Obere Schranken für die Punktezahl algebraischer Kurven über endlichen Körpern

Staatsexamensarbeit von
Jessica Seibert

Studiengang: Mathematik/Chemie
Lehramt an Gymnasien
Prüfer: Prof. Dr. E.-U. Gekeler

Saarbrücken, September 1998
Fachbereich 9, Mathematik

Inhaltsverzeichnis

Einleitung

Warum rationale Punkte einer Kurve über einem endlichen Körper zählen?

In der Zahlentheorie ist man insbesondere an den Lösungen von Gleichungen interessiert. Man möchte zum Beispiel die ganzzahligen Lösungen $(a,b) \in \mathbb{Z}^2$ von polynomialen Gleichungen der Form

$$f(x,y) \;=\; 0 \tag{0.1}$$

mit Koeffizienten aus $\mathbb{Z}$ bestimmen. Man bezeichnet (0.1) auch als eine *diophantische Gleichung*. Das Wort "diophantisch" deutet darauf hin, daß nur *ganzzahlige* Lösungen gesucht werden. Verzichtet man auf die Ganzzahligkeit, so bilden die Lösungen von (0.1) eine *algebraische Kurve*. Die Lösung einer diophantischen Gleichung in zwei Variablen ist also gleichbedeutend mit der Bestimmung ganzzahliger Punkte auf einer algebraischen Kurve. Da es aber im allgemeinen schwierig ist, solche ganzzahligen Lösungen zu finden, nimmt man eine Einschränkung vor. Man betrachtet die Gleichung (0.1) modulo der Primzahl p. Gesucht werden dann die ganzzahligen Lösungen $(a,b) \in \mathbb{Z}^2$ der Kongruenz

$$f(x,y) \equiv 0 \pmod{p}. \tag{0.2}$$

Diesen Ausdruck (0.2) nennt man eine *diophantische Kongruenz*. Durch die Betrachtung der Gleichung (0.1) modulo der Primzahlen erhofft man sich, Rückschlüsse auf alle ganzzahligen Lösungen ziehen zu können. Dies ist eine sehr wichtige und effiziente Methode in der Zahlentheorie. Reduziert man die Koeffizienten des gegebenen Polynoms $f(x,y)$ modulo p, so kann man die diophantische Kongruenz (0.2) nunmehr als Gleichung $f(x,y) = 0$ im Körper $\mathbb{Z}/p$ auffassen. Interessant ist nun die Anzahl N der Lösungen $a, b \in \mathbb{Z}/p$. Man kann eine nützliche Verallgemeinerung vornehmen, die es einem erlaubt, ein größeres Repertoire an Methoden anzuwenden. Dazu wird statt $\mathbb{Z}/p$ ein beliebiger endlicher Körper $\mathbb{F}_q$ mit $q = p^r$ Elementen zugrundegelegt. Gesucht ist nun die Anzahl N der Lösungen $(a,b) \in {\mathbb{F}_q}^2$ der Gleichung

$$f(x,y) \;=\; 0 \tag{0.3}$$

eines beliebigen Polynoms $f(x,y)$ zweier Variablen mit Koeffizienten aus dem Körper $\mathbb{F}_q$. Die Lösungen $(a,b) \in {\mathbb{F}_q}^2$ von (0.3) sind gerade die $\mathbb{F}_q$-*rationalen* Punkte der durch (0.3) gegebenen Kurve. Die Verallgemeinerung von $\mathbb{Z}/p$ zu dem endlichen Körper $\mathbb{F}_q$ hat den Vorteil, daß die Lösungen von (0.3) in allen Körpererweiterungen von $\mathbb{F}_q$ auf bestimmte Weise zusammenhängen.

Eine wichtige Anwendung algebraischer Kurven über endlichen Körpern stellt die Kodierungstheorie dar. Besonders interessant hierfür sind Kurven mit einer besonders großen Anzahl von rationalen Punkten. Die Länge eines Kodes über $\mathbb{F}_q$, der mit einer algebraischen Kurve C assoziiert ist, ist nämlich beschränkt durch die Anzahl der rationalen Punkte der Kurve C. Somit ist die Frage "Wie viele rationale Punkte kann eine Kurve besitzen?" besonders wichtig, weil man oft lange Kodes über $\mathbb{F}_q$ konstruieren möchte. Genaueres dazu siehe [Sti93, KapII und VII].

Der Begriff *algebraische Kurve* entstammt der Geometrie, wobei bei dem Begriff *algebraischer Funktionenkörper* eher der algebraische Aspekt im Vordergrund steht. Sei K ein endlicher Körper. Zwischen einer algebraischen Kurve über K und ihrem Funktionenkörper besteht folgender Zusammenhang: ein algebraischer Funktionenkörper F/K in einer Variablen wird erzeugt in der Form

$$F = K(x,y) \;\text{ mit }\; f(x,y) = 0\,, \tag{0.4}$$

wobei $f(x, y)$ ein Polynom mit Koeffizienten aus K ist. Umgekehrt führt jede Kurve, die durch ein Polynom $f(x, y)$ mit Koeffizienten aus K gegeben ist, vermöge (0.4) zu einem Funktionenkörper. Deshalb werden die Begriffe *algebraische Kurve* und *algebraischer Funktionenkörper* als gleichbedeutend angesehen.

Wie bekommt man nun Abschätzungen für die Anzahl N der $\mathbb{F}_q$-rationalen Punkte einer Kurve?

Die *Zeta-Funktion* einer algebraischen Kurve ist das wichtigste Werkzeug, um die Anzahl N der $\mathbb{F}_q$-rationalen Punkte einer Kurve zu studieren. Es handelt sich dabei um eine rationale Funktion über $\mathbb{Z}$, in der alle Informationen über die Anzahl von rationalen Punkten in Erweiterungskörpern von $\mathbb{F}_q$ enthalten sind.

H. Hasse interessierte das Verhalten von N einer Gleichung (0.3) für $q \longrightarrow \infty$, d. h. es werden alle endlichen Erweiterungskörper eines gewählten Grundkörpers durchlaufen. Er nahm an, daß

$$N = q + R \tag{0.5}$$

gilt. Das Fehlerglied R kann abgeschätzt werden durch

$$|R| \leq c \cdot \sqrt{q}\,,$$

wobei c eine Konstante ist, die nur vom Geschlecht der betrachteten Kurve abhängt. Das Geschlecht ist eine wichtige Invariante der Kurve, die ein Maß ihrer Komplexität darstellt. Hasse stellte fest, daß seine Annahme gleichbedeutend mit der sogenannten *Riemannschen Vermutung für die Zeta-Funktion von algebraischen Kurven* ist. Hasse bewies diese Vermutung für Kurven vom Geschlecht Eins. A. Weil konnte die Riemannsche Vermutung für algebraische Kurven schließlich für beliebiges Geschlecht beweisen. Deshalb wird sie auch als *Hasse-Weil-Theorem* bezeichnet:

Ist $w \in \mathbb{C}$ eine Nullstelle der Zeta-Funktion, dann gilt

$$|w| = \frac{1}{\sqrt{q}}\,. \tag{0.6}$$

An dieser Stelle sollte man anmerken, daß es ein heute immer noch ungelöstes Problem ist, die *Riemannsche Vermutung im Zahlkörperfall* zu beweisen.
Mit Hilfe des sehr wichtigen Hasse-Weil-Theorems kann man nun eine Abschätzung für die Anzahl N der $\mathbb{F}_q$-rationalen Punkte einer Kurve angeben, die *Hasse-Weil-Abschätzung*:

Die Zahl N der $\mathbb{F}_q$-rationalen Punkte einer Kurve C über dem Körper $\mathbb{F}_q$ kann abgeschätzt werden durch

$$|N - (q+1)| \leq 2g\sqrt{q}\,. \tag{0.7}$$

Diese Schranke ist sehr wichtig, aber noch nicht optimal. Ihre Obergrenze kann wesentlich verbessert werden, wenn das Geschlecht g groß in Bezug auf q ist.

Wie groß ist nun die maximale Anzahl der $\mathbb{F}_q$-rationalen Punkte, die Kurven von einem bestimmten Geschlecht haben können?

