Obere Schranken für die Punktanzahl von Kurven über endlichen Körpern

Diplomarbeit

von

Angelika Köhnlein

Betreuer: Prof. Dr. Norbert Schappacher

Technische Universität Darmstadt
Fachbereich Mathematik

4. Dezember 2003

Inhaltsverzeichnis

1 Einleitung

Wie viele Punkte können auf einer nichtsingulären projektiven Kurve von Geschlecht g über einem endlichen Körper mit q Elementen höchstens liegen?

Noch gibt es auf diese Frage keine allgemeingültige Antwort. Einige Fälle wurden schon gelöst, doch in den meisten Fällen ist die aktuelle Forschung noch nicht am Ziel. Zwar gibt es allgemeingültige Abschätzungen für die Höchstanzahl, doch diese oberen Schranken werden häufig nicht von konkreten Kurven erreicht.

Es stellt sich also die Frage nach möglichst guten Obergrenzen für die Punktanzahl von Kurven über endlichen Körpern, die die allgemein bekannten Schranken verbessern. Die Frage hat natürlich schon rein theoretisch ihre Berechtigung. Doch ist sie auch für die Anwendung von Interesse, denn in der Kryptographie können, ähnlich wie elliptische Kurven, auch Kurven von höherem Geschlecht zur Verschlüsselung verwendet werden.

Zur Bewältigung dieser Aufgabe wurde eine Idee von Kristin Lauter aufgegriffen, die sie in ihrem Artikel [Lau00] vorstellt. Dort zeigt sie an einem Beispiel, wie durch Anwendung zweier Kriterien die Existenz von Kurven mit einer vorgegebenen Punktanzahl ausgeschlossen und die obere Schranke dadurch gesenkt werden kann.

Kristin Lauters Methode wurde im Rahmen dieser Arbeit verwendet, ihr Algorithmus für Kurven beliebigen Geschlechts über beliebigen endlichen Körpern verallgemeinert und ein Programm implementiert, das die Obergrenzen für die Punktanzahl untersucht.

Im Kapitel 2 werden die mathematischen Grundlagen der projektiven Kurven und der Funktionenkörper vorgestellt. Das Ziel ist es, die bekannte Abschätzung nach Weil vorzustellen und einen Beweis dafür anzugeben. Gleichzeitig wird hier die mathematische Sprache der folgenden Kapitel eingeführt.

Die Idee von Kristin Lauter, auf der die ganze Arbeit aufbaut, wird in Kapitel 3 vorgestellt und der Algorithmus, der diese Idee auf beliebige Kurven verallgemeinert, wird in Kapitel 4 hergeleitet und erklärt. Das fünfte Kapitel geht auf die Implementierung des Algorithmus ein; hier wird die Struktur des pari-Programmes beschrieben, das zur Umsetzung der Tests erstellt wurde.

Im sechsten Kapitel schließlich finden sich die Ergebnisse, die mit Hilfe dieses Programmes erzielt werden konnten. Zum besseren Vergleich stehen sie neben den jeweiligen Abschätzungen nach Weil und anderen bekannten Obergrenzen, wie sie bei [vdGvdV03] gesammelt sind.

Bedanken möchte ich mich bei Professor Norbert Schappacher, der mir diese interessante Aufgabe stellte und mich bei der Bearbeitung unterstützte. Seine wertvollen Hinweise und Ratschläge, wie auch sein kritisches Hinterfragen brachten mich weiter. Auch auf große Entfernung riss der Kontakt nicht ab.

Vielen Dank auch an Dr. Werner Nickel, der gute Tips gab, als bei der Implementierung Probleme auftauchten und immer am Stand der Forschung interessiert war.

Dank sagen möchte ich allen, die mich während der Arbeit ermutigten, meine Fragen anhörten und mitdachten, meinem Kommilitonen Niklas Niemann besonders auch fürs Korrekturlesen, Michael Herty für seine programmiertechnischen Hinweise, Stefan König und Benjamin Höfler für ihr Mitdenken bei allgemeinmathematischen Problemen, Alexander Klink für viele Tips im Umgang mit LaTeX und mit den Rechnern im Pool.

Auch allen Freunden und Bekannten, von denen viele mich im Gebet unterstützten, und nicht zuletzt meiner Familie, die immer für mich da war und viel Verständnis und Unterstützung für mich aufbrachte, herzlichen Dank!

Vor allem aber gilt mein Dank meinem Schöpfer und Herrn, ohne den ich nichts tun könnte.

2 Grundlagen

Die folgende Einführung in die Theorie der Bewertungen und Primdivisoren von Funktionenkörpern, ihre Verbindung zu projektiven Kurven und deren Zetafunktionen ist eng an [Gol03] gehalten.

2.1 Bewertungen

Definition 2.1. Bewertungsring
Sei K ein Körper. Ein Integritätsbereich $\mathcal{O} \subseteq K$ ist ein *Bewertungsring* von K, falls $\mathcal{O} \neq K$ und für alle $x \in K$ gilt $x \in \mathcal{O}$ oder $x^{-1} \in \mathcal{O}$.

Definition 2.2. Bewertung
Sei $\mathcal{O}$ ein Bewertungsring von K und sei $V = K^\times/\mathcal{O}^\times$, wobei $K^\times$ bzw. $\mathcal{O}^\times$ die Gruppe der Einheiten bezeichnet. Dann ist die durch $\mathcal{O}$ gegebene *Bewertung* die natürliche Abbildung $\nu : K^\times \to V$. Man nennt V die *Bewertungsgruppe* von $\mathcal{O}$ und schreibt die Gruppenoperation additiv. Wir setzen $\nu(0) := \infty$.

Zusätzlich ist auf V die folgende Ordnung definiert: Für $a\mathcal{O}^\times, b\mathcal{O}^\times \in V$ ist $a\mathcal{O}^\times \leq b\mathcal{O}^\times$, falls $a^{-1}b \in \mathcal{O}$. Diese Relation ist wohldefiniert und macht V zu einer total geordneten Gruppe, und es gilt

$$\nu(a+b) \geq \min\{\nu(a), \nu(b)\}.$$

Sei $P = \{x \in \mathcal{O} | \nu(x) > 0\}$. Dann ist P die Menge der nicht invertierbaren Elemente von $\mathcal{O}$. Es ist ein Ideal und daher das eindeutige maximale Ideal von $\mathcal{O}$. Jeder Bewertungsring ist also ein lokaler Ring[1] .

Sei umgekehrt ν ein nicht trivialer Homomorphismus von $K^\times$ in eine total geordnete additive Gruppe G mit der Eigenschaft $\nu(a+b) \geq \min\{\nu(a), \nu(b)\}$. Dann erhält man durch $\mathcal{O}_\nu := \{x \in K^\times | \nu(x) \geq 0\} \cup \{0\}$ einen Bewertungsring von K und ν ist isomorph zur zugehörigen Bewertung.

Definition 2.3. Restklassenkörper
Sei weiter $P_\nu := \{x \in K | \nu(x) > 0\}$ das maximale Ideal von $\mathcal{O}_\nu$.
Dann nennen wir $F_\nu := \mathcal{O}_\nu/P_\nu$ den *Restklassenkörper* von ν. Falls K einen Unterkörper k enthält und $\nu(x) = 0$ für alle $x \in k^\times$ ist, nennt man ν eine k-Bewertung von K. In diesem Fall ist F_ν eine Körpererweiterung von k.

[1] Ein Ring R heißt *lokal*, wenn er ein Ideal M hat, so dass $R \setminus M \subseteq R^\times$. Das ist äquivalent dazu, dass R ein eindeutiges maximales Ideal hat.

Definition 2.4. Diskrete Bewertung
Falls eine Bewertung ν vorliegt, deren Bewertungsgruppe unendlich und zyklisch ist, so nennt man ν eine *diskrete Bewertung* und ihren Bewertungsring $\mathcal{O}_\nu$ einen *diskreten Bewertungsring* . Man kann die Bewertungsgruppe einer diskreten Bewertung mit der Gruppe der ganzen Zahlen identifizieren. Ein Element von $\mathcal{O}_\nu$ mit Bewertung 1 nennt man *lokalen Parameter* in ν. Ein lokaler Parameter ist also gerade ein Erzeuger von P_ν.

Definition 2.5. Fortsetzung von Bewertungen
Angenommen, ν sei eine diskrete Bewertung von K und K' eine endliche Erweiterung von K. Dann gibt es einen Bewertungsring $\mathcal{O}'$ von K', der $\mathcal{O}_\nu$ enthält und dessen maximales Ideal P_ν enthält. Ist ν' die zugehörige Bewertung von K', so sagt man ν' *teilt* ν und schreibt $\nu'|\nu$.

Dann ist auch ν' diskret und es gibt eine positive ganze Zahl $e \leq |K' : K|$, so dass $\nu'|_K = e\nu$. Es gilt $e = |V' : V|$, wobei V' bzw. V die Bewertungsgrupen von ν' bzw. ν sind. Diese Zahl $e = e(\nu'|\nu)$ bezeichnet man als *Verzweigungsindex* von ν' über ν. Oft benutzt man auch die Schreibweise $e(P'|P)$. Für $e > 1$ nennt man P *verzweigt* in K'.

Falls $\nu'|\nu$, so ist der Restklassenkörper $F_{\nu'}$ eine Erweiterung des Restklassenkörpers F_ν von höchstens Grad $|K' : K|$. Den Grad dieser Erweiterung nennt man *Restklassengrad* von ν' über ν und bezeichnet ihn mit$f(\nu'|\nu)$ oder auch $f(P'|P)$.

2.2 Funktionenkörper

Definition 2.6. Funktionenkörper
Sei K eine endlich erzeugte Erweiterung von k von Transzendenzgrad eins. Dann ist $K/k(x)$ für ein beliebiges transzendentes Element $x \in K$ eine endliche Erweiterung. Sei außerdem k algebraisch abgeschlossen in K, das heißt, jedes über k algebraische Element in K liegt schon in k. Dann nennen wir K einen *Funktionenkörper* über k und den Körper k den *Konstantenkörper* und schreiben häufig K/k.

Definition 2.7. Trennvariable
Sei K/k ein Funktionenkörper und $x \in K$ transzendent über k so gewählt, dass $K/k(x)$ eine endliche, separable Erweiterung ist. Dann wird x als *Trennvariable* für K/k bezeichnet.

Bemerkung: Falls k perfekt ist, gibt es nach Theorem 2.21 immer eine Trennvariable für K/k.

Definition 2.8. Primdivisor
Ein *Primdivisor* von K ist das maximale Ideal P eines k-Bewertungsrings von K. Die zugehörige Bewertung wird mit ν_P, der Restklassenkörper mit F_P bezeichnet. Ist $x \in K$ und $\nu_P(x) \geq 0$, so bezeichnet $x(P)$ die Nebenklasse $x + P \in F_P$ und x wird *endlich in* P genannt. Ist $\nu_P(x) < 0$, so hat x einen Pol der Ordnung $-\nu_P(x)$ in P.

Da K ein Funktionenkörper ist, sind alle k-Bewertungen von K diskret. Mit $\mathbb{P}_K$ sei die Menge aller Primdivisoren von K bezeichnet.

Da für einen Primdivisor P der Restklassenkörper F_P eine endliche Erweiterung von k ist, ist die folgende Definition sinnvoll:

Definition 2.9. Grad eines Primdivisors
Der *Grad* von P ist $\deg(P) := |F_P : k|$.

Definition 2.10. Punkt
Einen Primdivisor von Grad eins bezeichnet man als *Punkt*.

Definition 2.11. Divisor
Sei $Div(K)$ die freie abelsche Gruppe, die von den Primdivisoren erzeugt wird. Ihre Elemente heißen *Divisoren*, sind also ganzzahlige formale Linearkombinationen von Primdivisoren, wie etwa

$$D := \sum_{P \in \mathbb{P}_K} d_P P.$$

Dabei haben nur endlich viele Primdivisoren einen Koeffizienten ungleich Null. Der *Grad* dieses Divisors ist

$$\deg(D) := \sum_P d_P \ \deg(P).$$

Für eine beliebige Bewertung ν_P ist $\nu_P(D) := d_P$, es gilt also $\nu_P(D) = 0$ für fast alle P.

Bemerkung: Ist $x \in K^\times$, so ist $\nu_P(x)$ nur für endlich viele Primdivisoren P verschieden von Null. Daher ist die folgende Definition sinnvoll:

Definition 2.12. Hauptdivisor
Für ein Element $x \in K^\times$ ist $[x] := \sum_P \nu_P(x) P$ der *Hauptdivisor* von x.

Definition 2.13. Divisorklassengruppe
Die Hauptdivisoren bilden eine Untergruppe der Divisoren. Die Quotientengruppe ist die *Divisorklassengruppe*. Zwei Divisoren heißen *linear äquivalent*, $D \sim D'$, falls $D - D' = [x]$ für irgendeinen Hauptdivisor $[x]$. Auf der

Gruppe der Divisoren gibt es eine partielle Ordnung. Es gilt $D \leq D'$, falls $\nu_P(D) \leq \nu_P(D')$ für alle Bewertungen ν_P. Ein Divisor D mit $D \geq 0$ wird *nichtnegativ* oder *effektiv* genannt.

Definition 2.14. $L_K(D)$
Sei K ein Funktionenkörper und D ein Divisor auf K. Dann setzt man

$$L_K(D) := \{x \in K^\times | [x] \geq -D\} \cup \{0\}.$$

Satz 2.15. *(nach [Gol03] Lemma 2.1.5. und Corollary 2.1.10.)*
Für jeden Divisor D ist $L_K(D)$ ein endlichdimensionaler k-Untervektorraum von K und falls D nichtnegativ ist, so gilt

$$\dim L_K(D) \leq \deg(D) + 1.$$

Definition 2.16. $\delta(D)$
Für einen Divisor D definiert man $\delta(D) := \deg(D) + 1 - \dim L_K(D)$.

Es interessiert, wie groß diese Differenz $\delta(D)$ werden kann.

Satz 2.17. (Riemann) *(nach [Gol03] Theorem 2.1.19.)*
Sei K ein Funktionenkörper. Dann gibt es positive ganze Zahlen N und g, die nur von K abhängen, so dass

1. *$\delta(D) \leq g$ für alle Divisoren D;*
2. *$\delta(D) = g$ für alle Divisoren, deren Grad mindestens N ist.*

Definition 2.18. Geschlecht
Sei K ein Funktionenkörper. Dann nennt man die ganze Zahl $g = g_K$ aus dem obigen Satz das *Geschlecht* von K.

Definition 2.19. Geometrischer Funktionenkörper
Einen Funktionenkörper K/k bezeichnet man als *geometrisch*, wenn für jede endliche Erweiterung k'/k die Struktur $k' \otimes_k K$ wieder ein Körper ist.

