel der Elemente des Körpers k.

Die p-adischen Quotientenringe bilden ein projektives System, wobei die Projektion $\pi_n : R_m \to R_n$ für $(m > n)$ durch die Reduktion modulo p^{n+1} gegeben ist:

$$\pi_n \left(\sum_{i=0}^{m} p^i * a_i \right) = \sum_{i=0}^{n} p^i * a_i$$

Definition A.1 *Sei a ein Element aus R_n. Man nennt $\tilde{a} \in R_m$* ***eine Liftung*** *von a nach R_m, falls $\pi_n(\tilde{a}) = a$ gilt. Unter der* ***trivialen Liftung*** *von $a = \sum_{i=0}^{n} p^i * a_i \in R_n$ nach R_m verstehen wir eine Liftung $\tilde{a} \in R_m$ von a, in deren p-adischen Darstellung Koeffizienten a_i für alle $i > n$ verschwinden:*

$$a = \sum_{i=0}^{n} p^i * a_i + \sum_{j=n+1}^{m} p^j * 0 = \sum_{i=0}^{n} p^i * a_i$$

Die triviale Liftung von a nach R_m bezeichnen wir mit $(a)_m$.

Die gegebenen Definitionen der Liftungen, trivialen Liftungen und der p-adischen Darstellung kann man auf die über den Quoteintenringen R_n auf eine natürliche Weise erweitern.

Im Rest des Anhangs fassen wir einige Bemerkungen über den Liftungen von R_n nach R_m zusammen:

Lemma A.2 *Sei $a \in R_m$, mit $\pi_n(a) = 0$. Dann existiert ein eindeutiges $b \in R_{m-n}$, das die Gleichung $a = p^n \cdot (b)_m$ erfüllt.*

Beweis:
Betrachte die p-adische Entwicklung von a:

$$a = \sum_{i=0}^{m} p^i * a_i$$

Nach der Voraussetzung verschwinden alle a_i für $i < n$ und folglich erfüllt ein

$$b := \sum_{i=0}^{m-n} p^i * b_i \quad \in R_{m-n}$$

die Bedingung $a = p^n \cdot (b)_m$ genau dann, wenn $b_i = a_{i+n}$ gilt. Also ist das gesuchte b eindeutig gegeben durch:

$$b := \sum_{i=0}^{m-n} p^i * a_{i+n} \quad \in R_{m-n}$$

□.

Korollar A.3 *Seien $\hat{a}, \tilde{a} \in R_m$ zwei Liftungen von $a \in R_n$, dann existiert ein eindeutiges $b \in R_{m-n}$, so daß $p^n\,(b)_n = \hat{a} - \tilde{a}$.*

Für die Abschätzungen der Grade der Polynome in p-adischen Quotientenringen in den Abschnitten 4.3, 4.4. verwenden wir folgende Bemerkung:

Lemma A.4 *Seien $g, h \in R_n[x_1, \ldots, x_m]$ zwei beliebige Polynome mit folgenden p-adischen Darstellungen:*

$$g = \sum_{0}^{n} p^i * g_i \text{ bzw. } h = \sum_{0}^{n} p^i * h_i \quad \text{mit } h_i, g_i \in k[x_1, \ldots, x_m]$$

Dann gilt für jedes x_l:

$$\deg_{x_l}(g \cdot h) \leq \max\{\deg_{x_l}(g_i) + \deg_{x_l}(h_j) |\, i + j \leq n\}.$$

Beweis:
Zerlege das Produkt $g \cdot h$ in zwei Summen

$$g \cdot h = \sum_{0}^{n} p^i(g_i) * \sum p^j(h_j) = \sum_{i+j \leq n} p^{i+j} * (g_i \cdot h_j) + \sum_{i+j > n} p^{i+j} * g_i \cdot h_j$$

Die Aussage des Lemmas gilt, da die zweite Summe modulo p^{n+1} verschwindet. □.