J.-P. Serre führte die Methode der *expliziten Formeln* ein. Dabei wird benutzt, daß die Anzahl aller $\mathbb{F}_{q^n}$-rationalen Punkte der Kurve durch die Nullstellen der Zeta-Funktion bestimmt sind. Daraus erhält man eine Abschätzung für N. Diese Abschätzung will man nun für eine beliebige Kurve durchführen. Dabei ist das

Hasse-Weil-Theorem wesentlich: da die Nullstellen der Zeta-Funktion alle den Betrag $\sqrt{q}$ haben, gehen diese mittels eines trigonometrischen Polynoms, welches gewisse Eigenschaften erfüllen muß, in die expliziten Formeln ein. Somit kann N abgeschätzt werden durch eine reellwertige Funktion (M_g), welche von der Wahl der Koeffizienten des trigonometrischen Polynoms, deren Anzahl und von dem gewählten Geschlecht g abhängt. Wählt man nun ein festes g und setzt eine zulässige Wahl von Koeffizienten in die Funktion M_g ein, so erhält man schon eine obere Schranke für die maximale Anzahl der $\mathbb{F}_q$-rationalen Punkte von Kurven dieses Geschlechts. Es stellt sich das Problem, eine optimale Wahl von Koeffizienten zu finden. In dieser Arbeit werden Methoden untersucht, wie man M_g für fest gewählte g's minimieren kann. Wir betrachten die Funktion zunächst mit Hilfe der Differentialrechnung im Spezialfall $q = 2$. Dabei wird unter anderem klar, daß für wachsendes Geschlecht eine wachsende Anzahl von Variablen notwendig wird. Mit dem Computeralgebrasystem Maple kann man M_g nur bis zu einer Anzahl von 9 Variablen minimieren. Werte für große g's erhält man mit dem Computerprogramm, welches wir in Kapitel 4 erarbeiten. Im Anhang sind obere Schranken für die maximale Anzahl der $\mathbb{F}_q$-rationalen Punkte von Kurven bis $g = 10000$ aufgeführt.

Kurze Zusammenfassung des Inhaltes:

- Im ersten Kapitel führen wir das Geschlecht eines Funktionenkörpers ein und legen die Bedeutung des Begriffes dar.
- Im zweiten Kapitel stellen wir den Zusammenhang zwischen Kurven und Funktionenkörpern dar, und untersuchen die Zeta-Funktion algebraischer Kurven.
- Im dritten Kapitel betrachten wir obere Schranken für N und gelangen schließlich zur Serre-Methode. Diese wenden wir auf ein spezielles trigonometrisches Polynom an, das wir in die erforderliche Form bringen. Als Ergebnis erhalten wir eine reellwertige Funktion, die unter anderem von den Koeffizienten des trigonometrischen Polynoms abhängt.
- Im vierten Kapitel untersuchen wir die Funktion M_g mit Hilfe der Differentialrechnung. Auf der Basis der daraus gewonnenen Erkenntnisse entwerfen wir ein Programm, welches das Minimum von M_g auch für sehr große g's berechnen kann.

Danksagung:

Ich danke Herrn Prof. Dr. E.-U. Gekeler für das schöne Thema und die viele Zeit, die er sich für meine Fragen genommen hat. Desweiteren danke ich Herrn Dipl.-Math. M. Gebhardt, der mich während meiner Zeit am Lehrstuhl betreut und beim Erstellen meiner Staatsexamensarbeit unterstützt hat. Viele seiner Anmerkungen und Kommentare sind in meine Arbeit eingeflossen. Weiter bedanke ich mich für die sehr hilfreichen Anregungen von Herrn Dipl.-Math. B. Wack, der das Voranschreiten meiner Arbeit mit Interesse verfolgt hat. Ich möchte auch Herrn Dipl.-Inf. O. Scheja danken, der mir bei der Strukturierung meiner Arbeit geholfen hat und sie in letzter Minute noch Korrektur gelesen hat. Nicht zuletzt hat die kollegiale Atmosphäre am Lehrstuhl zum Gelingen meiner Staatsexamensarbeit beigetragen.

Kapitel 1

Das Geschlecht eines algebraischen Funktionenkörpers

In diesem Kapitel wird das Geschlecht algebraischer Funktionenkörper definiert und seine Bedeutung dargelegt. Wir werden später sehen, daß es möglich ist, Definitionen und Ergebnisse von algebraischen Funktionenkörpern auf algebraische Kurven zu übertragen. Dieses Kapitel richtet sich im wesentlichen nach dem Buch [Sti93]. Die Beweise zu den einzelnen Aussagen können dort nachgelesen werden.

Im folgenden bezeichnet K einen beliebigen Körper, $K(x)$ bezeichnet den rationalen Funktionenkörper über K in x.

Definition 1.1 Ein *algebraischer Funktionenkörper F/K in einer Variablen über K* ist eine endliche algebraische Erweiterung von $K(x)$. Hierbei ist x ein Element aus F welches transzendent über K ist.

Zur Abkürzung bezeichnen wir im weiteren Text F/K einfach als *Funktionenkörper*. Das einfachste Beispiel eines algebraischen Funktionenkörpers ist der *rationale Funktionenkörper*. F/K wird *rational* genannt, wenn $F = K(x)$ ist für ein $x \in F$, welches transzendent über K ist. Bekanntlich läßt sich jedes Element aus $K(x)$ als Produkt von Potenzen paarweise verschiedener Primpolynome schreiben. Wie sehen nun die Analoga zu diesen Primpolynomen aus, wenn F/K ein nicht-rationaler Funktionenkörper ist?
Zur Beantwortung dieser Frage ist es notwendig, die Begriffe *Bewertungsring*, *Stelle* und *Bewertungsfunktion* kurz zu definieren.

1.1 Stellen und ihre Bewertungsringe

Definition 1.2 Ein *Bewertungsring* des Funktionenkörpers F/K ist ein Ring $\mathcal{O} \subseteq F$ mit den folgenden Eigenschaften:

(i) $K \subsetneq \mathcal{O} \subsetneq F$, und

(ii) für jedes $z \in F$ gilt $z \in \mathcal{O}$ oder $z^{-1} \in \mathcal{O}$.

Bemerkung: Der Ring $\mathcal{O}$ ist ein *lokaler Ring*, d. h. $\mathcal{O}$ hat ein einziges maximales Ideal $P = \mathcal{O} \setminus \mathcal{O}^*$, wobei $\mathcal{O}^* = \{z \in \mathcal{O} \mid \text{es gibt ein } w \in \mathcal{O} \text{ mit } zw = 1\}$ die *Einheitengruppe* von $\mathcal{O}$ ist.

Definition 1.3

(i) Eine *Stelle* P des Funktionenkörpers F/K ist das maximale Ideal eines Bewertungsringes $\mathcal{O}$ von F/K. Jedes Element $t \in P$ für das $P = t\mathcal{O}$ gilt, nennt man *Primelement* für P. Die Menge der Stellen des Funktionenkörpers F/K wird mit $\mathbb{P}_F$ bezeichnet.

(ii) Ist $\mathcal{O}$ ein Bewertungsring von F/K und P sein maximales Ideal, dann ist $\mathcal{O}$ eindeutig bestimmt durch P, es gilt nämlich $\mathcal{O} = \{z \in F \mid z^{-1} \notin P\}$. Folglich wird $\mathcal{O}_P := \mathcal{O}$ *der Bewertungsring der Stelle* P genannt.

Definition 1.4 Eine *diskrete Bewertung* von F/K ist eine Funktion $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:

(i) $v(x) = \infty \Longleftrightarrow x = 0$.

(ii) $v(xy) = v(x) + v(y)$ für $x, y \in F$.

(iii) $v(x + y) \geq min\{v(x), v(y)\}$ für $x, y \in F$.

(iv) Es existiert ein Element $z \in F$ mit $v(z) = 1$.

(v) $v(a) = 0$ für $0 \neq a \in K$.

Lemma 1.5 (Strenge Dreiecksungleichung). *Sei v eine diskrete Bewertung von F/K und $x, y \in F$ mit $v(x) \neq v(y)$. Dann gilt $v(x + y) = min\{v(x), v(y)\}$.*

Definition 1.6 Jeder Stelle $P \in \mathbb{P}_F$ ordnen wir eine Funktion $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ zu. Es sei t ein Primelement für P. Nun hat jedes $0 \neq z \in F$ eine eindeutige Darstellung $z = t^n u$ mit $u \in \mathcal{O}_P^*$ und $n \in \mathbb{Z}$. Wir definieren $v_P(z) := n$ und $v_P(0) := \infty$.