Lemma 2.20. *(nach [Gol03] Lemma 2.4.5.)*
Sei K ein Funktionenkörper über einem perfekten Grundkörper k.
Dann ist K geometrisch.

Theorem 2.21. *(nach [Gol03] Theorem 2.4.6.)*
Sei K/k ein geometrischer Funktionenkörper der Charakteristik $p > 0$.
Dann ist $|K : kK^p| = p$, und für jedes $x \in K$ gilt folgende Äquivalenz:

$$x \in kK^p \quad \Leftrightarrow \quad x \text{ ist keine Trennvariable für } K/k$$

2.3 Endliche Erweiterungen

Sei $K' \supseteq K$ ein Paar von Funktionenkörpern mit $|K' : K| < \infty$. Dabei sei k der Konstantenkörper von K und damit algebraisch abgeschlossen in K. Es kann in K' jedoch noch mehr Elemente geben, die algebraisch über k sind; diese bilden den Kontantenkörper k' des Funktionenkörpers K'/k'. In diesem Fall bezeichnet man K'/k' als *endliche Erweiterung* von K/k.

Sei nun $Q \in \mathbb{P}_{K'}$. Wird die Bewertung ν_Q auf K eingeschränkt, so verschwindet sie dort nicht identisch. Denn angenommen, das wäre so und sei $x \in K'$. Dann würde für x, das algebraisch über K ist, also ein Minimalpolynom Min mit Koeffizienten in K hat, einerseits $\nu_Q(Min(x)) = \nu_Q(0) = \infty$ gelten, andererseits wäre $\nu_Q(Min(x)) = 0$, da alle seine Koeffizienten von Min verschwindende Bewertung hätten. Also ist $\mathcal{O}_Q \cap K$ ein Bewertungsring von K zur Bewertung $\nu_Q|_K$ mit Primideal $P := Q \cap K$. In diesem Fall sagt man *Q teilt P* oder auch *Q liegt über P*.

Satz 2.22. *(nach [Gol03] Corollary 2.1.17.)*
Sei K/k ein Funktionenkörper und K' eine endliche Erweiterung von K. Sei weiter P ein Primdivisor von K und $Q_1, \ldots, Q_r$ die Menge aller Primdivisoren von K', die P teilen.
Dann gilt

$$\sum_{i=1}^{r} e(Q_i|P) f(Q_i|P) = |K' : K|.$$

Satz 2.23. *(nach [Gol03] Theorem 2.4.9.)*
Sei K'/K eine endliche, separable Erweiterung von Funktionenkörpern.
Dann gilt $e(P'|P' \cap K) = 1$ für fast alle Primdivisoren $P' \in \mathbb{P}_{K'}$.

Definition 2.24. Skalare Erweiterung
Einen Funktionenkörper K'/k' nennt man *skalare Erweiterung* von K/k, wenn $K' = k'K$.

Definition 2.25. Singuläre und nichtsinguläre Primdivisoren
Sei K/k ein geometrischer Funktionenkörper und k'/k eine endliche Erweiterung. Ein Primdivisor $P \in \mathbb{P}_K$ wird als *singulär bezüglich k'* bezeichnet, wenn $k' \otimes_k \mathcal{O}_P$ echt im ganzen Abschluss von $\mathcal{O}_P$ in $k' \otimes_k K$ enthalten ist, andernfalls als *nichtsingulär bezüglich k'*.

Singulär wird P genannt, wenn es bezüglich irgendeiner endlichen Erweiterung k'/k singulär ist, andernfalls *nichtsingulär*.

Bemerkung: Falls k perfekt ist, sind alle Primdivisoren nichtsingulär.

Definition 2.26. Zerfällungskörper für Primdivisoren
Gilt für eine Erweiterung k'/k und einen Primdivisor $P \in \mathbb{P}_K$, dass alle Primdivisoren Q in $k' \otimes_k K$, die P teilen, Grad $\deg(Q) = 1$ haben, also Punkte sind, so nennt man k' einen *Zerfällungskörper* für P.

Lemma 2.27. *(nach [Gol03] Lemma 3.2.5.)*
Sei K/k ein geometrischer Funktionenkörper, $\overline{k}$ der algebraische Abschluss von k und $\overline{K} := \overline{k} \otimes_k K$. Dann ist $\overline{K}/\overline{k}$ ein Funktionenkörper.

Theorem 2.28. *(nach [Gol03] Theorem 3.2.6.)*
Sei K/k ein geometrischer Funktionenkörper, P ein nichtsingulärer Primdivisor von K und k'/k eine endliche Erweiterung, die ein Zerfällungskörper für P ist. Setze $K' := k' \otimes_k K$, so gibt es eine 1-zu-1 Entsprechung zwischen den Punkten Q von $\overline{K}$, für die $Q \cap K = P$ gilt, und den Punkten P' von K', die P teilen, gegeben durch $Q \cap K' = P'$ und $e(Q|P) = e(P'|P)$.

Definition 2.29. Sei mit der obigen Notation $k' \subseteq \overline{k}$, $K' := k' \otimes_k K$ und Q ein Punkt von $\overline{K}$. Dann heißt Q *über k' definiert*, falls $Q \cap K'$ ein Punkt ist.

Definition 2.30. Wirkung von $\mathbf{Aut}_k(K)$ auf $\mathbb{P}_K$
Sei K/k ein Funktionenkörper und Q ein Primdivisor von K mit zugehöriger Bewertung ν_Q. Ist nun $\sigma : K \to K$ ein k-Automorphismus von K, so ist auch $\nu_Q \circ \sigma$ eine diskrete k-Bewertung von K mit Bewertungsring $\sigma^{-1}(\mathcal{O}_Q)$ und maximalem Ideal $Q^\sigma := \sigma^{-1}(Q)$.

Theorem 2.31. *(nach [Gol03] Theorem 3.5.1.)*
Ist K'/k' eine galoische Erweiterung von K/k und $Gal(K'/K)$ die zugehörige Galoisgruppe, so wirkt $Gal(K'/K)$ auf der Menge der Primdivisoren von K' vermöge der Zuordnung $Q \mapsto Q^\sigma$.

Ist Q ein Primdivisor von K' und $P := Q \cap K$, dann ist auch $\sigma^{-1}(Q) \cap K = P$, denn σ lässt K fest. Das bedeutet, $Gal(K'/K)$ permutiert die Menge der Primdivisoren $\{Q_1, \ldots, Q_r\}$ von K', die ein und denselben Primdivisor P von K teilen. Auf dieser Menge ist die Wirkung sogar transitiv:

Seien Q_1 und Q_2 Primdivisoren auf K' mit $P := Q_1 \cap K = Q_2 \cap K$. Dann gibt es einen Automorphismus $\sigma \in Gal(K'/K)$ mit $Q_1^\sigma = Q_2$.

Korollar 2.32. *Für Q_1 und Q_2 gilt darüber hinaus $e(Q_1|P) = e(Q_2|P)$.*

Beweis. Laut Definition des Verzweigungsindex gilt $\nu_{Q_i}|_K = e(Q_i|P)\nu_P$ für $i = 1, 2$. Da $Q_1^\sigma = Q_2$ gilt, ist außerdem $\nu_{Q_2} = \nu_{Q_1} \circ \sigma$. Da σ konstant auf K ist, folgt daraus $\nu_{Q_1}|_K = \nu_{Q_2}|_K$. Nun gilt also

$$e(Q_1|P)\nu_P = \nu_{Q_1}|_K = \nu_{Q_2}|_K = e(Q_2|P)\nu_P$$

und daraus folgt die Behauptung $e(Q_1|P) = e(Q_2|P)$. □

2.4 Projektive Kurven

In diesem Abschnitt wird der Begriff der projektiven Kurve eingeführt und der Zusammenhang zwischen den bisher betrachteten Funktionenkörpern und projektiven Kurven dargestellt.

Definition 2.33. Projektiver Raum
Für einen Körper k ist der $n-$dimensionale *projektive Raum* $\mathbb{P}^n(k)$ definiert als die Menge der Geraden durch den Ursprung in k^{n+1}. Ist $(a_0, \ldots, a_n)$ ein Punkt verschieden von Null in k^{n+1}, so wird die Gerade durch den Nullpunkt, die durch diesen Punkt geht, mit $(a_0 : \cdots : a_n)$ bezeichnet. Jede solche Linie ist ein Punkt von $\mathbb{P}^n(k)$.

Definition 2.34. k_r-rationale Punkte
Einen Punkt von $\mathbb{P}^n(\overline{k})$, dessen Koordinaten bereits über k_r, einer Erweiterung von k von Grad r, definiert sind, nennt man *k_r-rationalen Punkt.*

Ist $f \in k[X_0, \ldots, X_n]$ ein homogenes Polynom von Grad d, so gilt für alle $\lambda \in k$, $a \in \overline{k}^{n+1}$, dass $f(\lambda a) = \lambda^d f(a)$ und seine Nullstellenmenge $\boldsymbol{V}(f)$ ist daher eine wohldefinierte Teilmenge von $\mathbb{P}^n(\overline{k})$.

Definition 2.35. Abgeschlossene Mengen
Die Menge der gemeinsamen Nullstellen in $\mathbb{P}^n(\overline{k})$ einer beliebigen Menge von homogenen Polynomen in $k[X_0, \ldots, X_n]$ wird *abgeschlossene Menge* genannt.

Definition 2.36. Irreduzible Menge, projektive Varietät
Eine abgeschlossene Menge wird *irreduzibel* genannt, wenn sie nicht als Vereinigung zweier echter abgeschlossener Teilmengen geschrieben werden kann. Eine abgeschlossene Menge in $\mathbb{P}^n(\overline{k})$ nennt man *projektive Varietät*, wenn sie irreduzibel ist.

Ist $J \subseteq k[X_0, \ldots, X_n]$ ein Ideal, so bezeichnet $\boldsymbol{V}(J) \subseteq \mathbb{P}^n(\overline{k})$ die Nullstellenmenge von J. Ist umgekehrt $S \subseteq \mathbb{P}^n(\overline{k})$, so bezeichnen wir mit $\boldsymbol{I}(S)$ das Ideal der auf S verschwindenden Funktionen.

Lemma 2.37. *(nach [Gol03] Lemma 4.1.7.)*
Eine abgeschlossene Menge V ist genau dann eine projektive Varietät, wenn $\boldsymbol{I}(V)$ ein Primideal ist.

Definition 2.38. Körper der rationalen Funktionen
Sei k ein Körper und $V \subseteq \mathbb{P}^n(\overline{k})$ eine projektive Varietät. Dann ist $\boldsymbol{I}(V)$ ein Primideal und damit $k[V] := k[X_0, \ldots, X_n]/\boldsymbol{I}(V)$ ein Integritätsbereich.

Nun bezeichne $k(V)$ den Körper der homogenen Quotienten von $k[V]$, das heißt

$$k(V) = \{ \frac{p}{q} \mid p, q \in k[V] \text{ homogen und vom gleichen Grad}\}.$$

Dieser Körper $k(V)$ wird *Körper der rationalen Funktionen auf* V genannt.

Definition 2.39. Projektive Kurve
Sei $V \subseteq \mathbb{P}^n(\overline{k})$ eine projektive Varietät. Die Dimension von V ist definiert als $\dim(V) = \text{trdeg(k(V)/k)}$, also der Transzendenzgrad der Erweiterung $k(V)/k$.
Ist $\dim(V) = 1$, also $k(V)$ ein Funktionenkörper im Sinne von Definition 2.6, so nennt man V eine *projektive Kurve*.

Ist nun umgekehrt ein Funktionenkörper K/k gegeben, so stellt sich die Frage, ob es eine projektive Kurve $V \subseteq \mathbb{P}^n(\overline{k})$ gibt, so dass $K = k(V)$ ist.

Es soll eine Abbildung konstruiert werden, die Punkte von K nach $\mathbb{P}^n$ abbildet und deren Bild eine projektive Kurve V mit $k(V) = K$ ist.

Theorem 2.40. *(nach [Gol03] Theorem 4.2.2.)*
Sei K/k ein Funktionenkörper und sei $\phi := (\phi_0, \phi_1, \ldots, \phi_n) \in K^{n+1}$, wobei $\phi_0 \neq 0$ und ϕ_i/ϕ_0 für irgendein i nichtkonstant ist. Für einen beliebigen Punkt P von K sei t_P ein lokaler Parameter in P und $e_P := -min_i\{\nu_P(\phi_i)\}$. Dann ist

$$\phi(P) := (t_P^{e_P}\phi_0(P) : \cdots : t_P^{e_P}\phi_n(P)) \in \mathbb{P}^n$$

wohldefiniert und unabhängig von der Wahl von t_P. Außerdem ist

$$V := im(\phi) = \{\phi(P) | P \in \mathbb{P}_K\}$$

eine projektive Kurve mit $k(V) = k(\phi_1/\phi_0, \ldots, \phi_n/\phi_0)$.

Sei nun $R := k[\phi_0, \ldots, \phi_n]$ und die Abbildung $\Phi : k[X_0, \ldots, X_n] \to R[T]$ für eine Unbestimmte T durch

$$\Phi(X_i) := \phi_i T \quad (0 \leq i \leq n)$$

gegeben. Sind $f, g \in k[X_0, \ldots, X_n]$ homogene Polynome vom gleichen Grad, so ist

$$\frac{\Phi(f)}{\Phi(g)} = \frac{f(\phi_0, \ldots, \phi_n)}{g(\phi_0, \ldots, \phi_n)} \in K.$$

Das macht die folgende Definition sinnvoll: Ist nun $a \in V$, so sei

$$\mathcal{O}_a := \{\frac{\Phi(f)}{\Phi(g)} \in K | g(a) \neq 0\},$$

$$P_a := \{\frac{\Phi(f)}{\Phi(g)} \in \mathcal{O}_a | f(a) = 0\}.$$

Der Ring $\mathcal{O}_a$ bildet einen lokalen Unterring von K mit maximalem Ideal P_a und wird der *lokale Ring in a* genannt.

Nun gilt folgende Ergänzung zu Theorem 2.40:

Theorem 2.41. *(nach [Gol03] Theorem 4.2.2.)*
Für $a \in V$ mit lokalem Ring $\mathcal{O}_a$ gilt

$$\phi^{-1}(a) = \{P \in \mathbb{P}_K \mid \mathcal{O}_a \subseteq \mathcal{O}_P \text{ und } P \cap \mathcal{O}_a = P_a\}.$$

So definiert also jedes Tupel $(\phi_0, \ldots, \phi_n) \in K^{n+1}$ mit mindestens einem nichtkonstanten ϕ_i/ϕ_0 eine Abbildung $\phi : \mathbb{P}_K \to V$ von den Punkten von K auf die Punkte einer projektiven Kurve $V \subseteq \mathbb{P}^n$. Man nennt ϕ eine *projektive Abbildung*. Beginnt man mit einer projektiven Kurve $V \subseteq \mathbb{P}^n \setminus V(X_0)$, so ist die *natürliche Abbildung* $\phi : \mathbb{P}_{k(V)} \to V$ definiert als die projektive Abbildung $\phi := (1, X_1/X_0, \ldots, X_n/X_0)$.