Literaturverzeichnis

[Car]: R. Carls: *Generalized AGM -Sequences and approximation of canonical lifts*, PhD Thesis, Universiteit Leiden (2003)

[CF$^+$]: H. Cohen, G. Frey (editors): *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman Hall (2005)

[DH]: W. Diffie, M.E. Hellman: *New directions in crptography*, IEEE Trans. Information Theory, IT-22(6):644-654 (1976)

[Gerk]: R. Gerkmann: *The p-adic cohomologie of varieties over finite fieds and applications on computation of zeta functions*, PhD Thesis, Universität Essen-Duisburg (2003)

[Harr]: J. Harris, I. Morrison *Moduli of Curves*, Springer Verlag (1991); Graduate Texts in Mathematics 187, insb. Chapter 3d.

[Hart]: R. Hartshorne: *Algebraic Geometry*, Springer-Verlag (1977); Graduate Texts in Mathematics 52, insb. Appendix C.

[Harv]: D. Harvey: *Kedlaya's Algorithm in Larger Characteristic*, Int. Math. Res. Notices (2007)

[Kedl]: K.S. Kedlaya: *Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology*, J. Ramanujan Math. Soc. (2001), 16(4):323-338

[Kobl]: N. Koblithz: *p-adic numbers, p-adic analysis and zeta-functions*, Springer-Verlag (1984); Graduates Text in Mathematics 58

[Liu]: Q. Liu: *Algebraic Geometry and Arithmetic Curves*, Oxford Science Publications (2002)

[LST]: J. Lubin, J.-P. Serre, J. Tate: *Elliptic curves and formal groups*, Woods Hole Summer Institute, 1964, verfügbar unter
http://www.ma.utexas.edu/users/voloch/lst.html

[LW1]: A.G.B. Lauder, D. Wan: *Computing zeta functions of Artin-Schreier curves over finite fields*, London Math. Soc. JCM 5 (2002) 34-55.

[LW2]: A.G.B. Lauder, D. Wan: *Counting points on varieties over finite fields of small characteristic* in J.P. Buhler, P. Stevenhagen (editors), Algorithmic Number Theory: *Lattices, Number Fields, Curves and Cryptography*, verfügbar unter http://web.comlab.ox.ac.uk/oucl/work/alan.lauder/

[Mat1]: H.Matsumura *Commutative Algebra*, W. A. Benjamin (1970)

[Mat2]: H.Matsumura *Commutative Ring Theory*, Cambridge University Press (1989)

[MW]: P. Monsky, G. Washnitzer: *Formal Cohomology* I- III, Ann. of Math. (2) 88 (1968), 181-238, Ann. of Math. (2) 93 (1971), 315-343.

[Oort]: F.Oort *Lifting algebraic curves, abelian varieties and their endomorphisms to characteristic zero*, Proceed. Sympos. Pure Math. 46, AMS (1987), p. 165- 195

[Sat]: T. Satoh: *The canonical lift of an ordinary elliptic curve over a finite field and its point counting*, in J. Ramanujan Math. Soc. 15, (2000) , pp 247-270

[Schl]: M. Schlessinger: *Functors of Artin Rings*, Transactions of the American Mathematical Society, Vol. 130, No. 2 (Feb., 1968), pp. 208-222

[Silv1]: J.H. Silverman: *The Arithmetic of Elliptic Curves*, Springer-Verlag (1986); Graduate Texts in Mathematics 102

[Silv2]: J.H. Silverman: *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer-Verlag (1991); Graduate Texts in Mathematics 151

[Sern]: E. Sernesi: *An overview of classical deformation theory*, verfügbar unter http://www.iasbs.ac.ir/faculty/varsaie/sernesi.pdf

[Srin]: V. Mehta, V. Srinivas *Varieties in positive characteristic with trivial tangent bundle*, (Appendix *Canonical Liftings*), Compositio Mathematica 64 no. 2 , (1987), pp. 191-212

[Serr]: J.P. Serre, *Zeta and L functions*, in Atihmetical Algebraic Geometry Harper & Row (1965)

[Verk]: F. Vercauteren: *Computing Zeta Functions of Curves over Finite Fields*. PhD thesis, Katholieke Universiteit Leuven (2003).

[Weil]: A. Weil, *Sur les Courbes Algébriques et les Variétés qui s'en Déduisent*. Paris: Hermann (1948)

[ZS]: O.Zariski, P. Samuel *Commutative Algebra*, Springer Verlag (1975)