Satz 1.7 *Sei F/K ein Funktionenkörper. Für jede Stelle $P \in \mathbb{P}_F$ ist die oben definierte Funktion v_P eine diskrete Bewertung von F/K. Darüberhinaus gilt*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid v_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{z \in F \mid v_P(z) = 0\}, \\ P &= \{z \in F \mid v_P(z) > 0\}. \end{aligned}$$

Ein Element $t \in F$ ist genau dann ein Primelement für P, wenn $v_P(t) = 1$ ist.

Definition 1.8

(i) Sei P eine Stelle von F/K und $\mathcal{O}_P$ ihr Bewertungsring. Da P ein maximales Ideal ist, ist der Restklassenring $\mathcal{O}_P/P$ ein Körper. $F_P := \mathcal{O}_P/P$ ist der *Restklassenkörper* von P. Für $x \in \mathcal{O}_P$ sei $x(P) \in \mathcal{O}_P/P$ die *Restklasse* von x modulo P. Für $x \in F \setminus \mathcal{O}_P$ setzen wir $x(P) := \infty$. Die Abbildung $x \longmapsto x(P)$ von F nach $F_P \cup \{\infty\}$ nennt man die *Restklassenabbildung* bezüglich P.

(ii) $deg\, P := [F_P : K]$ wird der *Grad* von P genannt.

Definition 1.9 Es seien $z \in F$ und $P \in \mathbb{P}_F$. Wir bezeichnen P als *Nullstelle* von z genau dann, wenn $v_P(z) > 0$ ist. P ist eine *Polstelle* von z genau dann, wenn $v_P(z) < 0$ gilt. Ist $v_P(z) = m > 0$, so ist P eine *Nullstelle von z der Ordnung m*; ist $v_P(z) = -m < 0$, so ist P eine *Polstelle von z der Ordnung m*.

1.2 Divisoren

Die Menge $\tilde{K} := \{z \in F \mid z \text{ ist algebraisch über } K\}$ ist ein Unterkörper von F, weil Summen, Produkte und Inversen algebraischer Elemente auch algebraisch sind. $\tilde{K}$ wird *Konstantenkörper* von F/K genannt. Weiter gilt $K \subseteq \tilde{K} \subset F$. Es ist leicht nachzuweisen, daß $F/\tilde{K}$ ein Funktionenkörper über $\tilde{K}$ ist. Wir sagen K ist *algebraisch abgeschlossen in* F (oder K ist der *volle Konstantenkörper von* F), wenn $\tilde{K} = K$ ist.

Von nun an bezeichne F/K immer einen algebraischen Funktionenkörper in einer Variablen, wobei K der volle Konstantenkörper von F/K sei.

Definition 1.10 Die additive freie abelsche Gruppe, welche durch die Stellen von F/K erzeugt wird, bezeichnet man mit $\mathcal{D}_F$, die *Divisorgruppe* von F/K.
Die Elemente von $\mathcal{D}_F$ werden *Divisoren* von F/K genannt. Ein Divisor ist also eine formale Summe

$$D = \sum_{P \in \mathbb{P}_F} n_P P \qquad \text{mit } n_P \in \mathbb{Z}, \text{ fast alle } n_P = 0.$$

Ein Divisor der Form $D = P$ mit $P \in \mathbb{P}_F$ wird *Primdivisor* genannt.
Für $Q \in \mathbb{P}_F$ und $D = \sum n_P P \in \mathcal{D}_F$ definieren wir $v_Q(D) := n_Q$, deshalb ist

$$D = \sum_{P \in \mathbb{P}_F} v_P(D) \cdot P.$$

Eine partielle Ordnung auf $\mathcal{D}_F$ ist definiert durch

$$D_1 \le D_2 \;:\Longleftrightarrow\; v_P(D_1) \le v_P(D_2) \qquad \text{für alle } P \in \mathbb{P}_F.$$

Ein Divisor $D \ge 0$ heißt *positiv*. Der *Grad* eines Divisors ist definiert durch

$$deg\, D := \sum_{P \in \mathbb{P}_F} v_P(D) \cdot deg\, P$$

und liefert einen Homomorphismus $deg\, D : \mathcal{D}_F \longrightarrow \mathbb{Z}$.

Bemerkung: Jedes Element $0 \neq x \in F$ hat nur endlich viele Nullstellen und Pole in $\mathbb{P}_F$. Deshalb ist die nachfolgende Definition sinnvoll.

Definition 1.11 Sei $0 \neq x \in F$ und Z (bzw. N) bezeichne die Menge der Nullstellen (bzw. Polstellen) von x in $\mathbb{P}_F$. Dann definieren wir durch

$$\begin{aligned}
(x)_0 &:= \sum_{P \in Z} v_P(x) P && \text{den } \textit{Nulldivisor} \text{ von } x,\\
(x)_\infty &:= \sum_{P \in N} -(v_P(x)) P && \text{den } \textit{Poldivisor} \text{ von } x,\\
(x) &:= (x)_0 - (x)_\infty && \text{den } \textit{Hauptdivisor} \text{ von } x.
\end{aligned}$$

Es ist klar, daß $(x)_0 \ge 0$, $(x)_\infty \ge 0$ und

$$(x) = \sum_{P \in \mathbb{P}_F} v_P(x) P$$

ist. Für $0 \neq x \in F$ gilt

$$x \in K \Longleftrightarrow (x) = 0\,.$$

1.3 $\mathcal{L}$-Räume von Divisoren

Sei F/K ein algebraischer Funktionenkörper mit Konstantenkörper K. Zu jeder Stelle P von F/K sei ein Element x_P aus F/K und eine ganze Zahl n_P gegeben. Es sei v_P die Bewertungsfunktion der Stelle P. Gesucht sind nun Funktionen $x \in F$, welche allen Bedingungen

$$v_P(x - x_P) \geq n_P \tag{1.1}$$

genügen. *Das bedeutet, man sucht $x \in F$, die an den Stellen P mit gegebenen Funktionen x_P mit gewisser Genauigkeit, die durch die Stellenbewertung n_P gegeben ist, übereinstimmen.*

Zu lösen ist also ein Gleichungssystem. Wie in der linearen Algebra geht man folgendermaßen vor: man findet eine spezielle Lösung von (1.1), falls es eine gibt, und berechnet die Lösungen des zugehörigen homogenen Systems. Dieses ist gegeben durch

$$v_P(x) \geq n_P. \tag{1.2}$$

Die Elemente x, die das System (1.2) erfüllen, bilden offensichtlich einen Vektorraum über K. Für jedes x ist für fast alle Stellen P von F/K bis auf endlich viele $\mathrm{v}_P(x) = 0$. Daher können wir uns auf den Fall beschränken, daß alle Zahlen n_P bis auf endlich viele gleich Null sind.

Der Divisor $-A = \sum_P n_P \cdot P$ ordnet einer endlichen Anzahl von Stellen die ganzen Zahlen n_P zu. Wir definieren:

Definition 1.12 Für einen Divisor $A \in \mathcal{D}_F$ setzen wir

$$\mathcal{L}(A) := \{x \in F \mid (x) \geq -A\} \cup \{0\}.$$

In dieser Bezeichnungsweise ist $\mathcal{L}(-A)$ gerade der Lösungsraum des homogenen Systems (1.2). Ist das System (1.1) lösbar, so ist die Lösungsmenge gleich $\tilde{x}+\mathcal{L}(-A)$, wobei $\tilde{x}$ eine spezielle Lösung ist und $-A$ der oben beschriebene Divisor.

Im Verlauf dieses Kapitels wird sich herausstellen, daß man mit Hilfe einer Invarianten des Funktionenkörpers F/K, dem *Geschlecht*, Aussagen über die Dimension von $\mathcal{L}(-A)$ machen kann. Genaueres zur Problemstellung (1.1) kann man in [Che51] nachlesen.