Definition 2.42. Nichtsinguläre projektive Abbildung und Kurve
Gilt für einen Punkt $P \in \mathbb{P}_K$, dass $\phi(P) = a$, dann bezeichnet man ϕ als *nichtsingulär in P (bzw. in a)*, falls $\mathcal{O}_a = \mathcal{O}_P$. Das bedeutet, dass die Abbildung an dieser Stelle injektiv ist.

Sei nun V eine projektive Kurve mit Funktionenkörper K. Dann nennen wir V *nichtsingulär in* $a \in V$, falls die natürliche Abbildung $\phi : \mathbb{P}_K \to V$ nichtsingulär in a ist. Weiter nennen wir V *nichtsingulär*, falls V in jedem Punkt nichtsingulär ist.

Für eine nichtsinguläre Kurve gibt es also eine bijektive Entsprechung zwischen den Punkten ihres Funktionenkörpers und den Punkten der Kurve.

Definition 2.43. Zetafunktion einer projektiven Kurve
Ist V eine projektive Kurve über einem Körper k mit q Elementen und N_r die Anzahl der k_r-rationalen Punkte auf V, so ist die *Zetafunktion* der projektiven Kurve V definiert als

$$Z(V, t) = exp(\sum_{n \geq 1} N_n \frac{t^n}{n}).$$

Definition 2.44. Primdivisoren auf einer projektiven Kurve
Sei $\alpha = (a_0 : \cdots : a_n) \in V$ ein Punkt auf V und k_d der kleinste Erweiterungskörper, der alle seine Koordinaten enthält. Dann bezeichnet man

$$\mathfrak{P} := \{\alpha^{q^j} | j = 0, 1, \ldots, d-1\}$$

als einen *Primdivisor* auf V vom Grad $\deg(\mathfrak{P}) = d$.

Die Punkte $\{\alpha, \alpha^q, \ldots, \alpha^{q^{d-1}}\}$ sind alle verschieden und liegen auf V. Die Primdivisoren bilden eine Partition der Menge der Punkte von V. Ist $\alpha \in V$ mit Koordinaten in k_s, dann definiert α einen eindeutigen Primdivisor von Grad d für ein gewisses $d|s$. Dieser Primdivisor enthält d verschiedene Punkte auf V, die alle wiederum Koordinaten in $k_d \subseteq k_s$ haben. Daher gilt

Lemma 2.45. *(aus [IR90], Lemma 1, Seite 157)*
Ist a_d die Anzahl der Primdivisoren auf V vom Grad d und N_s die Anzahl der k_s-rationalen Punkte auf V, dann gilt

$$N_s = \sum_{d|s} d a_d.$$

Unter Verwendung der Primdivisoren einer projektiven Kurve erhält man folgende Produktdarstellung für ihre Zetafunktion:

Lemma 2.46. *(aus [IR90], Proposition 11.1.3.)*
Für die Zetafunktion einer projektiven Kurve V gilt

$$Z(V, t) = \prod_{\mathfrak{P}} \frac{1}{1 - t^{\deg(\mathfrak{P})}},$$

wobei $\mathfrak{P}$ über alle Primdivisoren auf V läuft.

Nun stellt sich die Frage, was diese Primdivisoren mit den Primdivisoren des Funktionenkörpers der Kurve zu tun haben. Tatsächlich gibt es zwischen ihnen eine graderhaltende bijektive Entsprechung.

Lemma 2.47. *Sei V eine nichtsinguläre projektive Kurve über dem Körper k und K/k ihr Funktionenkörper. Dann gibt es eine Bijektion ψ zwischen den Primdivisoren von V und den Primdivisoren von K, die den Grad erhält, also für alle Primdivisoren $\mathfrak{P}$ von V*

$$\deg(\psi(\mathfrak{P})) = \deg(\mathfrak{P})$$

erfüllt.

Beweis. Sei $\mathfrak{P} = (a, a^q, \ldots, a^{q^{d-1}})$ ein Primdivisor auf V. Sei k' der Erweiterungskörper von k von Grad d und $K' := k' \otimes_k K$. Dann gibt es zwischen den k'-rationalen Punkten von V und den Punkten von K' eine bijekive Entsprechung. Sei $Q_i \in \mathbb{P}_{K'}$ dabei der zu a^{q^i} gehörige Punkt, das heißt $Q_i = \phi^{-1}(a^{q^i})$, wobei ϕ die natürliche Abbildung von $\mathbb{P}_{K'}$ nach V ist. Dann teilen alle Q_i dasselbe $P \in \mathbb{P}_K$, denn

$$Q_i = \{\frac{\Phi(f)}{\Phi(g)} \in K' | g(a^{q^i}) \neq 0, f(a^{q^i}) = 0\}$$

$$Q_i \cap K = \{\frac{\Phi(f)}{\Phi(g)} \in K | g(a^{q^i}) \neq 0, f(a^{q^i}) = 0\}$$

und da bei den Mengen $Q_i \cap K$ die Polynome f, g Koeffizienten in k haben und somit invariant unter der Abbildung $x \mapsto x^q$ (Frobenius) sind, ist $f(a^{q^j}) = 0 \Leftrightarrow f(a^{q^k}) = 0$ für alle j, k. Somit sind diese Mengen alle gleich $P_{\mathfrak{P}}$, nämlich

$$P_{\mathfrak{P}} := P_a = \{\frac{\Phi(f)}{\Phi(g)} \in K | g(a) \neq 0, f(a) = 0\}.$$

Nun gibt es in K' also d Punkte $Q_0, \ldots, Q_{d-1}$, die dieses $P_{\mathfrak{P}} \in \mathbb{P}_K$ teilen. Nach Satz 2.22 gilt

$$\sum_Q e(Q|P_{\mathfrak{P}}) f(Q|P_{\mathfrak{P}}) = [K' : K] = [k' : k] = d$$

wobei die Summe über alle Primdivisoren in K' läuft, die $P_{\mathfrak{P}}$ teilen. Davon gibt es mindestens die d, die wir bereits kennen. Mehr kann es auf Grund der Formel auch nicht geben und es gilt $e(Q_i|P_{\mathfrak{P}}) = f(Q_i|P_{\mathfrak{P}}) = 1$ für alle i. Daraus folgt

$$\deg(P_{\mathfrak{P}}) = [F_{P_{\mathfrak{P}}} : k] = [F_{Q_i} : k] = [k' : k] = d.$$

Der Primdivisor $P_{\mathfrak{P}} \in \mathbb{P}_K$ hat also Grad d und mit $\psi(\mathfrak{P}) := P_{\mathfrak{P}}$ ist die gesuchte graderhaltende Zuordnung zwischen den Primdivisoren der Kurve V und den Primdivisoren ihres Funktionenkörpers K gegeben.

Diese Zuordnung ist bijektiv: Sei nun umgekehrt ein Primdivisor $P \in \mathbb{P}_K$ von Grad d gegeben und ϕ die natürliche Abbildung von $\mathbb{P}_K$ nach V, so ist $a := \phi(P)$ ein Punkt auf V, der über k_d, einem Erweiterungskörper von k von Grad d, definiert ist.

Angenommen, die Koordinaten von a liegen auch schon in $k_{d'}$ und $d'|d$. Dann ist $\mathfrak{P}_P := \{a, a^q, \ldots, a^{q^{d'-1}}\}$ ein Primdivisor von Grad d'. Zu diesem Primdivisor gehört nach der zuerst beschriebenen Zuordnung ein Primdivisor $P' := \psi(\mathfrak{P}_P) = P_{\mathfrak{P}_P}$ des Funktionenkörpers $k'_d \otimes_k K$, für den $P' = P_a \in \phi^{-1}(a)$ gilt. Es ist also $\phi(P') = a = \phi(P)$ und da wir eine nichtsinguläre Kurve betrachten, ist $P' = P$ und somit $d' = d$.

Also ist k_d ist der kleinste Erweiterungskörper von k, der alle Koordinaten von a enthält. Daher ist $\mathfrak{P}_P := \{a, a^q, \ldots, a^{q^{d-1}}\}$ ein Primdivisor von V mit Grad d. Die dadurch gegebene Zuordnung $P \mapsto \mathfrak{P}_P$ kehrt ψ um.
□

Nun soll noch ein Satz zitiert werden, der eine Folgerung aus dem Satz von Stöhr-Voloch ([Gol03] Theorem 4.4.24.) ist, einem tiefliegenden Satz, der hier weder bewiesen noch zitiert werden soll, und in dem es um eine Abschätzung für die Anzahl starker Fixpunkte geht.

Definition 2.48. Grad und starker Fixpunkt einer k-Einbettung
Sei $\tau : K \to K$ eine $k-$Einbettung von K in sich. Der *Grad* von τ ist definiert als $\deg(\tau) := |K : \tau(K)|$. Ein Primdivisor P von K ist genau dann ein Fixpunkt von τ, wenn $\tau(P) \subseteq P$. Ein *starker Fixpunkt* von τ ist P, falls $\tau(P) \subseteq P^2$ ist.

Satz 2.49. *(nach [Gol03] Corollary 4.4.25.)*
Sei K/k ein Funktionenkörper mit Geschlecht g und $\tau : K \to K$ eine $k-$Einbettung. Dann gilt für beliebiges $n > g$, dass die Anzahl der starken Fixpunkte von τ höchstens

$$1 + \deg(\tau) + \Big(n + \frac{\deg(\tau)}{n}\Big)g + \frac{2g^2(g-1)}{n}$$

beträgt.

2.5 Zetafunktionen

Definition 2.50. Zetafunktion eines Funktionenkörpers
Sei nun k ein endlicher Körper der Charakteristik p mit $q = p^r$ Elementen und K/k ein Funktionenkörper. Es soll eine allgemeingültige Abschätzung für die Anzahl der Punkte des Funktionenkörpers K/k hergeleitet werden. Dazu definieren wir die folgende Größe:

$$a_K(n) := |\{D \in Div(K) | D \geq 0 \text{ und } \deg(D) = n\}|$$

und gewinnen daraus die *Zetafunktion*:

$$Z_K(t) := \sum_{n=0}^{\infty} a_K(n) t^n$$

Es bezeichnet also $a_K(1)$ gerade die Anzahl von Punkten auf K.

Mit k_r wird im Folgenden die (bis auf Isomorphie eindeutige) Erweiterung von k von Grad r bezeichnet. Zu einem Funktionenkörper K sei $K_r := k_r \otimes_k K$ die (eindeutige) skalare Erweiterung von K von Grad r.

Analog zur Zetafunktion von projektiven Kurven hat auch diese Zetafunktion eine Produktdarstellung (nach [Gol03] Formel 5.1.1):

$$Z_K(t) = \prod_{P \in \mathbb{P}_K} \frac{1}{1 - t^{\deg(P)}}$$

Im Vergleich mit Lemma 2.46 stellt man also fest, dass die Zetafunktion einer nichtsingulären projektiven Kurve V mit der Zetafuntion ihres Funktionenkörpers K übereinstimmt, denn gemäß Lemma 2.47 gibt es zwischen den Primdivisoren der Kurve und den Primdivisoren ihres Funktionenkörpers eine graderhaltende Bijektion.

Das, was nun über die Zetafunktion $Z_K(t)$ des Funktionenkörpers K hergeleitet wird, lässt sich also auch auf die Zetafunktion $Z(V, t)$ der nichtsingulären projektiven Kurve V, deren Funktionenkörper K ist, übertragen.

Satz 2.51. *(nach [Gol03] Theorem 5.1.8. und Corollary 5.2.5.)*
Sei K ein Funktionenkörper von Geschlecht g über einem endlichen Körper k der Ordnung q. Dann gilt

$$Z_K(t) = \frac{L_K(t)}{(1-t)(1-qt)} ,$$

wobei

$$L_K(t) = \prod_{i=1}^{2g}(1-\alpha_i t)$$

für algebraische Zahlen $\{\alpha_1, \ldots, \alpha_{2g}\}$ *mit* $\alpha_i \alpha_{2g-i+1} = q$ *für* $1 \leq i \leq g$.

Riemannsche Vermutung. Die Riemannsche Vermutung für die Zetafunktion eines Funktionenkörpers K besagt, dass alle Nullstellen von $Z_K(t)$ Betrag $q^{-1/2}$ haben, was gleichbedeutend dazu ist, dass die im Zähler der Zetafunktion auftauchenden α_i von Betrag $q^{1/2}$ sind.

Korollar 2.52. *(nach [Gol03] Corollary 5.3.1.)*
Die Riemannsche Vermutung gilt für K genau dann, wenn sie für eine skalare Erweiterung K_n gilt.

Satz 2.53. *(nach [Gol03] Theorem 5.3.4.)*
Sei K ein Funktionenkörper von Geschlecht g über einem endlichen Körper k der Ordnung q und sei

$$L_K(t) = \prod_{i=1}^{2g}(1-\alpha_i t).$$

Dann gilt

$$\mathcal{L}_K(t) := \frac{Z_K'(t)}{Z_K(t)} = \frac{1}{1-t} + \frac{q}{1-qt} - \sum_{i=1}^{2g}\frac{\alpha_i}{1-\alpha_i t} = \sum_{n=0}^{\infty} b_K(n+1)t^n,$$

wobei $b_K(n) = a_{K_n}(1) = 1 + q^n - \sum_{i=1}^{2g}\alpha_i^n$.

Korollar 2.54. *(nach [Gol03] Corollary 5.3.5.)*
Mit der oben eingeführten Notation sind die folgenden Behauptungen äquivalent:

1. $|\alpha_i| = q^{1/2}$ *für alle* i.
2. *Es gibt Konstanten* $C_0, C_1 \in \mathbb{R}$ *so dass* $|a_{K_n}(1) - q^n| \leq C_0 + C_1 q^{n/2}$ *für fast alle positiven ganzen Zahlen* n.

Es genügt also, die Gültigkeit der Abschätzung in Punkt zwei zu zeigen, dann kann die Riemannsche Vermutung für die Zetafunktion von nichtsingulären

projektiven Kurven bzw. ihren Funktionenkörpern (Satz von Weil 2.59) gefolgert werden. Dazu sollen nun zwei Lemmata hergeleitet werden.

Sei $\overline{k}$ der (bis auf Isomorphie eindeutige) algebraische Abschluss von k. Nach Lemma 2.27 ist $\overline{K} := \overline{k} \otimes_k K$ ein Funktionenkörper mit Konstantenkörper $\overline{k}$. Nach Theorem 2.28 können die Punkte von $K_n := k_n \otimes_k K$, mit den Punkten von $\overline{K}$, die über k_n definiert sind, identifiziert werden.