Interpretation: Für

$$-A = \sum_{j=1}^{s} m_j Q_j - \sum_{i=1}^{r} n_i P_i \qquad \text{mit } n_i > 0,\ m_j > 0,$$

besteht $\mathcal{L}(A)$ aus allen Elementen $x \in F$ solcherart, daß

(i) x Nullstellen Q_j der Ordnung größer gleich m_j hat für $j = 1, \ldots, s$, und

(ii) x nur an den Stellen $P_1, \ldots, P_r$ Pole haben kann mit Polordnung höchstens n_i $(i = 1, \ldots, r)$.

Bemerkung: Sei $A \in \mathcal{D}_F$. Ein x aus F liegt genau dann in $\mathcal{L}(A)$, wenn $v_P(x) \geq -v_P(A)$ für alle $P \in \mathbb{P}_F$ gilt. $\mathcal{L}(A)$ ist ein Vektorraum über K.

Definition 1.13 Für $A \in \mathcal{D}_F$ heißt die Zahl $dim\, A := dim\, \mathcal{L}(A)$ die *Dimension* des Divisors A.

Satz 1.14 *Jeder Hauptdivisor hat den Grad Null. Genauer: Sei $x \in F$. Dann gilt*

$$deg\,(x)_0 = deg\,(x)_\infty = [F : K(x)]\,.$$

Korollar 1.15 *Seien A, A' Divisoren aus $\mathcal{D}_F$.*

(i) Gilt $A \leq A'$, so ist $\mathcal{L}(A)$ Untervektorraum von $\mathcal{L}(A')$ und

$$dim\,(\mathcal{L}(A')/\mathcal{L}(A)) \leq deg\,A' - deg\,A\,.$$

(ii) $\mathcal{L}(0) = K$; $\mathcal{L}(A)$ ist gleich dem Nullraum, falls $deg\,A < 0$.

(iii) $\mathcal{L}(A)$ ist endlichdimensional für alle $A \in \mathcal{D}_F$. Ist $deg\,A \geq 0$, dann ist

$$dim\,A \leq deg\,A + 1\,.$$

Eine untere Abschätzung für $dim\,A$ liefert die folgende Proposition.

Proposition 1.16 *Es gibt eine Konstante $\gamma \in \mathbb{Z}$ solcherart, daß für alle Divisoren $A \in \mathcal{D}_F$ das folgende gilt:*

$$deg\,A - dim\,A \leq \gamma\,.$$

Das Entscheidende hierbei ist: $\gamma \in \mathbb{Z}$ ist nicht abhängig von dem gewählten Divisor A, sondern nur von dem betrachteten Funktionenkörper F/K.
Aufgrund der obigen Proposition können wir nun das *Geschlecht von F/K* definieren, dies ist die wichtigste Invariante eines Funktionenkörpers.

Definition 1.17 Das *Geschlecht* g von F/K ist definiert durch

$$g := max\{deg\,A - dim\,A + 1 \mid A \in \mathcal{D}_F\}.$$

Bemerkung: Das Geschlecht von F/K ist eine nicht-negative ganze Zahl.

Satz 1.18 (Riemann). *Sei F/K ein Funktionenkörper vom Geschlecht g.*

(i) Für jeden Divisor $A \in \mathcal{D}_F$ gilt

$$dim\,A \geq deg\,A + 1 - g\,.$$

(ii) Es gibt eine ganze Zahl c, welche von F/K abhängt, so daß

$$dim\,A = deg\,A + 1 - g$$

gilt, wenn $deg\,A \geq c$ ist.

Der nächste Satz gibt genau an, wie man die Konstante c wählen kann. Dieser Satz ist eine Folgerung aus dem Satz von *Riemann-Roch*, dem bei weitem wichtigsten Satz in der Theorie algebraischer Funktionenkörper.

Satz 1.19 *Ist A ein Divisor von F/K vom Grad größer gleich $2g - 1$, dann gilt*

$$dim\,A = deg\,A + 1 - g\,.$$

Kennt man also das Geschlecht eines Funktionenkörpers F/K, so kann man zu jedem Divisor A von F/K, für den $deg\, A \geq 2g-1$ gilt, die Dimension seines $\mathcal{L}$-Raumes bestimmen.

Die Spezialfälle $\mathbf{g = 1}$ und $\mathbf{g = 0}$.
Wir betrachten nun Funktionenkörper vom Geschlecht Null und Funktionenkörper vom Geschlecht Eins. Wie verhält sich in diesen Fällen die Dimension des $\mathcal{L}$-Raumes eines Divisors in Abhängigkeit von seinem Grad?
Nach Teil *(ii)* von Korollar (1.15) haben die $\mathcal{L}$-Räume von Divisoren negativen Grades, bei beliebigem Geschlecht des Funktionenkörpers F/K, die Dimension Null.

(i) Sei F/K ein Funktionenkörper vom Geschlecht $g = 1$ (elliptischer Funktionenkörper).

   (a) Sei ein Divisor $A \in \mathcal{D}_F$ mit $deg\, A = 0$ gegeben.
   Nach Teil *(i)* des Satzes von Riemann (1.18) ist dann $dim\, A \geq 0$. Außerdem ergibt sich aus (1.15)*(iii)*, daß $dim\, A \leq 1$ ist.

   (b) Ein Divisor $A \in \mathcal{D}_F$ habe die Eigenschaft $deg\, A > 0$.
   Gemäß (1.19) folgt für Divisoren vom Grad größer gleich 1, daß
   $$dim\, A = deg\, A$$
   ist.

(ii) Sei F/K ein Funktionenkörper vom Geschlecht $g = 0$ (z. B. der rationale Funktionenkörper $K(x)$).
Ist ein Divisor $A \in \mathcal{D}_F$ mit $deg\, A \geq 0$ gegeben, so ist nach (1.18) $dim\, A \geq deg\, A + 1$. Zusätzlich ist $dim\, A \leq deg\, A + 1$ wegen (1.15)*(iii)*. Also haben wir insgesamt
$$dim\, A = deg\, A + 1.$$

Ist ein elliptische Funktionenkörper gegeben, so muß man für einen Divisor vom Grad Null nur entscheiden, ob die Dimension des Raumes Null oder Eins ist. Für einen Divisor A mit $deg\, A > 0$ kann man direkt die Dimension des zugehörigen Vektorraumes aus dem Grad berechnen. Dies werden wir im nachfolgenden Beispiel bei der Bestimmung der Basis von $\mathcal{L}$-Räumen positiver Divisoren eines elliptischen Funktionenkörpers benutzen. Liegt ein Funktionenkörper vom Geschlecht Null vor, so kann man die Dimension aller Divisoren mit Hilfe des Grades berechnen.

Wir betrachten zunächst algebraische Erweiterungen des rationalen Funktionenkörpers $K(x)$. Wie verhalten sich die Stellen von $K(x)$ zu den Stellen aus der algebraischen Erweiterung?

Definition 1.20 Betrachte eine algebraische Erweiterung F'/K' von F/K. Wir sagen, eine Stelle $P' \in \mathbb{P}_F{}'$ *liegt über* $P \in \mathbb{P}_F$, wenn $P \subseteq P'$ gilt. Wir bezeichnen P' als *Erweiterung* von P und schreiben $P' \mid P$.

Proposition 1.21 *Sei F'/K' eine algebraische Erweiterung von F/K. Sei P (bzw. P') eine Stelle von F/K (bzw. F'/K'), und bezeichne $\mathcal{O}_P \subseteq F$ (bzw. $\mathcal{O}_{P'} \subseteq F'$) den entsprechenden Bewertungsring, v_P (bzw. $v_{P'}$) die entsprechende diskrete Bewertung. Dann sind die folgenden Aussagen äquivalent:*

(i) $P' \mid P$.

(ii) $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$.

(iii) Es gibt eine ganze Zahl $e \geq 1$, so daß $v_{P'}(x) = e \cdot v_P(x)$ für alle $x \in F$.

Die Zahl $e =: e(P' \mid P)$ wird Verzweigungsindex von P' über P genannt. Liegt P' über P, so gilt $P = P' \cap F$ und $\mathcal{O}_P = \mathcal{O}_{P'} \cap F$. Aus diesem Grund nennt man P die Restriktion von P' auf F.

Kennt man den Verzweigungsindex der Stellen einer algebraischen Erweiterung des rationalen Funktionenkörpers, so kann man Berechnungen von diskreten Bewertungen auf den Fall $K(x)$ zurückführen.

Bevor wir mit dem Beispiel beginnen, beweisen wir noch ein Lemma, mit dem wir die lineare Unabhängigkeit von Funktionen aus F mit Hilfe (1.5) nachweisen können:

Lemma 1.22 *Es seien Funktionen $f_1, \ldots, f_n$ aus F gegeben. Es sei P eine beliebige Stelle des Funktionenkörpers. Falls die Bewertungen $v_P(f_1), \ldots, v_P(f_n)$ paarweise verschieden sind, so sind die Funktionen $f_1, \ldots, f_n$ linear unabhängig.*

Beweis: Seien $f_1, \ldots, f_n$ linear abhängig, das heißt es gelte $a_1 \cdot f_1 + \cdots + a_n \cdot f_n = 0$ für $a_1, \ldots, a_n \in K$, wobei nicht alle $a_1, \ldots, a_n$ gleich Null sind. Es seien nun ohne Beschränkung der Allgemeinheit alle $a_1, \ldots, a_n$ ungleich Null. Nach Definition (1.4) ist $v_P(0) = \infty$ und $v_P(a) = 0$ für $0 \neq a \in K$. Da die $v_P(f_1), \ldots, v_P(f_n)$ nach Voraussetzung paarweise verschieden sind, können wir die strenge Dreiecksungleichung für Bewertungen (1.5) benutzen, und erhalten

$$\begin{aligned} \infty = v_P(0) &= v_P(a_1 \cdot f_1 + \cdots + a_n \cdot f_n) \\ &= min\{v_P(a_1) + v_P(f_1), \ldots, v_P(a_n) + v_P(f_n)\} \\ &= min\{v_P(f_1), \ldots, v_P(f_n)\}\,. \end{aligned}$$

Der Wert $min\{v_P(f_1), \ldots, v_P(f_n)\}$ ist endlich. Also sind $f_1, \ldots, f_n$ linear unabhängig. □

Wir wollen nun konkret die $\mathcal{L}$-Räume von ausgewählten Divisoren eines speziellen Funktionenkörpers vom Geschlecht 1 bestimmen.

Beispiel: *K sei ein endlicher Körper mit $char\,K \neq 2$. Betrachte den Funktionenkörper $F = K(x, y)$, eine einfache algebraische Erweiterung von $K(x)$, die gegeben ist durch*

$$y^2 = (x-\alpha)(x-\beta)(x-\gamma) = f(x) \in K[x],$$

wobei $\alpha, \beta, \gamma \in K$ alle verschieden sind.
Es bezeichne $P_i \in \mathbb{P}_{K(x)}$ die Stelle von $K(x)$, die zu dem Polynom $(x - i)$ gehört, $(i = \alpha, \beta, \gamma)$, und $P_\infty \in \mathbb{P}_{K(x)}$ bezeichne den Pol von x. Nach [Sti93, KapVI, S.189] *gilt:*

(i) K ist der volle Konstantenkörper von F, und F/K ist ein elliptischer Funktionenkörper.

(ii) Die Erweiterung $F/K(x)$ ist zyklisch vom Grad 2. Die Stellen $P_\alpha, P_\beta, P_\gamma$ sind verzweigt in $F/K(x)$. Jede der Stellen hat genau eine Erweiterung in F, diese seien durch $Q_\alpha, Q_\beta, Q_\gamma$ und Q_∞ bezeichnet. Es gilt $e(Q_i \mid P_i) = e(Q_\infty \mid P_\infty) = 2$, $deg\,Q_i = deg\,P_i = 1$ und $deg\,Q_\infty = 1$, $(i = \alpha, \beta, \gamma)$.

Bestimmen wir nun die $\mathcal{L}$-Räume einiger Divisoren aus $\mathcal{D}_F$:

(i) $D = Q_\infty$.
Dann gilt für den $\mathcal{L}$-Raum von D nach Definition (1.12):

$$\mathcal{L}(D) = \{f \in F \mid v_{Q_\infty}(f) \geq -1 \; und \; v_Q(f) \geq 0 \; f\ddot{u}r \; Q \in \mathbb{P}_F, Q \neq Q_\infty\} \cup \{0\}.$$

In dem Vektorraum $\mathcal{L}(D)$ liegen also alle diejenigen Funktionen aus F, die höchstens einen Pol an Q_∞ haben, der höchstens von der Ordnung 1 ist. Die Funktionen dürfen an allen anderen Stellen keine Pole haben. Diese Bedingung erfüllen auf jeden Fall die konstanten Funktionen, die überhaupt keine Polstellen haben:

$$v_{P_\infty}(a) = v_{Q_\infty}(a) = 0, \qquad \textit{für } \; 0 \neq a \in K.$$

Hierbei ist v_{P_∞} die Gradbewertung von $K(x)$. Wir haben oben gesehen, daß für elliptische Funktionenkörper die Dimension von $\mathcal{L}(D)$, falls $\deg D > 0$, gleich dem Grad des Divisors D ist. Also ist $\dim D = 1$. In $\mathcal{L}(D)$ liegen also keine Funktionen außer den konstanten Funktionen. In diesem Fall ist $\mathcal{L}(D) = K$.

(ii) $D = 2Q_\infty$.
Der zugehörige $\mathcal{L}$-Raum hat folgende Gestalt:

$$\mathcal{L}(D) = \{f \in F \mid v_{Q_\infty}(f) \geq -2 \textit{ und } v_Q(f) \geq 0 \textit{ für } Q \in \mathbb{P}_F, Q \neq Q_\infty\} \cup \{0\}.$$

Gesucht sind alle Funktionen, die höchstens an der Stelle Q_∞ einen Pol haben, dessen Ordnung nicht größer als 2 ist. Das sind zunächst wieder die konstanten Funktionen. Der Grad des Divisors D ist gleich 2, somit ist $\dim D = 2$. Es muß also noch weitere Funktionen geben.
Da der Verzweigungsindex von Q_∞ über P_∞ gleich 2 ist, gilt für $f \in F$:

$$v_{Q_\infty}(f) = 2 \cdot v_{P_\infty}(f).$$

Um eine Auswahl treffen zu können, berechnen wir die Bewertungen bezüglich der Stelle Q_∞ einiger Funktionen (Rechenregeln für Bewertungen siehe (1.4)):

$$\begin{aligned}
v_{Q_\infty}(x) &= 2 \cdot v_{P_\infty}(x) = -2,\\
v_{Q_\infty}(x^2) &= 2 \cdot v_{Q_\infty}(x) = -4,\\
v_{Q_\infty}(x^3) &= 3 \cdot v_{Q_\infty}(x) = -6,\\
v_{Q_\infty}(y^2) &= v_{Q_\infty}(x^3) = -6,\\
v_{Q_\infty}(y) &= v_{Q_\infty}(y^2)/2 = -3,\\
v_{Q_\infty}(xy) &= v_{Q_\infty}(x) + v_{Q_\infty}(y) = -5,\\
v_{Q_\infty}(x^2y) &= v_{Q_\infty}(x^2) + v_{Q_\infty}(y) = -7.
\end{aligned}$$

Es ist $v_{Q_\infty}(x) = -2$. Weiter ist $v_Q(x) \geq 0$ für alle $Q \in \mathbb{P}_F$ mit $Q \neq Q_\infty$. Somit hätten wir zwei Elemente des Vektorraumes $\mathcal{L}(D)$, nämlich $\{1, x\}$. Da $v_{Q_\infty}(1) \neq v_{Q_\infty}(x)$ ist, besteht der $\mathcal{L}$-Raum des Divisors $D = 2Q_\infty$ aus allen Polynomen $f(x) \in K[x]$, die als Linearkombinationen aus 1 und x dargestellt werden können. Eine Basis von $\mathcal{L}(D)$ ist also $\{1, x\}$.

(iii) $D = 3Q_\infty$.

$$\mathcal{L}(D) = \{f \in F \mid v_{Q_\infty}(f) \geq -3 \textit{ und } v_Q(f) \geq 0 \textit{ für } Q \in \mathbb{P}_F, Q \neq Q_\infty\} \cup \{0\}.$$

Die Dimension des $\mathcal{L}$-Raumes beträgt 3. Es ist $v_{Q_\infty}(y) = -3$. Somit ist $v_{Q_\infty}(1) \neq v_{Q_\infty}(x) \neq v_{Q_\infty}(y)$. Also bildet $\{1, x, y\}$ eine Basis des Vektorraumes.