Definition 2.55. Frobeniusabbildung
Sei q die Ordnung von k, $\mathfrak{f}_0 : K \to K : x \mapsto x^q$ die $q-$te Potenzabbildung und $\mathfrak{f} = \mathfrak{f}_K := 1 \otimes \mathfrak{f}_0 : \overline{K} \to \overline{K}$. Diese Abbildung $\mathfrak{f}$ ist ein Automorphismus von $\overline{K}$ und konstant auf den Skalaren in k. Sie heißt *Frobeniusabbildung.*

Erweitert man die Skalare zu k_n, so ist $\overline{K_n} = \overline{K}$, die Frobeniusabbildung jedoch wird zu $\mathfrak{f}^n$.

Da $\mathfrak{f} \in \mathrm{Aut}_{\overline{k}}(\overline{K})$, wirkt $\mathfrak{f}$ wie in Definition 2.30 beschrieben auf den Punkten von $\overline{K}$ durch $Q \mapsto Q^{\mathfrak{f}}$.

Lemma 2.56. *(nach [Gol03] Lemma 5.3.6.)*
Sei $\mathfrak{f} = \mathfrak{f}_K$ die Frobeniusabbildung und sei $Q \in \mathbb{P}_{\overline{K}}$. Es ist genau dann $Q^{\mathfrak{f}} = Q$, wenn Q über k definiert ist, das heißt, wenn $Q \cap K$ ein Punkt von K ist.

Sei nun K'/k eine endliche Erweiterung von K/k. Es gibt eine natürliche Inklusion $\overline{K} \hookrightarrow \overline{K'}$. Da $\mathfrak{f}_{K'}$ auf den Skalaren die Identität und eingeschränkt auf K' die $q-$te Potenzabbildung ist, stimmt $\mathfrak{f}_{K'}$ auf $\overline{K}$ mit $\mathfrak{f}_K$ überein.

Sei K'/K außerdem galoisch. Dann kann jedes $\sigma \in \mathrm{Gal}(K'/K)$ zu einem Automorphismus $1 \otimes \sigma$ von $\overline{K'} = \overline{k} \otimes_k K'$ erweitert werden, der auf $\overline{K}$ die Identität ist, also $1 \otimes \sigma \in \mathrm{Gal}(\overline{K'}/\overline{K})$. Da die so entstehenden Automorphismen alle verschieden sind, folgt $|K' : K| \leq |\mathrm{Gal}(\overline{K'}/\overline{K})| \leq |\overline{K'} : \overline{K}|$. Andererseits gilt $|\overline{K'} : \overline{K}| \leq |K' : K|$, denn falls $u_1, \ldots, u_r$ eine K-Basis von K' ist, spannt $1 \otimes u_1, \ldots, 1 \otimes u_r$ den $\overline{K}$-Vektorraum $\overline{K'}$ auf. Es folgt also $|\overline{K'} : \overline{K}| = |K' : K|$.

Da einerseits $|\mathrm{Gal}(\overline{K'}/\overline{K})| \leq |\overline{K'} : \overline{K}| \leq |K' : K| = |\mathrm{Gal}(K'/K)|$, andererseits die Abbildung $\sigma \mapsto 1 \otimes \sigma$ injektiv ist, ist sie sogar ein Isomorphismus zwischen $\mathrm{Gal}(K'/K)$ und $\mathrm{Gal}(\overline{K'}/\overline{K})$. Auf diese Weise können alle Gruppen $\mathrm{Gal}(K'_n/K_n)$ miteinander identifiziert werden. Die Erweiterung $\overline{K'}/\overline{K}$ ist galoisch.

Sei nun n eine positive ganze Zahl und Q ein Punkt von $\overline{K'}$, so dass $P = Q \cap \overline{K}$ ein Punkt und über k_n definiert ist. Im Allgemeinen muss Q selbst aber nicht über k_n definiert sein. Ist das so, und ist $\mathfrak{f} = \mathfrak{f}_{K'}$ die Frobeniusabbildung, so

ist $Q^{\mathfrak{f}^n}$ wieder ein anderer Punkt von K', der aber dasselbe P teilt. Nach Theorem 2.31 gibt es dann aber ein $\sigma \in \mathrm{Gal}(\overline{K'}/\overline{K})$, so dass $Q^{\mathfrak{f}^n} = Q^\sigma$. Dieses σ nennen wir die *Frobeniussubstitution* im Punkt Q. Es hängt von der Wahl von n ab.

Nun sollen alle Punkte von $\overline{K'}$, die über irgendeinem k_n-rationalen Punkt von $\overline{K}$ liegen, gezählt werden, und zwar in Abhängigkeit von der Frobeniussubstitution, zu der sie gehören. Da der Grundkörper $\overline{k}$ algebraisch abgeschlossen ist, sind alle Primdivisoren von $\overline{K'}$ und $\overline{K}$ Punkte.

Seien also Funktionenkörper $K'/k \supseteq K/k$ mit der Frobeniusabbildung $\mathfrak{f} \in \mathrm{Aut}_{\overline{k}}(\overline{K'})$ sowie ein Automorphismus $\sigma \in G = \mathrm{Gal}(\overline{K'}/\overline{K})$ gegeben. Dann sei

$$\mathbb{P}_n(K'/K, \sigma) := \{Q \in \mathbb{P}_{\overline{K'}} \mid e(Q|Q \cap \overline{K}) = 1 \text{ und } Q^{\mathfrak{f}^n} = Q^\sigma\}.$$

Falls $Q \in \mathbb{P}_n(K'/K, \sigma)$ für irgendein σ, so ist $Q \cap \overline{K}$ nach Lemma 2.56 über k_n definiert, denn σ lässt $\overline{K}$ fest und $Q^{\mathfrak{f}^n} = Q^\sigma$, folglich ist $(Q \cap \overline{K})^{\mathfrak{f}^n} = Q \cap \overline{K}$.

Da nur endlich viele Punkte von $\overline{K}$ über k_n definiert sind, sind die Mengen $\mathbb{P}_n(K'/K, \sigma)$ endlich, disjunkt und ihre Vereinigung ist die Menge aller Punkte $Q \in \mathbb{P}_{\overline{K'}}$, für die $Q \cap \overline{K}$ über k_n definiert und über $\overline{K'}$ unverzweigt ist.

Sei nun $p_n(K'/K, \sigma) := |\mathbb{P}_n(K'/K, \sigma)|$. Nach Theorem 2.32 haben alle Punkte $Q \in \mathbb{P}_{\overline{K'}}$, die einen gegebenen Punkt $P \in \mathbb{P}_{\overline{K}}$ teilen, den gleichen Verzweigungsindex. Ist also eines dieser Q unverzweigt, so sind auch alle anderen Punkte von $\overline{K'}$, die P teilen, unverzweigt. Da $\overline{k}$ algebraisch abgeschlossen ist, beträgt die Anzahl dieser Punkte folglich nach Satz 2.22 $|K' : K|$.

Die Gesamtzahl der Punkte $P \in \mathbb{P}_{\overline{K}}$, die in $\overline{K'}$ verzweigt sind, ist nach Satz 2.23 endlich, unabhängig davon, über welcher Erweiterung von k sie definiert sind. Es folgt also

$$|\sum_{\sigma \in G} p_n(K'/K, \sigma) - |K' : K| a_{K_n}(1)| \leq C'$$

für eine von n unabhängige Konstante C'. Damit ist das folgende Lemma bewiesen:

Lemma 2.57. *(nach [Gol03] Lemma 5.3.7.)*
Es gibt eine Konstante C, die nicht von n abhängt, so dass

$$|a_{K_n}(1) - \frac{1}{|G|} \sum_{\sigma \in G} p_n(K'/K, \sigma)| \leq C.$$

Lemma 2.58. *(nach [Gol03] Lemma 5.3.8.)*
Sei $g := g_{K'}$ das Geschlecht des Funktionenkörpers K'. Falls q die Ordnung von k ist und $q = p^{2r} > 4g^4(g-1)^2$ ist, dann gilt

$$p_m(K'/K, \sigma) \leq 1 + q^m + 2gq^{m/2}$$

für alle $\sigma \in G$ und alle positiven ganzen Zahlen m.

Beweis. Sei $\sigma \in G$, m eine positive ganze Zahl, $\mathfrak{f} = \mathfrak{f}_{K'}$ die Frobeniusabbildung und $\tau := \mathfrak{f}^m \sigma^{-1}$. Dann ist $\mathbb{P}_m(K'/K, \sigma)$ gerade die Menge der Fixpunkte von τ auf $\mathbb{P}_{\overline{K'}}$, die über $\overline{K}$ unverzweigt sind. Es gilt außerdem $\tau(\overline{K'}) = \overline{K'}^{q^m}$ und $\tau(P) \subseteq \overline{K'}^{q^m}$. Daher folgt aus $\tau(P) \subseteq \tau$ schon $\tau(P) \subseteq P^2$. Jeder Fixpunkt ist also ein starker Fixpunkt. Um $p_m(K'/K, \sigma)$ abzuschätzen, genügt es daher, die Anzahl der starken Fixpunkte von τ abzuschätzen. Dafür nutzen wir Satz 2.49. Es ist $\deg(\tau) = q^m$, wir wählen

$$n = q^{m/2} > (4g^4(g-1)^2)^{m/2} = (2g^2(g-1))^m > g$$

und erhalten, dass τ höchstens

$$1 + q^m + (q^{m/2} + \frac{q^m}{q^{m/2}})g + \frac{2g^2(g-1)}{q^{m/2}} = 1 + q^m + 2q^{m/2}g + \frac{2g^2(g-1)}{q^{m/2}}$$

Fixpunkte hat. Der letzte Term $\frac{2g^2(g-1)}{q^{m/2}}$ verschwindet, falls $g = 1$ ist. Für $g > 1$ ist $(2g^2(g-1))^m > 2g^2(g-1)$ und damit

$$1 > \frac{(2g^2(g-1))^m}{q^{m/2}} > \frac{2g^2(g-1)}{q^{m/2}}$$

und daher folgt nun insgesamt

$$p_m(K'/K, \sigma) \leq 1 + q^m + 2gq^{m/2}. \qquad \square$$

Theorem 2.59. (Weil) *(nach [Gol03] Theorem 5.3.9.)*
Sei K ein Funktionenkörper über einem endlichen Körper k der Ordnung q und sei $L_K(t) = \prod_{i=1}^{2g}(1 - \alpha_i t)$ der Zähler seiner Zetafunktion.
Dann gilt $|\alpha_i| = q^{1/2}$ für alle i.

Beweis. Zunächst sei $x \in K$ so gewählt, dass $K/k(x)$ separabel ist (siehe 2.21). Falls die Erweiterung $K/k(x)$ nicht normal ist, wähle eine galoische Erweiterung $K \subseteq K'$. Möglicherweise ist der Konstantenkörper k' von K' eine endliche Erweiterung von k, doch Korollar 2.52 sei Dank, kann k falls

nötig zu k' erweitert werden und die Bezeichnung soweit geändert werden, dass $k' = k$ angenommen werden darf. Aus dem gleichen Grund kann auch angenommen werden, dass q groß genug ist, um die Bedingung von Lemma 2.58 zu erfüllen.

Sei nun $G := \mathrm{Gal}(K'/k(x))$ die Galoisgruppe der galoischen Erweiterung $K'/k(x)$. Wie aus der Algebra bekannt, ist K' auch über dem Zwischenkörper K galoisch. Die zugehörige Galoisgruppe sei $H := \mathrm{Gal}(K'/K)$. Wird nun Lemma 2.57 auf beide Erweiterungen angewandt, so ergeben sich folgende Abschätzungen:

$$\left|a_{k_n(x)}(1) - \frac{1}{|G|}\sum_{\sigma\in G} p_n(K'/k(x),\sigma)\right| \leq C \tag{1}$$

$$\left|a_{K_n}(1) - \frac{1}{|H|}\sum_{\sigma\in H} p_n(K'/K,\sigma)\right| \leq C_1 \tag{2}$$

Es gilt $|a_{k_n(x)}(1)| = q^n + 1$. Ungleichung (1) besagt also, dass $p_n(K'/k(x),\sigma)$ im Durchschnitt für alle σ etwa q^n ist. Sei nun g das Geschlecht von K' und $d = |K' : k(x)| = |G|$. Aus Lemma 2.58 folgt für ein beliebiges $\sigma \in G$:

$$p_n(K'/k(x),\sigma) + (d-1)(q^n + 1 + 2gq^{n/2}) \geq \sum_{\tau\in G} p_n(K'/k(x),\tau)$$

Und mit obiger Abschätzung (1) ergibt sich

$$\sum_{\tau\in G} p_n(K'/k(x),\tau) \geq d(q^n + 1 - C),$$

woraus zusammen folgt

$$p_n(K'/k(x),\sigma) \geq q^n - (d-1)(1 + 2gq^{n/2}) + d - dC.$$

Nun gilt also einerseits

$$q^n - p_n((K'/k(x),\sigma) \leq A_1 + B_1 q^{n/2},$$

andererseits liefert 2.58 auch die Abschätzung

$$p_n((K'/k(x),\sigma) - q^n \leq 1 + 2gq^{n/2},$$

es gilt also insgesamt

$$|p_n((K'/k(x),\sigma) - q^n| \leq A + Bq^{n/2},$$

wobei die Konstanten A und B nicht von n abhängen.

Nun sind für $\sigma \in H$ die Mengen $\mathbb{P}_n(K'/k(x), \sigma)$ und $\mathbb{P}_n(K'/K, \sigma)$ im Wesentlichen dieselben. Denn beide Male werden Punkte von $\overline{K'}$ gezählt, in $\mathbb{P}_n(K'/k(x), \sigma)$ die, die über $\overline{k}(x)$ unverzweigt sind, in $\mathbb{P}_n(K'/K, \sigma)$ solche, die über $\overline{K}$ unverzweigt sind. Sie unterscheiden sich aber nur um eine endliche (von n unabhängige) Zahl von Punkten, nämlich denen, die über $\overline{K}$ unverzweigt, aber über $\overline{k}(x)$ verzweigt sind.