(iv) $D = 2Q_\alpha$.
Der Divisor D hat den Grad 2, was der Dimension des Raumes

$$\mathcal{L}(D) = \{f \in F \mid v_{Q_\alpha}(f) \geq -2 \textit{ und } v_Q(f) \geq 0 \textit{ für } Q \in \mathbb{P}_F, Q \neq Q_\alpha\} \cup \{0\}$$

entspricht. Die Funktion $\frac{1}{x-\alpha}$ *hat nur einen Pol an der Stelle* Q_α*. Es ist* $v_{Q_\alpha}(\frac{1}{x-\alpha}) = 2 \cdot v_{P_\alpha}(\frac{1}{x-\alpha}) = -2$*, also liegt* $\frac{1}{x-\alpha}$ *in dem Raum* $\mathcal{L}(D)$*. Auch die konstanten Funktionen sind in* $\mathcal{L}(D)$ *enthalten. Da* $v_{Q_\alpha}(\frac{1}{x-\alpha}) \neq v_{Q_\alpha}(1)$ *ist, haben wir eine Basis* $\{1, \frac{1}{x-\alpha}\}$.

(v) $D = Q_\infty + Q_\alpha$.
Der Raum des Divisors D läßt sich folgendermaßen beschreiben:

$$\mathcal{L}(D) = \left\{ f \in F \,\middle|\, \begin{array}{c} v_{Q_\infty}(f) \geq -1,\ v_{Q_\alpha}(f) \geq -1 \text{ und } v_Q(f) \geq 0 \\ \text{für } Q \in \mathbb{P}_F \text{ mit } Q \neq Q_\alpha, Q_\infty \end{array} \right\} \cup \{0\}.$$

Wir betrachten die Funktion $\frac{y}{x-\alpha}$*. Ihre Bewertung an der Stelle Unendlich ist gegeben durch:* $v_{Q_\infty}(\frac{y}{x-\alpha}) = v_{Q_\infty}(y) + v_{Q_\infty}(\frac{1}{x-\alpha}) = -3 + 2 = -1$*. An der Stelle* Q_α *ergibt sich für die Funktion y:*

$$\begin{aligned} 2 \cdot v_{Q_\alpha}(y) = v_{Q_\alpha}(y^2) &= v_{Q_\alpha}((x-\alpha)(x-\beta)(x-\gamma)) \\ &= v_{Q_\alpha}(x-\alpha) + v_{Q_\alpha}(x-\beta) + v_{Q_\alpha}(x-\gamma) \\ &= v_{Q_\alpha}(x-\alpha) \\ &= 2 \cdot v_{P_\alpha}(x-\alpha) \\ &= 2\,. \end{aligned}$$

Also hat y an Q_α *die Bewertung 1. Da* $y^2 = (x-\alpha)(x-\beta)(x-\gamma)$ *ist, hat y nur einen Pol bei Unendlich und sonst keine Polstellen. Nun ist* $v_{Q_\alpha}(\frac{y}{x-\alpha}) = v_{Q_\alpha}(y) + v_{Q_\alpha}(\frac{1}{x-\alpha}) = 1 + (-2) = -1$*. Für* $\frac{1}{x-\alpha}$ *liegt nur an der Stelle* Q_α *ein Pol vor. Die Dimension des* $\mathcal{L}$*-Raumes von D beträgt 2, und es ist* $v_{Q_\infty}(\frac{y}{x-\alpha}) \neq v_{Q_\infty}(1)$*, also ist eine Basis für* $\mathcal{L}(D)$ *gegeben durch* $\{1, \frac{y}{x-\alpha}\}$.

Kapitel 2

Die Zeta-Funktion einer algebraischen Kurve

Im ersten Abschnitt dieses Kapitels gehen wir kurz auf die Beziehungen zwischen algebraischen Kurven und algebraischen Funktionenkörpern ein. Die Beweise zu den Aussagen findet man in [Ful69].

Es sei K ein perfekter Körper, $\bar{K} \supseteq K$ bezeichne den algebraischen Abschluß von K.

2.1 Zusammenhang algebraische Kurve - algebraischer Funktionenkörper

Der n-dimensionale *affine Raum* $\mathbf{A}^n = \mathbf{A}^n(\bar{K})$ ist die Menge aller n-Tupel von Elementen aus $\bar{K}$. Ein Element $P = (a_1, \ldots, a_n) \in \mathbf{A}^n$ ist ein *Punkt* mit den *Koordinaten* $a_1, \ldots, a_n$.

Auf der Menge $\mathbf{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ ist eine Äquivalenzrelation $\sim$ gegeben durch

$$(a_0, a_1, \ldots, a_n) \sim (b_0, b_1, \ldots, b_n) \iff \begin{array}{l}\text{es gibt ein Element } 0 \neq \lambda \in \bar{K} \text{ solcherart,}\\ \text{daß } b_i = \lambda a_i \text{ für } 0 \leq i \leq n \text{ gilt.}\end{array}$$

Die Äquivalenzklasse von $(a_0, a_1, \ldots, a_n)$ bezüglich der Relation $\sim$ wird mit $(a_0 : a_1 : \ldots : a_n)$ bezeichnet. Der n-dimensionale projektive Raum $\mathbf{P}^n = \mathbf{P}^n(\bar{K})$ ist die Menge aller Äquivalenzklassen

$$\mathbf{P}^n = \left\{(a_0 : a_1 : \ldots : a_n) \mid a_i \in \bar{K}, \text{ nicht alle } a_i = 0\right\}.$$

Ein Element $P = (a_0 : a_1 : \ldots : a_n) \in \mathbf{P}^n$ nennt man *Punkt*, und die $a_0, a_1, \ldots, a_n$ nennt man *homogene Koordinaten* von P.

Ein Polynom F ist ein *homogenes Polynom*, falls F die Summe von Monomen vom gleichen Grad ist. Ein Punkt $P = (a_0 : \ldots : a_n) \in \mathbf{P}^n$ heißt *Nullstelle* eines homogenen Polynoms $F \in \bar{K}[X_0, \ldots, X_n]$, wenn $F(a_0, \ldots, a_n) = 0$ ist für jede Wahl von homogenen Koordinaten für P. Dies ist sinnvoll, da $F(\lambda a_0, \ldots, \lambda a_n) = \lambda^d \cdot F(a_0, \ldots, a_n)$ mit $d = deg\, F$ ist. Wir schreiben dann $F(P) = 0$.

Eine Teilmenge $V \subseteq \mathbf{P}^n$ ist eine *projektive algebraische Menge*, wenn es eine Menge von homogenen Polynomen $M \subseteq \bar{K}[X_0, \ldots, X_n]$ gibt, so daß gilt:

$$V = \{P \in \mathbf{P}^n \mid F(P) = 0 \text{ für alle } F \in M\}.$$

Ein Ideal $I \subseteq \bar{K}[X_0, \ldots, X_n]$, welches durch homogene Polynome erzeugt wird, nennt man ein *homogenes Ideal.* Das Ideal $I(V) \subseteq \bar{K}[X_0, \ldots, X_n]$, welches von allen homogenen Polynomen F erzeugt wird, für die alle $P \in V$ Nullstellen sind, nennt man das *Ideal* von V. Dieses Ideal ist homogen.

Eine projektive algebraische Menge nennt man *irreduzibel*, wenn sie keine Vereinigung von zwei kleineren algebraischen Mengen ist. Es gilt: eine projektive algebraische Menge V ist genau dann irreduzibel, wenn $I(V)$ ein homogenes Primideal in $\bar{K}[X_0, \ldots, X_n]$ ist.

Eine *projektive Varietät* V ist eine irreduzible projektive algebraische Menge. Jede projektive algebraische Menge kann eindeutig als eine disjunkte Vereinigung von projektiven Varietäten, ihren irreduziblen *Komponenten*, dargestellt werden.