Nun folgt aus den obigen Ungleichungen, dass es von n unabhängige Konstanten A' und B' gibt, für die gilt

$$|a_{K_n}(1) - q^n| \leq A' + B' q^{n/2}$$

und das gilt für alle n, also ist die Aussage zwei von Korollar 2.54 bewiesen und der Satz kann gefolgert werden. □

Korollar 2.60. *Mit Satz 2.51 folgt nun aus $\alpha_i \cdot \alpha_{2g-i+1} = q$ unmittelbar $\overline{\alpha_i} = \alpha_{2g-i+1}$. Damit ergibt sich die folgende Darstellung für die Zetafunktion:*

$$Z_K(t) = \frac{\prod_{i=1}^{g}(1 - \alpha_i t)(1 - \overline{\alpha_i} t)}{(1-t)(1-qt)}$$

Korollar 2.61. (Weil) *(nach [Gol03] Corollary 5.3.13.)*
Sei K/k ein Funktionenkörper von Geschlecht g über einem endlichen Körper k der Ordnung q. Dann gilt die Abschätzung

$$|a_K(1) - q - 1| \leq 2gq^{1/2}.$$

Beweis. Nach Theorem 2.53 ist (für $n = 1$) $a_K(1) = 1 + q - \sum_{i=1}^{2g} \alpha_i$, daher ist

$$|a_K(1) - q - 1| \leq |\sum_{i=1}^{2g} \alpha_i| \leq 2gq^{1/2}.$$

□

Aus dem Satz von Weil ergibt sich also eine Abschätzung für die Höchstanzahl der Punkte eines Funktionenkörpers:

$$a_K(1) \leq 2gq^{1/2} + q + 1$$

Nach der in Abschnitt 2.4 erläuterten bijektiven Entsprechung zwischen Punkten einer nichtsingulären projektiven Kurve und Punkten ihres Funktionenkörpers gilt diese Abschätzung auch für nichtsinguläre projektive Kurven.

Als letzte Folgerung aus dem Satz von Weil steht nun das folgende Korollar, das die beiden Darstellungen der Zetafunktion 2.43 und 2.60 in Verbindung bringt:

Korollar 2.62. *Sei X eine nichtsinguläre projektive Kurve von Geschlecht g über einem Körper k mit q Elementen, die N_n Punkten über dem Erweiterungskörper k_n besitzt. Hat die Zetafunktion von X die Darstellung*

$$Z(t) = \frac{\prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha_i}t)}{(1-t)(1-qt)},$$

so gilt für alle n

$$N_n = q^n + 1 - \sum_{i=1}^{g}(\alpha_i^n + \overline{\alpha_i}^n).$$

Beweis: Betrachtet man die logarithmische Ableitung der Zetafunktion in der oben angegebenen Form, so erhält man

$$\frac{Z'(t)}{Z(t)} = \sum_{l=1}^{g}\frac{-\alpha_l}{1-\alpha_l t} + \sum_{l=1}^{g}\frac{-\overline{\alpha}_l}{1-\overline{\alpha}_l t} + \frac{1}{1-t} + \frac{q}{1-qt}$$

Multipliziert man beide Seiten mit t und wendet die geometrische Reihe $\sum_{n=1}^{\infty}(at)^n = \frac{at}{1-at}$ an, so ergibt sich die folgende Potzenreihendarstellung:

$$\frac{tZ'(t)}{Z(t)} = \sum_{n=1}^{\infty}\big(-\sum_{i=1}^{g}\alpha_i^n - \sum_{i=1}^{g}\overline{\alpha}_i^n + 1 + q^n\big)t^n$$

Aus der Definition der Zetafunktion $Z(t) = \exp(\sum_{n=1}^{\infty}\frac{N_n t^n}{n})$ erhält man

$$\frac{tZ'(t)}{Z(t)} = \frac{tZ(t)\sum_{n=1}^{\infty}\frac{nN_n t^{n-1}}{n}}{Z(t)} = \sum_{n=1}^{\infty}N_n t^n$$

Vergleicht man nun die Koeffizienten von t^n, so kann man den Beweis beschließen:

$$N_n = -\sum_{i=1}^{g}\alpha_i^n - \sum_{i=1}^{g}\overline{\alpha}_i^n + 1 + q^n$$

□

3 Die Idee

Die Abschätzung für die Anzahl von Punkten einer nichtsingulären projektiven Kurve, die im vorigen Abschnitt vorgestellt wurde, ist zwar allgemeingültig, doch dafür auch nicht sehr scharf. Es gibt zwar noch eine etwas verbesserte Version dieser allgemeingültigen Abschätzung nach Serre [Ser83], doch liegt auch diese in vielen Beispielen noch weit jenseits der Punktanzahl von tatsächlich gefundenen Kurven.

Es interessiert daher, wie sich diese oberen Grenzen in Einzelfällen noch weiter verbessern lassen. Kristin Lauter beschreibt in [Lau00] eine Methode zur Ermittlung besserer oberer Schranken, die hier vorgestellt werden soll.

Sei X eine nichtsinguläre projektive Kurve von Geschlecht g über $k = \mathbb{F}_q$ mit N_n Punkten über dem Erweiterungskörper $k_n = \mathbb{F}_{q^n}$. Für die Zetafunktion der Kurve X gilt:

$$Z(X,t) = exp(\sum_{n\geq 1} N_n \frac{t^n}{n}) = \frac{h(t)}{(1-t)(1-qt)}$$

Hierbei faktorisiert sich das Polynom $h(t)$ nach Korollar 2.60 wie folgt:

$$h(t) = \prod_{i=1}^{g} (1-\alpha_i t)(1-\overline{\alpha_i} t)$$

Aus dem Satz von Weil folgt, dass die komplexen Zahlen α_i sich auf einem Kreis mit Radius $\sqrt{q}$ um die Null befinden. Aus $h(t)$ lässt sich ein weiteres Polynom bilden, das im Folgenden als **Zetapolynom** bezeichnet werden soll.

$$F(T) := \prod_{i=1}^{g} (T - u_i), \quad u_i = \alpha_i + \overline{\alpha_i}$$

Die Nullstellen des Zetapolynoms $F(T)$ sind also reell und liegen im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$. Letzteres folgt aus $\alpha_i \overline{\alpha}_i = q$. Das gleiche gilt auch für Nullstellen beliebiger Ableitungen dieses Polynoms, denn nach dem Satz von Rolle hat die Ableitung zwischen je zwei unterschiedlichen Nullstellen wieder eine Nullstelle. Hat das Polynom mehrfache Nullstellen, so verschwindet an diesen auch die Ableitung. Insgesamt sind also auch die Nullstellen der Ableitung (und damit jeder beliebigen Ableitung) des Polynoms reell und liegen im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$. Siehe dazu auch Satz 4.3.

Falls alle Nullstellen reell sind und im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$ liegen, wollen wir sie **zulässig** nennen und sagen, das Zetapolynom erfülle das **Nullstellenkriterium**.

Diese Eigenschaft schränkt die mögliche Gestalt des Zetapolynoms zu gegebenen Daten (g, q, N_1) schon erheblich ein. Im folgenden Abschnitt wird ein Algorithmus beschrieben, mit dem alle möglichen Zetapolynome zu (g, q, N_1) gefunden werden können.

Eine weitere Eigenschaft des Zetapolynoms einer Kurve beschreibt das Resultantenkriterium.

Definition 3.1. Resultante (nach [Lan02] IV. §8, Proposition 8.3)
Für zwei Polynome $p(x) = \prod_{k=1}^{n}(x - \alpha_k)$ und $q(x) = \prod_{j=1}^{m}(x - \beta_j)$ ist die *Resultante*

$$Res(p, q) = \prod_{k=1}^{n}\prod_{j=1}^{m}(\alpha_k - \beta_j).$$

Satz 3.2. Resultantenkriterium *(aus [Lau00] Lemma 1)*
Sei X eine nichtsinguläre projektive Kurve und ihr Zetapolynom

$$F(T) = \prod_{i=1}^{g}(T - u_i) \qquad mit \qquad u_i = \alpha_i + \overline{\alpha_i}.$$

Dann kann $F(T)$ über $\mathbb{Z}[T]$ nicht in nichtkonstante Polynome r und s faktorisiert werden, $F(T) = r(T)s(T)$, so dass ihre Resultante $Res(r, s) = \pm 1$ ist.

Lässt sich also ein gefundenes Zetapolynom, das das Nullstellenkriterium erfüllt, so zerlegen, dass die Faktoren Resultante 1 haben, kann das Zetapolynom nicht zur gesuchten Kurve gehören, denn es erfüllt das Resultantenkriterium nicht.

Gibt es zu gegebenen Daten (g, q, N_1) kein Zetapolynom, das das Nullstellen- und das Resultantenkriterium erfüllt, so kann es auch keine Kurve zu diesen Daten geben. Das ist die Grundidee, auf die der im Folgenden beschriebene Algorithmus aufbaut.

4 Der Algorithmus

4.1 Eigenschaften des Zetapolynoms

Die hier zu untersuchende Frage ist, ob es zu den Daten (g, q, N_1) eine Kurve gibt, wobei g das Geschlecht der Kurve, q die Ordnung des Körpers und N_1 die Anzahl der über $\mathbb{F}_q$ definierten Punkte auf der Kurve ist.

Gibt es eine solche Kurve, so hat sie ein Zetapolynom $F(T)$, das sowohl das Nullstellen- als auch das Resultantenkriterium erfüllt. Es soll nun ein Algorithmus hergeleitet werden, der entscheidet, ob es zu den Daten (g, q, N_1) ein solches Zetapolynom gibt oder nicht.

Sei X eine nichtsinguläre projektive Kurve von Geschlecht g über $\mathbb{F}_q$ mit N_n Punkten über dem Erweiterungskörper $\mathbb{F}_{q^n}$. Für die Zetafunktion der Kurve X gilt:

$$Z(X,t) = exp(\sum_{n\geq 1} N_n \frac{t^n}{n}) = \frac{\prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha_i}t)}{(1-t)(1-qt)}$$

Die Größe N_n hängt mit diesen $\{\alpha_i\}$ zusammen (vgl. Korollar 2.62):

$$N_n = q^n + 1 - \sum_{i=1}^{g}(\alpha_i^n + \overline{\alpha_i}^n).$$

Es gibt eine weitere Darstellung (siehe Lemma 2.45):

$$N_n = \sum_{d|n} d a_d \tag{3}$$

wobei a_d die Anzahl der Primdivisoren der Kurve von Grad d ist.

Nun wollen wir einen Zusammenhang zwischen dem Zetapolynom

$$F(T) = \prod_{i=1}^{g}(T - u_i), \quad u_i = \alpha_i + \overline{\alpha_i}$$

und den Größen a_d herleiten.

Ausmultipliziert ist das Polynom

$$F(T) = \sum_{i=0}^{g} b_i T^{g-i},$$

wobei die $\{b_i\}$ die elementarsymmetrischen Polynome in den $\{u_i\}$ sind, der Leitkoeffizient ist $b_0 = 1$. Das Ziel ist es, die Koeffizienten dieses Polynoms in Abhängigkeit von den $\{a_d\}$ darzustellen.

Dabei verwenden wir die folgenden Polynome:

$$s_n = \sum_{i=1}^{g} u_i^n$$

Diese hängen gemäß den Newtonschen Identitäten ([Bou90] A.IV.70) mit den elementarsymmetrischen Polynomen zusammen :

$$b_1 s_{n-1} + b_2 s_{n-2} + \cdots + b_{n-1} s_1 + n b_n = -s_n \tag{4}$$

Sie lassen sich also durch Lösen eines linearen Gleichungssystems aus den $\{s_n\}$ bestimmen. Die $\{s_n\}$ wiederum hängen mit den $\{N_n\}$ auf folgende Weise zusammen:

$$s_n = \sum_{k=0}^{\frac{n}{2}-1} \Big[\binom{n}{k} q^k (q^{n-2k} + 1 - N_{n-2k}) \Big] + \binom{n}{\frac{n}{2}} q^{\frac{n}{2}} g \quad \text{falls} \quad n \quad \text{gerade} \tag{5}$$

$$s_n = \sum_{k=0}^{\frac{n-1}{2}} \Big[\binom{n}{k} q^k (q^{n-2k} + 1 - N_{n-2k}) \Big] \quad \text{falls} \quad n \quad \text{ungerade} \tag{6}$$

Beweis. Sei n gerade.

$$\begin{aligned}
s_n &= \sum_{i=1}^{g} u_i^n = \sum_{i=1}^{g}\sum_{k=0}^{n} \alpha_i^{n-k}\overline{\alpha}_i^k \binom{n}{k} \\
&= \sum_{i=1}^{g}\Big(\alpha_i^n + \sum_{k=1}^{\frac{n}{2}-1}(\alpha_i\overline{\alpha}_i)^k\alpha_i^{n-2k}\binom{n}{k} + \alpha_i^{\frac{n}{2}}\overline{\alpha}_i^{\frac{n}{2}}\binom{n}{\frac{n}{2}} + \sum_{k=\frac{n}{2}+1}^{n-1}(\alpha_i\overline{\alpha}_i)^{n-k}\overline{\alpha}_i^{2k-n}\binom{n}{k} + \overline{\alpha}_i^n\Big) \\
&= \sum_{i=1}^{g}(\alpha_i^n + \overline{\alpha}_i^n) + \sum_{i=1}^{g}(\alpha_i\overline{\alpha}_i)^{\frac{n}{2}}\binom{n}{\frac{n}{2}} + \sum_{i=1}^{g}\sum_{k=1}^{\frac{n}{2}-1}(\alpha_i\overline{\alpha}_i)^k(\alpha_i^{n-2k} + \overline{\alpha_i}^{n-2k})\binom{n}{k} \\
&= q^n + 1 - N_n + gq^{\frac{n}{2}}\binom{n}{\frac{n}{2}} + \sum_{k=1}^{\frac{n}{2}-1}\binom{n}{k}q^k\sum_{i=1}^{g}(\alpha_i^{n-2k} + \overline{\alpha_i}^{n-2k}) \\
&= gq^{\frac{n}{2}}\binom{n}{\frac{n}{2}} + \sum_{k=0}^{\frac{n}{2}-1}\binom{n}{k}q^k(q^{n-2k} + 1 - N_{n-2k})
\end{aligned}$$

Sei n ungerade.

$$\begin{aligned}
s_n &= \sum_{i=1}^{g} u_i^n = \sum_{i=1}^{g}\sum_{k=0}^{n} \alpha_i^{n-k}\overline{\alpha}_i^k \binom{n}{k} \\
&= \sum_{i=1}^{g}\Big(\alpha_i^n + \overline{\alpha}_i^n + \sum_{k=1}^{\frac{n-1}{2}}(\alpha_i\overline{\alpha}_i)^k\alpha_i^{n-2k}\binom{n}{k} + \sum_{k=\frac{n+1}{2}}^{n-1}(\alpha_i\overline{\alpha}_i)^{n-k}\overline{\alpha}_i^{2k-n}\binom{n}{k}\Big) \\
&= q^n + 1 - N_n + \sum_{k=1}^{\frac{n-1}{2}}q^k\binom{n}{k}\sum_{i=1}^{g}(\alpha_i^{n-2k} + \overline{\alpha}_i^{n-2k}) \\
&= \sum_{k=0}^{\frac{n-1}{2}}\binom{n}{k}q^k(q^{n-2k} + 1 - N_{n-2k})
\end{aligned}$$

□

So lassen sich die $\{b_i\}$ als Polynome in den $\{a_d\}$ ausdrücken. Die Idee des Algorithmus ist nun, systematisch alle Möglichkeiten für die Wahl der $\{a_d\}$ auszuprobieren, so dass das zugehörige Polynom $F(T)$ ausschließlich reelle Nullstellen im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$ hat.

Betrachtet man das Polynom $F(T)$ genauer, so beobachtet man folgenden Zusammenhang zwischen seinen Koeffizienten und den Parametern $\{a_i\}$:

Lemma 4.1. Wovon $F(T)$ abhängt
Für alle $1 \leq k \leq g$ gilt:

N_k hängt höchstens von $a_1, \ldots, a_k$ ab

$$N_k = polynom(a_1, \ldots, a_{k-1}) + ka_k$$

s_k hängt höchstens von $N_1, \ldots, N_k$ ab

$$s_k = polynom(N_1, \ldots, N_{k-1}) - N_k$$

b_k hängt ab von $s_1, \ldots, s_k$

$$b_k = polynom(s_1, \ldots, s_{k-1}) - \frac{1}{k} s_k$$

Der Koeffizient b_k hängt also nur von $a_1, \ldots, a_k$ ab, wobei gilt:

$$b_k = polynom(a_1, \ldots, a_{k-1}) + a_k$$

Die Gültigkeit dieser Aussagen ist direkt aus den Gleichungen (3) bis (6) ersichtlich.

Entsprechende Ergebnisse folgen für die Ableitungen von $F(T)$:

Lemma 4.2. Wovon $F^{(k)}(T)$ abhängt
Das Polynom $F(T)$ und seine k-te Ableitung $F^{(k)}(T)$ sind

$$F(T) = \sum_{i=0}^{g} b_i T^{g-i} \qquad F^{(k)}(T) = \sum_{i=0}^{g-k} \frac{(g-i)!}{(g-k-i)!} b_i T^{g-k-i}$$

Also hängen die Koeffizienten von $F^{(k)}(T)$ von $a_1, \ldots, a_{g-k}$ ab und es gilt

$$F^{(k)}(T) = polynom(a_1, \ldots, a_{g-k-1}) + k! \cdot a_{g-k}.$$

Man kann also durch $(g-2)$-faches Ableiten von $F(T)$ erreichen, dass $F^{(g-2)}(T)$ nur von a_1 (das bereits fest gewählt ist, denn $a_1 = N_1$) und von dem noch unbestimmten a_2 abhängt.

Nun werden alle natürlichen Werte für a_2 bestimmt, so dass $F^{(g-2)}(T)$ zulässige Nullstellen hat.

Für jede dieser Varianten für die Wahl von a_2 werden daraufhin die Möglichkeiten für die Wahl von a_3 untersucht, so dass das Polynom $F^{(g-3)}(T)$ (welches von a_1, a_2 und a_3 abhängt) zulässige Nullstellen hat.

Auf diese Weise kann die Suche fortgesetzt werden, so dass alle Lösungen für $a_2, \ldots, a_g$ gefunden werden, für die $F(T)$ zulässige Nullstellen hat.

4.2 Wahl der Parameter des Zetapolynoms

Bisher wurde noch nicht näher erläutert, wie die Bestimmung aller natürlichen Werte für a_i, für die $F^{(g-i)}(T)$ zulässige Nullstellen hat, erfolgt, oder allgemeiner ausgedrückt, wie der konstante Term eines gegebenen Polynoms gewählt werden muss, damit es das Nullstellenkriterium erfüllt.

Dazu zunächst einige Vorbemerkungen zu Polynomen:

Satz 4.3. *Sei $c(x)$ ein reelles Polynom von Grad n mit n reellen Nullstellen $\alpha_1 \leq \alpha_2 \leq \cdots \leq \alpha_n$. Dann gilt:*

1. *Zwischen je zwei benachbarten Nullstellen α_i, α_{i+1} gibt es einen kritischen Punkt (d.h. die erste Ableitung verschwindet dort).*
2. *$c(x)$ hat $n-1$ kritische Punkte.*
3. *Zwischen je zwei benachbarten kritischen Punkten gibt es eine Nullstelle.*

Beweis. Die erste Behauptung folgt für $\alpha_i < \alpha_{i+1}$ durch den Satz von Rolle aus der Analysis. Falls $\alpha_i = \alpha_{i+1}$, liegt eine doppelte Nullstelle vor und auch die Ableitung c' verschwindet dort. Die zweite und dritte Behauptung folgen unmittelbar daraus. □

Gegeben sei nun ein Polynom $c(x)$ von mindestens Grad 2. Gesucht werden alle natürlichen Zahlen r, für die das Polynom $c(x) + r$ zulässige Nullstellen hat.

Das Polynom $c(x)$ wird nun einer genauen Untersuchung unterzogen. Es liegt einer der folgenden vier Fälle vor:

1. Es gibt einen kritischen Punkt P, wo auch c'' Null wird.
   Der kritische Punkt ist eine mehrfache Nullstelle von c', also muss nach dem vorangehenden Satz (Punkt 3) dort auch eine Nullstelle von c vorliegen. Wähle $r = -c(P)$, falls $-c(P) \in \mathbb{N}_0$ ist.

2. Es gibt keinen kritischen Punkt, wo auch c'' Null wird.

   (a) Es gibt einen Tiefpunkt TP, aber keinen Hochpunkt.
   Falls möglich, muss r so in $\mathbb{N}_0$ gewählt werden, dass der Tiefpunkt nicht oberhalb der $x-$Achse liegt. Wähle also $0 \leq r \leq -c(TP)$.

   (b) Es gibt einen Hochpunkt HP, aber keinen Tiefpunkt.
   Der Hochpunkt darf nicht unterhalb der x-Achse liegen, entsprechend ist $r \in \mathbb{N}_0$ zu wählen: $r \geq -c(HP)$.

   (c) Es gibt Hoch- und Tiefpunkte.
   Diesmal ist $r \in \mathbb{N}_0$ so zu wählen, dass die $x-$Achse zwischen dem größten Tiefpunkt TP und dem kleinsten Hochpunkt HP verläuft: $-c(HP) \leq r \leq -c(TP)$.

Jedesmal muss nach der Wahl eines r, das die obigen Bedingungen erfüllt, überprüft werden, ob die Nullstellen von $c(x) + r$ wirklich zulässig sind.

4.3 Überprüfung der Zulässigkeit der Nullstellen

Im Laufe der Implementierung stellte sich heraus, dass die Suche der Nullstellen bei Polynomen mit mehrfachen Nullstellen unstabil und unzuverlässig ist, wenn sie mit Methoden der Numerik, wie sie beispielsweise `roots` von matlab anbietet, durchgeführt wird.

Das folgende Vorgehen war jedoch erfolgreich:

Es soll untersucht werden, ob das Polynom $P(x)$ reelle Nullstellen im Intervall $[a, b]$ hat.

1. Berechne $Q(x) := \frac{P(x)}{ggt(P(x),P'(x))}$. Das Polynom $Q(x)$ hat die gleichen Nullstellen wie $P(x)$, jedoch alle mit der Vielfachheit eins. (Dabei treten keine Rundungsfehler auf, da die Polynome rationale Koeffizienten haben und pari damit exakt rechnet.)

2. Überprüfe, ob $Q(x)$ im Intervall $[a, b]$ genau $\deg(Q(x))$ reelle Nullstellen hat. Dabei wird in der Implementierung die pari-Funktion `polsturm` verwendet. Diese Funktion zählt Nullstellen eines quadratfreien Polynoms (daher ist das Vorgehen in Punkt 1 nötig) innerhalb des vorgegebenen Intervalls. Sie arbeitet dabei mit Sturmschen Ketten, die auf dem euklidischen Algorithmus aufbauen. Es werden bestimmte darin auftretende Polynome an den Intervallgrenzen ausgewertet und Vorzeichenwechsel gezählt. Das Polynom darf an den Intervallgrenzen nicht

verschwinden. Deshalb wird das Intervall $[a, b]$ um einen winzigen Betrag vergrößert, denn der Algorithmus soll natürlich auch Zetapolynome finden, die Nullstellen auf den Intervallgrenzen haben.

4.4 Warum der Algorithmus terminiert

Es müssen nur endlich viele Koeffizienten, nämlich a_2 bis a_g, bestimmt werden. Für die Wahl des Koeffizienten a_i gibt es an jeder Stelle im Algorithmus nur endlich viele Möglichkeiten, denn im Fall

1. wird überhaupt nur ein Wert für r ausprobiert;
2. (a) gibt es nur endlich viele natürliche Zahlen zwischen 0 und $-c(TP)$;
   (b) gibt es zwar unendlich viele natürliche Zahlen $r \geq -c(HP)$, aber die Suche bricht ab, sobald $c(x)+r$ mindestens eine seiner beiden Nullstellen außerhalb des vorgegebenen Intervalls annimmt, was nach endlich vielen Schritten der Fall ist;
   (c) liegen zwischen $-c(HP)$ und $-c(TP)$ nur endlich viele natürliche Zahlen.

Sobald eine Kombination von Koeffizienten $a_2, \ldots, a_g$ gefunden ist, für die $F(T)$ zulässige Nullstellen hat, muss überprüft werden, ob $F(T)$ das Resultantenkriterium erfüllt. Dazu wird $F(T)$ zunächst faktorisiert und dann wird getestet, ob man die Faktoren so zusammenstellen kann, dass $F(T) = r(T)s(T)$ mit Resultante $Res(r, s) = \pm 1$.

Falls das geht, ist $F(T)$ kein Zetapolynom zu den gegebenen Daten. Die Suche nach Koeffizienten $a_2, \ldots, a_g$ wird fortgesetzt.

Falls eine solche Zerlegung nicht möglich ist, ist $F(T)$ als Zetapolynom zu einer Kurve der Daten $(g, q, N = a_1)$ nicht auszuschließen. Der Algorithmus endet hier, N ist die neue obere Schranke.

Wird ein Zetapolynom gefunden, so heißt das nicht, dass eine Kurve dazu tatsächlich existiert. Seine Existenz ist notwendig für die Existenz einer Kurve, aber nicht hinreichend.

Ist die Suche nach Koeffizienten $a_2, \ldots, a_g$ beendet, ohne dass ein Zetapolynom, das beide Kiterien erfüllt, gefunden wurde, so kann es keine Kurve zu den Daten $(g, q, N = a_1)$ geben. Die obere Schranke N kann also zur neuen oberen Schranke $N - 1$ korrigiert werden. Diese obere Schranke kann man

mit der gleichen Methode überprüfen und so die obere Schranke so weit wie möglich herabsetzten.

4.5 Überblick über die Struktur des Algorithmus

5 Die Implementierung

5.1 Beschreibung der Funktionen

Der Kern des im vorigen Abschnitt beschriebenen Algotithmus ist die Suche nach einem Zetapolynom zu den gegebenen Daten (g, q, N), das sowohl das Nullstellenkriterium als auch das Resultantenkriterium erfüllt. Dazu wurde ein Programm in der Sprache pari geschrieben. Es gliedert sich in die Funktionen `findzeta`, `findallsol`, `computenextcoeff`, `convert2poly`, `zetapoly`, `singlerestest`, `resultant` und `products`. Diese Funktionen sollen nun erläutert werden.

`findzeta`$(g, q, N, filename)$

Die Funktion überprüft, ob es zu gegebenen Daten (Geschlecht g, Körper $\mathbb{F}_q$, $N = a_1$) eine Lösung für $a_2, \ldots, a_g$ gibt, so dass das zugehörige Polynom $F(T)$ zulässige Nullstellen hat (d.h. alle Nullstellen reell und im Intervall $[-2\sqrt{q}, 2\sqrt{q}]$). Gefundene Lösungen werden mit Hilfe des Resultantenkriteriums weiter untersucht. Falls die Lösung durch das Resultantenkriterium nicht ausgeschlossen werden kann, wird sie in das Dokument $filename$ geschrieben und `findzeta` terminiert.

1. Berechne das Polynom $F(T)$ für $a_1 = N, a_2 = 0, \ldots, a_g = 0$.
2. Sind die Nullstellen von $F^{(g-1)}$ zulässig?
   Falls nein $\rightarrow$ Abbruch.
3. Rufe `findallsol`(g, q, N) auf.
4. Gib an, ob eine Lösung existiert oder nicht.

`findallsol`$(g, q, a, lim, filename)$

Die Koeffizienten $a_1, \ldots, a_l$ stehen schon fest und werden in der Variablen a übergeben. Die Funktion sucht rekursiv die Lösungen für die fehlenden Koeffizienten $a_{l+1}, \ldots, a_g$. Falls eine Lösung gefunden wird, wird das dazugehörige Zetapolynom berechnet und mit Hilfe von `singlerestest` wird überprüft, ob es das Resultantenkriterium erfüllt. Wenn das der Fall ist, wird die Lösung in der Datei $filename$ ausgegeben und `findallsol` terminiert.

1. Falls $l = g$ (d.h. alle Koeffizienten sind berechnet):
   Lösung ausgeben. `singlerestest` aufrufen. Falls Resultantenkriterium

nicht erfüllt, kann Lösung ausgeschlossen werden. Zurück zum Aufrufer, wo die Suche ggf. fortgesetzt wird.

2. Falls $l < g$:
   Es müssen noch Koeffizienten $a_{l+1}, \ldots, a_g$ bestimmt werden.

   (a) Berechne $F(T)$ für a, $a_{l+1} = 0, \ldots, a_g = 0$.

   (b) Bestimme $F(T)^{(g-l-1)}$.
   Bem.: diese Ableitung hängt nur von $a_1, \ldots, a_{l+1}$ ab, der konstante Term ist $const + (g-l-1)! \cdot a_{l+1}$

   (c) Berechne $faktor := (g-l-1)!$.

   (d) Rufe $R :=$`computenextcoeff(`$F(T)^{g-l-1}, lim, faktor$`)` auf.
   In R sind nun alle nichtnegativen Vielfachen von $faktor$, so dass $F(T)^{g-l-1} + r$ für $r \in R$ zulässige Nullstellen hat.

   (e) falls $R = \{\}$
   zurück. Es gibt keine Lösung.

   (f) Bestimme $T := \{\frac{r}{(g-l-1)!} | r \in R\}$.

   (g) Für alle $t \in T$:
   Rufe `findallsol(`$g, q, [a, t]$`)` auf (Rekursion!)
   Falls eine Lösung gefunden wurde, beende die Suche.

   (h) Gib die Anzahl gefundener Lösungen (0 oder 1) zurück.

`computenextcoeff(`$c(x), lim, faktor$`)`

Diese Funktion berechnet für ein Polynom $c(x)$ von Grad $n \geq 2$ die Menge R aller natürlichen Zahlen r, die durch $faktor$ teilbar sind und für die $c(x) + r$ zulässige Nullstellen (d.h. reell und im Intervall $[-lim, lim]$) hat.

1. Fall 1: $c'(x)$ hat eine mehrfache Nullstelle ($ggt(c', c'') \neq 1$).

   (a) Wähle eine solche mehrfache Nullstelle α aus. $c(x)$ muss auch in α Null werden. Setze also $r := -c(\alpha)$.