Gegeben sei eine nichtleere Varietät $V \subseteq \mathbf{P}^n$, wir definieren ihren *homogenen Koordinatenring* durch

$$\Gamma_h(V) = \bar{K}[X_0, \ldots, X_n]/I(V).$$

Dies ist ein Integritätsring, welcher $\bar{K}$ enthält. Ein Element $g \in \Gamma_h(V)$ heißt eine *Form* vom Grad d, wenn $g = G + I(V)$ für ein homogenes Polynom $G \in \bar{K}[X_0, \ldots, X_n]$ mit $deg\ G = d$ gilt.

Sei $P = (a_0 : \ldots : a_n) \in V$. Wähle ein Element f aus dem Quotientenkörper $Quot(\Gamma_h(V))$ von $\Gamma_h(V)$, mit der Eigenschaft $f = g/h$, wobei $g = G + I(V)$ und $h = H + I(V)$ Formen vom Grad d in $\Gamma_h(V)$ sind. Dann definiert g/h eine Funktion, falls $H(P) \neq 0$ ist:

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, \ldots, a_n)}{\lambda^d \cdot H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)}.$$

Somit ist $f(P)$ unabhängig von der Wahl der homogenen Koordinaten für P und wir können schreiben $f(P) = G(a_0, \ldots, a_n)/H(a_0, \ldots, a_n) \in \bar{K}$. Dann ist f *definiert* in P und $f(P)$ ist der *Wert* von f in P.

Der *Funktionenkörper* von V ist definiert durch:

$$\bar{K}(V) = \left\{ \frac{g}{h} \,\middle|\, g, h \in \Gamma_h(V) \text{ sind Formen von gleichem Grad, und } h \neq 0 \right\}.$$

Der Funktionenkörper von V ist ein Unterkörper des Quotientenkörpers von $\Gamma_h(V)$. Die Elemente von $\bar{K}(V)$ nennt man *rationale Funktionen* auf V. Die *Dimension* von V ist der Transzendenzgrad von $\bar{K}(V)$ über $\bar{K}$.

Der Ring

$$\mathcal{O}_P(V) = \left\{ f \in \bar{K}(V) \mid f \text{ ist definiert bei } P \right\} \subseteq \bar{K}(V)$$

ist ein lokaler Ring mit maximalem Ideal

$$M_P(V) = \{f \in \mathcal{O}_P(V) \mid f(P) = 0\}.$$

Eine **projektive algebraische Kurve** C ist eine projektive Varietät der Dimension Eins. Dies bedeutet, daß der Funktionenkörper $\bar{K}(C)$ der rationalen Funktionen auf C ein algebraischer Funktionenkörper in einer Variablen ist.

Ein Punkt P der Kurve C ist *nicht-singulär*, wenn der lokale Ring $\mathcal{O}_P(C)$ ein diskreter Bewertungsring ist. Die Kurve C nennt man *nicht-singulär*, wenn alle Punkte $P \in C$ nicht-singulär sind.

Eine projektive algebraische Kurve $C \subseteq \mathbf{P}^n(\bar{K})$ ist *definiert über* K, falls das Ideal $I(C)$ von homogenen Polynomen $F_1, \ldots, F_r \in K[X_0, \ldots, X_n]$ erzeugt wird. Einen Punkt $P \in C$ nennt man *K-rational*, wenn es homogene Koordinaten $a_0, \ldots, a_n$ von P gibt, welche alle in K liegen. Wir schreiben

$$C(K) = \{P \in C \mid P \text{ ist } K\text{-rational}\}.$$

In dieser Schreibweise bezeichnet $C(\bar{K}) = C$ alle Punkte der Kurve.

Sei $C \subseteq \mathbf{P}^n(\bar{K})$ eine projektive algebraische Kurve definiert über K. Wir definieren das Ideal

$$I(C/K) = I(C) \cap K[X_0, \ldots, X_n]$$

und den Restklassenring

$$\Gamma_h(C/K) = K[X_0, \ldots, X_n]/I(C/K).$$

In entsprechender Weise werden dann auch der lokale Ring $\mathcal{O}_P(C/K)$ und sein maximales Ideal $M_P(C/K)$ definiert. Der Körper

$$K(C) = \left\{ \frac{g}{h} \,\middle|\, g, h \in \Gamma_h(C/K) \text{ sind Formen von gleichem Grad, und } h \neq 0 \right\}$$

ist der Körper der *K-rationalen Funktionen* auf C. Der Transzendenzgrad der Körpererweiterung $K(C)/K$ beträgt Eins.

Es gibt noch eine andere Art, die K-rationalen Punkte der Kurve C, die über dem Körper K definiert ist, zu beschreiben: Sei $Gal(\bar{K}/K)$ die Galois-Gruppe von $\bar{K}/K$. Wir betrachten einen Punkt $P = (a_0 : \ldots : a_n) \in C$ und einen Automorphismus $\sigma \in Gal(\bar{K}/K)$, dann ist $\sigma(P) = (\sigma(a_0) : \ldots : \sigma(a_n))$. Man kann leicht zeigen, daß

$$C(K) = \{P \in C \mid \sigma(P) = P \text{ für alle } \sigma \in Gal(\bar{K}/K)\}$$

ist. Läßt man die Galois-Gruppe $Gal(\bar{K}/K)$ auf allen Punkten der Kurve C, also auf $C(\bar{K})$, operieren, so erhält man eine Zerlegung der Menge $C(\bar{K})$ in disjunkte Bahnen. Diese Bahnen nennen wir *Primdivisoren.* Jedem beliebigen Punkt $P \in C$ ordnen wir seine Bahn unter der Galois-Gruppe $Gal(\bar{K}/K)$ zu. Wir bezeichnen den Primdivisor des Punktes P mit $[P]$. Der *Grad* eines Primdivisors $[P]$ ist die Länge seiner Bahn. Die K-rationalen Punkte der Kurve C sind also gerade die Primdivisoren vom Grad Eins.

Nicht-singuläre Kurven und algebraische Funktionenkörper. Geht man von einem algebraischen Funktionenkörper in einer Variablen F/K aus, so gibt es eine nicht-singuläre projektive Kurve C definiert über K, deren Funktionenkörper $K(C)$ *K-isomorph* zu F ist.
Sei umgekehrt C eine nicht-singuläre projektive Kurve definiert über K und $K(C)$

ihr Funktionenkörper. Es gibt eine Bijektion zwischen den Primdivisoren $[P]$ der Kurve C und den Stellen von $K(C)/K$, gegeben durch

$$[P] \longmapsto M_P(C/K),$$

wobei $M_P(C/K)$ das maximale Ideal des lokalen Ringes $\mathcal{O}_P(C/K)$ ist. Die Abbildung ist wohldefiniert: Liegen zwei Punkte $P, P' \in C$ in der gleichen Bahn, d.h. ist $[P] = [P']$, so stimmen auch die maximalen Ideale der von P und P' erzeugten Bewertungsringe überein. Der Grad eines Primdivisors $[P]$ (die Anzahl der Punkte auf der Bahn) ist gleich dem Grad der entsprechenden Stelle (der Grad der Körpererweiterung $\mathcal{O}_P(C/K)/M_P(C/K)$ über K).
Diese Übereinstimmung macht es möglich, Definitionen und Ergebnisse von algebraischen Funktionenkörpern auf algebraische Kurven (und umgekehrt) zu übertragen:

Sei C eine nicht-singuläre projektive Kurve definiert über K. Dann gilt:

(i) Das *Geschlecht* der Kurve C ist das Geschlecht des Funktionenkörpers $K(C)$.

(ii) Ein Divisor D von C ist eine formale Summe

$$D = \sum_{[P] \in C/Gal(\bar{K}/K)} n_P \cdot [P],$$

wobei fast alle $n_P \in \mathbb{Z}$ gleich Null sind. Der *Grad* von D ist gegeben durch

$$deg\ D = \sum_{[P] \in C/Gal(\bar{K}/K)} n_P \cdot deg\ [P]\,.$$

Die Divisoren von C bilden eine additive abelsche Gruppe $\mathcal{D}(C)$, die Divisorgruppe von C.

(iii) Die *Ordnung einer rationalen Funktion* $f \in K(C)$ an einem Punkt $P \in C$ ist per Definition gleich $v_P(f)$, wobei v_P die diskrete Bewertung von $K(C)$ bezüglich des Bewertungsringes $\mathcal{O}_P(C/K)$ ist.