   (b) Ist $r \in \mathbb{N}_0$ und durch $faktor$ teilbar und sind die Nullstellen von $c(x) + r$ zulässig? Dann $R := \{r\}$, sonst $R := \{\}$.

2. Für Fall 2 (a) bis (c): Suche die Hoch- und Tiefpunkte von $c(x)$, den kleinsten Hochpunkt HP und den größten Tiefpunkt TP.

3. Fall 2 (a): Es gibt einen Tiefpunkt TP, aber keinen Hochpunkt.
   Bem.: $c(x)$ ist eine nach oben geöffnete Parabel.
   $R := \{r \in \mathbb{N}_0 |\ r \leq -c(TP), faktor | r$, NS von $c(x) + r$ sind zulässig $\}$

4. Fall 2 (b): Es gibt einen Hochpunkt HP, aber keinen Tiefpunkt.
   Bem.: $c(x)$ ist eine nach unten geöffnete Parabel.
   $R := \{r \in \mathbb{N}_0 | r \geq -c(HP), faktor | r$, NS von $c(x) + r$ sind zulässig $\}$

5. Fall 2 (c): Es gibt Hochpunkt HP und Tiefpunkt TP.
   Bem.: In Frage kommen alle natürlichen Vielfachen von $faktor$, die zwischen $-c(HP)$ und $-c(TP)$ liegen.
   $R := \{r \in \mathbb{N}_0 | -c(HP) \leq r \leq -c(TP), faktor | r$, NS von $c(x) + r$ zulässig$\}$.

6. Gib Lösungsmenge R zurück.

`convert2poly(`c`)`

Hilfsfunktion, die einen Vektor c von Koeffizienten in ein Polynom in der symbolischen Variablen x umwandelt.

`zetapoly(`g, q, a`)`

Berechnet in Abhängigkeit von g, q und a_1 bis a_g die Koeffizienten b_0 bis b_g des Zetapolynoms $F(T)$.

1. Für $i = 1, \ldots, g$:
$$N_i := \sum_{d|i} d a_d$$

2. Für $n = 1, \ldots, g$:
$$s_n := \sum_{k=0}^{\frac{n}{2}-1} \left[\binom{n}{k} q^k (q^{n-2k} + 1 - N_{n-2k}) \right] + \binom{n}{\frac{n}{2}} q^{\frac{n}{2}} g \quad \text{falls} \quad n \quad \text{gerade}$$
$$s_n := \sum_{k=0}^{\frac{n-1}{2}} \left[\binom{n}{k} q^k (q^{n-2k} + 1 - N_{n-2k}) \right] \quad \text{falls} \quad n \quad \text{ungerade}$$

3. Lösen des Gleichungssystems
$$\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ s_1 & 2 & 0 & 0 & \cdots & 0 \\ s_2 & s_1 & 3 & 0 & \cdots & 0 \\ s_3 & s_2 & s_1 & 4 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ s_{g-1} & \cdots & s_3 & s_2 & s_1 & g \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \vdots \\ b_g \end{pmatrix} = \begin{pmatrix} -s_1 \\ -s_2 \\ -s_3 \\ -s_4 \\ \vdots \\ -s_g \end{pmatrix}$$

4. Der Leitkoeffizient ist $b_0 := 1$

5. Rückgabe von $b_0, b_1, \ldots, b_g$

Die drei folgenden Funktionen werden zur Überprüfung des Resultantenkriteriums benötigt.

`singlerestest`$(v, filename)$

Diese Funktion stellt fest, ob das Polynom $v(x)$ so in Faktoren $r(x) \cdot s(x)$ zerlegt werden kann, dass die Resultante $Res(r, s) = \pm 1$ ist.

1. Faktorisiere $v(x)$ in ein Produkt irreduzibler Polynome

2. Fall 1: $v(x)$ ist irreduzibel, es muss als Lösung akzeptiert werden.

3. Fall 2: $v(x)$ ist reduzibel und hat nur zwei unterschiedliche irreduzible Faktoren $r(x), s(x)$:
   Überprüfe, ob `resultant`$(r, s) = \pm 1$.
   Falls ja ist $v(x)$ keine Lösung, falls nein, ist es eine Lösung.

4. Fall 3: $v(x)$ ist reduzibel und hat mehr als zwei unterschiedliche irreduzible Faktoren. Dann gibt es mehrere Möglichkeiten, $v(x)$ in zwei Polynome $v_1(x), v_2(x)$ zu faktorisieren, so dass `resultant`$(v_1, v_2) \neq 0$.
   Alle diese Aufteilungen findet die Funktion `products`.
   Für jede solche Faktorisierung muss nun überprüft werden, ob `resultant`$(v_1, v_2) = \pm 1$ ist und falls das mindestens einmal der Fall ist, kann $v(x)$ durch das Resultantenkriterium als Lösung ausgeschlossen werden, andernfalls nicht.

`resultant`(p, q)

Mit Hilfe dieser Funktion wird die Resultante der beiden nichtkonstanten Polynome $p(x)$ und $q(x)$ berechnet.

1. Bestimme die Nullstellen von p und q. Es gilt nun

$$p(x) = \prod_{i=1}^{n}(x - a_i) \qquad\qquad q(x) = \prod_{j=1}^{m}(x - b_j)$$

2. Die Resultante berechnet sich wie folgt

$$\texttt{resultant}(p, q) = \prod_{i=1}^{n}\prod_{j=1}^{m}(a_i - b_j)$$

`products`$(g_1, \ldots, g_n)$

Die Funktion erhält die Polynome $g_1, \ldots, g_n$. Es werden alle Möglichkeiten bestimmt, diese Polynome in zwei nichtleere Mengen zu partitionieren. Die Polynome dieser Mengen werden dann zu zwei Produkten zusammengefasst und in die Spalten der Matrix B geschrieben, so dass für alle Spalten k gilt $B_{1,k} \cdot B_{2,k} = \prod_{i=1}^{n} g_i$.

Die Funktion arbeitet rekursiv.

1. Falls $n = 2$:
$$B := \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$$
2. Falls $n > 2$: Rekursiver Aufruf $P = \begin{pmatrix} \vec{p}_1 \\ \vec{p}_2 \end{pmatrix}$:=`products`$(g_2, \ldots, g_n)$
3. Berechne B als
$$B := \begin{pmatrix} \vec{p}_1 \cdot g_1 & \vec{p}_1 & g_1 \\ \vec{p}_2 & \vec{p}_2 \cdot g_1 & \prod_{i=2}^{n} g_i \end{pmatrix}$$
4. Gib die Lösungsmatrix B zurück

5.2 Übersicht über den Aufbau der Funktionen

<table>
<tr><td colspan="3"><code>findzeta</code>$(g, q, N, filename)$
return(1) falls Lösung gefunden wird
return(0) falls es keine Lösung gibt</td></tr>
<tr><td colspan="3">$a := (N, 0, 0, \ldots, 0)$
$F(T) :=$ <code>convert2poly</code>(<code>zetapoly</code>(g, q, a))
berechne $F^{(g-1)}(T)$
sind die Nullstellen von $F^{(g-1)}(T)$ zulässig?</td></tr>
<tr><td colspan="2">ja</td><td>nein</td></tr>
<tr><td colspan="2">$lim := 2 \cdot \sqrt{q}$
<code>findallsol</code>$(g, q, a, lim, filename)$
Lösung gefunden?</td><td rowspan="2">“there is no solution”
return(0)</td></tr>
<tr><td>ja</td><td>nein</td></tr>
<tr><td>“found 1 solution”
return(1)</td><td>“no solution found”
return(0)</td><td></td></tr>
</table>

`findallsol`$(g, q, a, lim, filename)$
return(1) falls Lösung gefunden wird
return(0) falls es keine Lösung gibt

$l := length(a)$

$l = g$		$l < g$	
Lösung a ausgeben $ZP =$ `zetapoly`(g, q, a) $F(T) =$ `convert2poly`(ZP) $s :=$ `singlerestest`$(F(T))$		$F(T) =$ `convert2poly`(`zetapoly`$(g, q, a))$ $G := F^{(g-l-1)}(T)$ $faktor := (g - l - 1)!$ $R =$ `computenextcoeff`$(G, lim, faktor)$	
$s = 1$	$s = 0$	$R = \{\}$	$R \neq \{\}$
return(0)	return(1)	return(0)	$T := \{\frac{r}{faktor} \mid r \in R\}$
			für alle $t \in T$ $f =$ `findallsol`$(g, q,$ $[a_1, \ldots, a_l, t], lim, filename)$ $f = 0$ | $f = 1$ | return(1)
			return(0)

`computenextcoeff`$(c(x), lim, faktor)$
$return(R)$ R ist die Menge der natürlichen Vielfachen von $faktor$, so dass $c(x) + r$ zulässige Nullstellen hat

hat $c'(x)$ eine mehrfache Nullstelle M?

ja		nein		
Fall 1		suche Hoch- und Tiefpunkte von $c(x)$ H der kleinste Hochpunkt, T der größte Tiefpunkt		
$r := -c(M)$				
gilt $r \in \mathbb{N}_0$, $faktor \mid r$, hat $c(x) + r$ zulässige NS?		**Fall 2 (a)** $c(x)$ hat nur T	**Fall 2 (b)** $c(x)$ hat nur H	**Fall 2 (c)** $c(x)$ hat H, T
ja	nein	für alle $r \in \mathbb{N}_0$ mit $faktor \mid r$, $r \leq -c(T)$	für alle $r \in \mathbb{N}_0$ mit $faktor \mid r$, $r \geq -c(H)$	für alle $r \in \mathbb{N}_0$ mit $faktor \mid r$, $-c(H) \leq r$, $r \leq -c(T)$
$R = \{r\}$	$R = \{\}$	hat $c(x) + r$ zulässige NS? ja: $r \in R$ | nein: $r \notin R$	hat $c(x) + r$ zulässige NS? ja: $r \in R$ | nein: $r \notin R$ return(R)	hat $c(x) + r$ zulässige NS? ja: $r \in R$ | nein: $r \notin R$
return(R)				

`zetapoly`(g, q, a)
berechne $N_1, \ldots, N_g$ aus $a_1, \ldots, a_g$: $N_i = \sum_{d\|i} d a_d$
berechne $s_1, \ldots, s_g$ aus $q, N_1, \ldots, N_g$
löse $\begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ s_1 & 2 & 0 & 0 & \cdots & 0 \\ s_2 & s_1 & 3 & 0 & \cdots & 0 \\ s_3 & s_2 & s_1 & 4 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \ddots & \vdots \\ s_{g-1} & \cdots & s_3 & s_2 & s_1 & g \end{pmatrix} \begin{pmatrix} b_1 \\ b_2 \\ b_3 \\ b_4 \\ \vdots \\ b_g \end{pmatrix} = \begin{pmatrix} -s_1 \\ -s_2 \\ -s_3 \\ -s_4 \\ \vdots \\ -s_g \end{pmatrix}$
$return(b_0 = 1, b_1, \ldots, b_g)$

<table>
<tr><td colspan="4"><code>singlerestest</code>$(v(x))$
return(1): $v(x)$ ist keine gültige Lösung
return(0): $v(x)$ ist gültige Lösung</td></tr>
<tr><td colspan="4">faktorisiere $v(x)$
($v(x) = f_1^{e_1}(x) \cdot f_2^{e_2}(x) \cdots f_n^{e_n}(x)$; f_i irreduzibles Polynom)</td></tr>
<tr><td>$n = 1$</td><td colspan="2">$n = 2$</td><td>$n > 2$</td></tr>
<tr><td>return(0)</td><td colspan="2">r:=<code>resultant</code>(f_1, f_2)</td><td>P:=<code>products</code>$(f_1^{e_1}(x), \ldots, f_n^{e_n}(x))$</td></tr>
<tr><td rowspan="2"></td><td>$r = \pm 1$

return(1)</td><td>$r \neq \pm 1$

return(0)</td><td>für alle Spalten von P: $i = 1, 2, 3, \ldots$
<table><tr><td colspan="2">r:=<code>resultant</code>$(P_{1,i}, P_{2,i})$</td></tr><tr><td>$r \neq \pm 1$</td><td>$r = \pm 1$
return(1)</td></tr></table></td></tr>
<tr><td colspan="3">return(0)</td></tr>
</table>

`resultant`$(p(x), q(x))$
Nullstellen bestimmen: $a := polroots(p(x))$ $b := polroots(q(x))$
$r := \prod_{i=1}^{length(a)} \prod_{j=1}^{length(b)} (a_i - b_j)$
return(r)

$\texttt{products}(g_1, \ldots, g_n)$	
$n = 2$	$n > 2$
$B := \begin{pmatrix} g_1 \\ g_2 \end{pmatrix}$	$P = \begin{pmatrix} \vec{p}_1 \\ \vec{p}_2 \end{pmatrix} := \texttt{products}(g_2, \ldots, g_n)$ $B := \begin{pmatrix} \vec{p}_1 \cdot g_1 & \vec{p}_1 & g_1 \\ \vec{p}_2 & \vec{p}_2 \cdot g_1 & \prod_{i=2}^{n} g_i \end{pmatrix}$
return(B)	return(B)

Abbildung 1: Diagramm der Funktionsaufrufe

6 Ergebnisse

Die folgenden Tabellen enthalten Abschätzungen für die maximale Anzahl von Punkten auf nichtsingulären projektiven Kurven über endlichen Körpern. Dabei werden die Ergebnisse dieser Arbeit bereits bekannten Abschätzungen gegenübergestellt.

In Tabelle 1 geht es um Kurven über Körpern der Charakteristik 2. Es wurden Körper der Ordnung $q \in \{2, 4, 8, 16, 32, 64, 128\}$ betrachtet. In Tabelle 2 sind es die Körper der Charakteristik 3 mit Ordnung $q \in \{3, 9, 27, 81, 243\}$. Um andere Charakteristiken $q \in \{5, 7, 11, 13, 17\}$ geht es in Tabelle 3. Die jeweils betrachtete Ordnung findet sich am Kopf der Spalte.

Das Geschlecht g der untersuchten Kurven reicht von 1 bis 40. Zu jedem Geschlecht gehören zwei bzw. drei Zeilen der Tabelle. Die erste Zeile enthält die oberen Grenzen, die sich aus dem Satz von Weil ableiten lassen (vgl. Korollar 2.61).

Bei Tabelle 2 und 3 sind in der mittleren Zeile bekannte Intervalle für die Höchstanzahl von Punkten aufgelistet, wie sie in [vdGvdV03] für Charakteristik 2 und 3 gesammelt sind. Die unteren Intervallgrenzen sind im Wesentlichen durch die Konstruktion von Kurven entstanden. Im Rahmen dieser Arbeit liegt das Augenmerk jedoch auf den Obergrenzen. Wenn in der Tabelle anstelle eines Intervalls nur ein Wert steht, bedeutet das, dass die Höchstzahl von Punkten auf Kurven dieser Daten bekannt ist.

Die untere Zeile schließlich fasst die Ergebnisse dieser Diplomarbeit zusammen. Der erläuterte Algorithmus wurde wie beschrieben implementiert und auf die in diesen Tabellen aufgelisteten Fälle angewandt. Zur Ermittlung der dargestellten Ergebnisse war bei vielen Beispielen ein nicht unerheblicher Rechenaufwand erforderlich. Daher konnten nicht bei allen untersuchten Fällen die gestarteten Rechnungen bis zum Ende ausgeführt werden.

In den Tabellen sind durch **Fettdruck** gekennzeichnete Ergebnisse Verbesserungen der bisher bekannten Grenzen. Das heißt, in diesen Fällen wurde entweder eine bei [vdGvdV03] veröffentlichte Grenze gesenkt, oder es wurde, falls dort nichts angegeben ist, die Weilschranke unterboten.

Ein * kennzeichnet gültige Obergrenzen, die jedoch unter Umständen nicht das jeweils beste Ergebnis sind, das mit der hier vorgestellten Methode erreicht werden kann. Es sind Zwischenergebnisse nicht beendeter Rechnungen. Das bedeutet, dass kein Zetapolynom zu den gegebenen Daten gefunden wurde, die Suche aber aus Zeitgründen nicht beendet werden konnte.

Tabelle 1: Obergrenzen für Kurven mit Körpercharakteristik 2

g \ q	2	4	8	16	32	64	128
	5	9	14	25	44	81	151
1	5	9	14	25	44	81	150
	5	9	14	25	44	81	151
	8	13	20	33	55	97	174
2	6	10	18	33	53	97	172
	6	11	19	33	55	97	173
	11	17	25	41	66	113	196
3	7	14	24	38	64	113	192
	7	14	24	41	66	113	195
	14	21	31	49	78	129	219
4	8	15	25	45	71-74	129	215
	8	15	29	49	77	129	217
	17	25	37	57	89	145	242
5	9	17	29-30	49-53	83-85	132-145	227-234
	9	18	32	57	88	145	239
	19	29	42	65	100	161	264
6	10	20	33-35	65	86-96	161	243-258
	10	20	35	65	99	161	261
	22	33	48	73	112	177	287
7	10	21-22	34-38	63-69	98-107	177	258-283
	10	22	39	70	110	177	283
	25	37	54	81	123	193	310
8	11	21-24	34-42	61-75	97-118	169-193	257-302
	11	24	42	75	121	193	305
	28	41	59	89	134	209	332
9	12	26	45	72-81	108-128	209	288-322
	12	26	46	81	132	209	327
	31	45	65	97	146	225	355
10	13	27	42-49	81-87	113-139	225	289-345
	13	28	50	87	143	225	349
	34	49	71	105	157	241	377
11	14	26-29	48-53	80-91	120-150	201-236	
	14	29	53	92	154	241	**371**
	36	53	76	113	168	257	400
12	14-15	29-31	49-57	83-97	129-161	257	321-388
	15	31*	57	97	165	257	393
	39	57	82	121	180	273	423
13	15	33	56-61	97-102	129-172	225-268	
	15*	33*	61	102	176	273	**415**

g \ q	2	4	8	16	32	64	128
14	42 15-16 16*	61 32-35 35*	88 65 65	129 97-107 107	191 146-183 187	289 241-284 289	445 353-437 437
15	45 17 18*	65 33-37 37*	93 57-67 67	137 98-113 113	202 158-194 196	305 258-300 305	468 386-455 459
16	48 17-18 19*	69 36-38 39*	99 56-71 71	145 95-118 118	214 147-204 204	321 267-316 321	491 **481**
17	51 17-18 20*	73 40 41*	105 63-74 74	153 112-124 **123**	225 154-212 212	337 **337**	513 **503**
18	53 18-19 21*	77 41-42 42*	110 65-77 77*	161 113-129 129	236 161-220 220	353 281-348 353	536 **525**
19	56 20 22*	81 37-43 44*	116 60-80 80*	169 129-134 134	247 172-228 228	369 315-364 369	558 **547**
20	59 19-21 23*	85 40-45 46*	122 68-83 83*	177 127-140 **139**	259 177-236 236	385 297-380 385	581 **569**
21	62 21 24*	89 41-47 48*	127 72-86 86*	185 129-145 145	270 185-244 **243**	401 281-396 401	604 **591***
22	65 21-22 25*	93 42-48 49*	133 74-89 89*	193 129-150 150	281 **251**	417 321-412 417	626 **613***
23	68 22-23 26*	97 45-50 51*	139 68-92 93*	201 126-155 155	293 **259**	433 **433**	649 **636***
24	70 21-23 28*	101 49-52 53*	144 81-95 96*	209 129-161 161	304 225-267 267	449 337-444 449	672 513-653 659*
25	73 24 29*	105 51-53 55*	150 86-97 99*	217 144-166 **165**	315 **274**	465 335-460 465	694 **681***
26	76 24-25 30*	109 55 56*	156 82-100 102*	225 150-171 171	327 **282**	481 385-476 481	717 **704***
27	79 24-25 31*	113 50-56 58*	161 96-103 105*	233 145-176 176	338 213-290 290	497 401-492 497	739 **726***

g \ q	2	4	8	16	32	64	128
28	82 25-26 33*	117 53-58 60*	167 97-106 108*	241 145-181 181	349 257-298 298	513 513 513	762 577-745 749*
29	85 25-27 34*	121 52-60 61*	173 97-109 111*	249 161-187 **186**	361 227-306 **305**	529 **524**	785 **772***
30	87 25-27 35*	125 53-61 63*	178 96-112 114*	257 162-192 **191**	372 273-313 313	545 401-536 **535**	807 609-784 795*
31	90 27-28 36*	129 60-63 65*	184 89-115 117*	265 165-197 **196**	383 **321**	561 386-547 547	830 578-807 818*
32	93 26-29 37*	133 57-65 67*	190 90-118 121*	273 **202**	395 **328**	577 **558***	853 **841***
33	96 28-29 39*	137 65-66 69*	195 97-121 124*	281 193-207 207	406 **336***	593 **570**	875 **864***
34	99 27-30 40*	141 65-68 71*	201 98-124 127*	289 183-213 **212**	417 **344**	609 447-582 **581***	898 **886***
35	101 29-31 41*	145 64-69 73*	206 112-127 130*	297 **217**	428 253-352 **351**	625 **593**	920 **908***
36	104 30-31 42*	149 64-71 75*	212 107-130 133*	305 185-223 **222**	440 **359**	641 441-604 605	943 **932***
37	107 30-32 43*	153 66-72 77*	218 121-132 136*	313 208-228 **227**	451 **367**	657 **616**	966 **954***
38	110 30-33 45*	157 64-74 79*	223 129-135 139*	321 193-233 233	462 291-375 375	673 449-627 627	988 **976***
39	113 33 46*	161 65-75 81*	229 120-138 142*	329 194-239 **238**	474 **382**	689 **638**	1011 **999***
40	116 32-34 47*	165 75-77 83*	235 103-141 145*	337 225-244 **243***	485 293-390 390	705 489-650 649*	1034 **1022***

Tabelle 2: Obere Grenzen der Punktanzahl von Kurven bei Charakteristik 3

g \ q	3	9	27	81	243
	7	16	38	100	275
1	7	16	38	100	
	7	16	38	100	275
	10	22	48	118	306
2	8	20	48	118	
	8	22	48	118	306
	14	28	59	136	337
3	10	28	56	136	
	10	28	58	136	337
	17	34	69	154	368
4	12	30	64	154	
	12	31	68	154	368
	21	40	79	172	399
5	13	32-35	72-75	160-172	
	13	35	78	172	399
	24	46	90	190	431
6	14	35-40	76-85	190	
	15	40	88	190	**430**
	28	52	100	208	462
7	16	40-43	82-95	180-208	
	16	43	98	208	**461**
	31	58	111	226	493
8	17-18	40-47	92-105	226	
	18	47	108	226	**492**
	35	64	121	244	524
9	19	48-50	99-113	244	
	19	51	118	244	**523**
	38	70	131	262	555
10	20-21	54	94-123	226-262	
	21	54	128	262	**554**
	42	76	142	280	586
11	20-22	55-58	100-133	220-280	
	22	58	138	280	**585**
	45	82	152	298	618
12	22-24	56-62	109-143	298	
	23	62	148	298	**616**
	49	88	163	316	649
13	24-25	64-65	136-153	256-312	
	25*	66	156	316	**647**

g \ q	3	9	27	81	243
14	52 24-26 26*	94 56-69 70	173 **163**	334 278-330 334	680 **678**
15	55 28 28*	100 64-73 73	183 136-171 **170**	352 292-348 352	711 **709**
16	59 27-29 29*	106 74-77 77	194 144-178 178	370 370 370	742 **740**
17	62 24-30 30*	112 74-81 81	204 **185**	388 288-384 388	774 **771**
18	66 26-31 32*	118 67-84 85	215 148-192 192	406 406	805 **802**
19	69 32 33*	124 84-88 88	225 **199**	424 424	836 **833**
20	73 30-34 34*	130 70-91 91	235 **206**	442 442	867 **858**
21	76 32-35 36*	136 88-95 95*	246 163-214 **213**	460 352-455 460	898 **895**
22	80 30-36 37*	142 78-98 98*	256 **220**	478 478	929 **926**
23	83 32-37 39*	148 92-101 101*	267 **227**	496 496	961 **957**
24	87 31-38 40*	154 91-104 105*	277 208-235 **234**	514 514	992 **988**
25	90 36-40 42*	160 82-108 108*	287 196-242 **241**	532 392-527 532	1023 **1019**
26	94 36-41 43*	166 110-111 112*	298 **248**	550 550	1054 **1050**
27	97 39-42 45*	172 91-114 115*	308 **255**	568 568	1085 **1081**

g \ q	3	9	27	81	243
28	100 37-43 46*	178 105-117 119*	318 **262**	586 586	1116 **1112**
29	104 42-44 48*	184 104-120 122*	329 **269***	604 604	1148 **1143**
30	107 37-46 49*	190 91-123 125*	339 196-277 **276***	622 622	1179 **1174**
31	111 40-47 51*	196 101-127 129*	350 **283***	640 460-635 640	1210 **1205**
32	114 40-48 52*	202 92-130 132*	360 **290***	658 658	1241 **1236**
33	118 46-49 54*	208 128-133 135*	370 220-298 **297**	676 676	1272 **1267**
34	121 45-50 55*	214 111-136 139*	381 **304***	694 496-689 694	1304 **1298**
35	125 47-51 57*	220 116-139 142*	391 **311**	712 712	1335 **1329**
36	128 48-52 59*	226 118-142 145*	402 244-319 **318**	730 730	1366 **1360**
37	132 52-54 61*	232 120-145 149*	412 236-326 **325**	748 586-743 **742**	1397 **1391**
38	135 **62***	238 105-149 152*	422 **332**	766 **755**	1428 **1422**
39	139 48-56 64*	244 140-152 155*	433 271-340 340	784 **768**	1459 **1453***
40	142 56-57 66*	250 118-155 159*	443 244-346 346	802 **781***	1491 **1484***

Tabelle 3: Obergrenzen für Kurven verschiedener Charakteristik

g \ q	5	7	11	13	17
1	10	13	18	21	26
	10	13	18	21	26
2	14	18	25	28	34
	14	18	24	28	34
3	19	23	31	35	42
	16	21	30	35	42
4	23	29	38	42	50
	18	25	36	42	50
5	28	34	45	50	59
	21	28	42	49	58
6	32	39	51	57	67
	24	32	46	54	66
7	37	45	58	64	75
	27	36	51	58	74
8	41	50	65	71	83
	29	38	55	63	79
9	46	55	71	78	92
	32	42	59	68	85
10	50	60	78	86	100
	34	45	64	73	90
11	55	66	84	93	108
	36	48	68	78	96
12	59	71	91	100	116
	38*	51	72	82	102
13	64	76	98	107	125
	41*	54	77	87	107
14	68	82	104	114	133
	43*	57	81	92	113
15	73	87	111	122	141
	45*	60*	85	96	118
16	77	92	118	129	149
	48*	63*	90	101	124
17	82	97	124	136	158
	50*	66*	94	106	129
18	86	103	131	143	166
	52*	69*	98	110	134
19	90	108	138	151	174
	54*	72*	102	115	140
20	95	113	144	158	182
	56*	75*	106	120	145

g \ q	5	7	11	13	17
21	99	119	151	165	191
	58*	78*	110	124	151
22	104	124	157	172	199
	61*	80*	115	129	156
23	108	129	164	179	207
	63*	83*	119	134	162
24	113	134	171	187	215
	65*	86*	123	138	167
25	117	140	177	194	224
	67*	89*	127	143	172
26	122	145	184	201	232
	69*	92*	131*	148	178
27	126	150	191	208	240
	71*	95*	135*	152	183*
28	131	156	197	215	248
	73*	97*	138*	157	189
29	135	161	204	223	257
	75*	100*	142*	162	194
30	140	166	210	230	265
	77*	103*	146*	166	200
31	144	172	217	237	273
	80*	106*	150*	171	205
32	149	177	224	244	281
	82*	109*	154*	175	210
33	153	182	230	251	290
	84*	111*	158*	179	216
34	158	187	237	259	298
	86*	114*	162*	183*	222
35	162	193	244	266	306
	89*	117*	165*	188*	227
36	166	198	250	273	314
	91*	119*	169*	192*	232
37	171	203	257	280	323
	93*	122*	173*	196*	237
38	175	209	264	288	331
	95*	125*	177*	200*	243
39	180	214	270	295	339
	98*	127*	181*	204*	248
40	184	219	277	302	347
	100*	130*	185*	209*	253

Literatur

[Bou90] Nicolas Bourbaki. *Algebra II, Chapters 4-7 (translation of: Algèbre)*. Springer, 1990.

[Gol03] David M. Goldschmidt. *Algebraic functions and projective curves*. Springer, first edition, 2003.

[IR90] Kenneth Ireland and Michael Rosen. *A classical introduction to modern number theory*. Springer, second edition, 1990.

[Lan02] Serge Lang. *Algebra*. Springer, revised third edition, 2002.

[Lau00] Kristin Lauter. Zeta funktions of curves over finite fields with many rational points. In *Coding theory, cryptography and related areas (Guanajuato, 1998)*, pages 167–174. Springer, Berlin, 2000.

[Ser83] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, (9):397–402, 1983.

[vdGvdV03] Gerard van der Geer and Marcel van der Vlugt. *Tables of curves with many points*. Internet: http://www.science.uva.nl/∼geer/tables-mathcomp13.pdf, 31. August 2003.