(iv) Der *Hauptdivisor* (f) einer rationalen Funktion $0 \neq f \in K(C)$ ist

$$(f) = \sum_{[P] \in C/Gal(\bar{K}/K)} v_P(f) \cdot [P]\,.$$

Der Grad eines Hauptdivisors ist Null.

2.2 Die Zeta-Funktion

In diesem Abschnitt sei C eine nicht-singuläre projektive algebraische Kurve, definiert über dem endlichen Körper $\mathbb{F}_q$.

Definition 2.1 Es bezeichne $C(\mathbb{F}_{q^n})$, $n \geq 1$, die Menge von Punkten aus C mit Koordinaten in $\mathbb{F}_{q^n}$. Diese Punkte nennt man $\mathbb{F}_{q^n}$*-rationale* Punkte der Kurve C.

Unser Ziel ist es, die Anzahl der $\mathbb{F}_q$-rationalen Punkte einer Kurve C abzuschätzen. Dazu definieren wir eine äußerst wichtige Funktion: die *Zeta-Funktion*. Die Zeta-Funktion einer Kurve C, die definiert ist durch eine oder mehrere polynomiale Gleichungen über dem endlichen Körper $\mathbb{F}_q$, ist eine formale Potenzreihe, in der alle Informationen über die Anzahl von rationalen Punkten in Erweiterungskörpern von $\mathbb{F}_q$ enthalten sind.

Im nachfolgenden Abschnitt betrachten wir die Funktionen log und exp als formale Potenzreihen. Alle Eigenschaften, die wir benutzen, können in [Lor96, KapVIII, S.277f] nachgeschlagen werden.

Definition 2.2 Sei C eine nicht-singuläre projektive Kurve, definiert über dem endlichen Körper $\mathbb{F}_q$. Sei $N_n := \mid C(\mathbb{F}_{q^n}) \mid$ die Anzahl der $\mathbb{F}_{q^n}$-rationalen Punkte der Kurve C. Die formale Potenzreihe

$$Z(T) \;:=\; \exp\left\{\sum_{n\geq 1} N_n \frac{T^n}{n}\right\} \;\in\; \mathbb{Q}[[T]]$$

nennt man die *Zeta-Funktion* der Kurve C.

Bemerkung: Die Funktion $Z(T)$ ist wohldefiniert, da die formale Potenzreihe $\sum\limits_{n\geq 1} N_n \frac{T^n}{n}$ kein Absolutglied besitzt. Absolute Konvergenz der Funktion $Z(T)$ erhält man für $|T| < 1/q$. Die Zeta-Funktion der Kurve C hängt von dem Körper ab, über dem wir die Kurve definieren.

Lemma 2.3 *Gegeben sei eine Kurve C definiert über $\mathbb{F}_q$, die nicht-singulär und projektiv ist. Es bezeichne b_d die Anzahl der Bahnen von C unter der Galois-Gruppe $Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$, die die Länge d besitzen. Dann gilt:*

$$N_n = \sum_{d|n} d \cdot b_d \;.$$

Beweis: [Lor96, KapVII, S.235].

Unter Zuhilfenahme von Lemma (2.3) können wir folgenden Satz beweisen:

Satz 2.4 (Euler-Darstellung). *Die Zeta-Funktion $Z(T) = \exp\left\{\sum_{n\geq 1} N_n \frac{T^n}{n}\right\}$ der Kurve C über $\mathbb{F}_q$ besitzt folgende Produktdarstellung:*

$$Z(T) = \prod_{[P]\in C/\,Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \left(1 - T^{deg\,[P]}\right)^{-1}.$$

Beweis: Es ist $Z(T) = \exp\left\{\sum_{n\geq 1} N_n \frac{T^n}{n}\right\}$. Setze nach Lemma (2.3) für die Anzahl der $\mathbb{F}_{q^n}$-rationalen Punkte N_n die Summe $\sum_{d|n} d \cdot b_d$ ein, dann ist

$$Z(T) = \exp\left\{\sum_{n\geq 1} N_n \frac{T^n}{n}\right\} \;=\; \exp\left\{\sum_{n\geq 1}\left(\sum_{d|n} d\cdot b_d\right)\frac{T^n}{n}\right\}.$$

Da die Reihenentwicklung von exp mit $1 + \ldots$ beginnt, dürfen wir die Exponentialdarstellung der Zeta-Funktion logarithmieren (s.[Lor96, KapVIII, S.278f]):

$$\log\left(Z(T)\right) \;=\; \sum_{n\geq 1}\left(\sum_{d|n} d\cdot b_d\right)\frac{T^n}{n}.$$

Für $n = d \cdot i$ erhält man nach Umordnung den Ausdruck

$$\sum_{d\geq 1} d\cdot b_d \left(\sum_{i\geq 1}\frac{T^{d\cdot i}}{d\cdot i}\right) \;=\; \sum_{d\geq 1} b_d \left(\sum_{i\geq 1}\frac{T^{d\cdot i}}{i}\right).$$

Da $-\sum_{i\geq 1}\frac{T^{di}}{i} \;=\; \log\left(1 - T^d\right)$ ist, ergibt sich

$$\begin{aligned}\sum_{d\geq 1} b_d \left(\sum_{i\geq 1}\frac{T^{d\cdot i}}{i}\right) \;&=\; \sum_{d\geq 1} b_d \left(-\log\left(1 - T^d\right)\right) \\ &=\; \sum_{d\geq 1}(-b_d)\log\left(1 - T^d\right).\end{aligned}$$

Da es sich beim letzten Ausdruck um eine spezielle (s. [Lor96, KapVIII, S.278f]) formale Potenzreihe handelt, kann man dafür auch schreiben

$$\log \prod_{d \geq 1} \left(1 - T^d\right)^{-b_d}.$$

Also ist

$$\begin{aligned} Z(T) &= \prod_{d \geq 1} \left(1 - T^d\right)^{-b_d} \\ &= \prod_{[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \left(1 - T^{deg\ [P]}\right)^{-1}, \end{aligned}$$

da die Zahl b_d die Anzahl der Primdivisoren $[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ vom Grad d bezeichnet. □

Satz 2.5 *Für die Zeta-Funktion der Kurve C definiert über $\mathbb{F}_q$ gilt:*

$$Z(T) = \prod_{[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \left(1 - T^{deg\ [P]}\right)^{-1} = \sum_{\substack{D \in \mathcal{D}(C) \\ D\ positiv}} T^{deg\ D}.$$

Beweis: Jeder Faktor des Eulerproduktes kann als geometrische Reihe geschrieben werden, und wir erhalten

$$\prod_{[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \left(1 - T^{deg\ [P]}\right)^{-1} = \prod_{[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)} \sum_{n \geq 0} T^{n \cdot deg\ [P]}.$$

Ausmultiplizieren und Sortieren liefert

$$1 + \sum_{k \geq 1} \sum_{[P]} T^{k \cdot deg\ [P]} + \sum_{\substack{k \geq 1 \\ l \geq 1}} \sum_{[P]} \sum_{[Q]} T^{k \cdot deg\ [P] + l \cdot deg\ [Q]} + \dots .$$

Da der Grad eines positiven Divisors D einer Kurve C gegeben ist durch $deg\ D = \sum_{[P]} n_P \cdot deg\ [P]$ mit $n_P \geq 0$, läßt sich obige Summe schreiben als

$$\sum_{\substack{D \in \mathcal{D}(C) \\ D\ positiv}} T^{deg\ D}.$$

□

Bezeichnet a_d die Anzahl der positiven Divisoren der Kurve C, die den Grad d besitzen, dann kann man für $\sum_{\substack{D \in \mathcal{D}(C) \\ D\ positiv}} T^{deg\ D}$ auch

$$\sum_{n \geq 0} a_n T^n$$

schreiben.

Die Zahlen N_d, b_d und a_d aus den äquivalenten Darstellungen der Zeta-Funktion kann man ineinander überführen. Bevor wir dies demonstrieren, führen wir aber noch eine weitere Zahl ein:

Definition 2.6 Ein Punkt $P \in C$ heißt *primitiv vom Grad* d, wenn er erst in der Körpererweiterung $\mathbb{F}_{q^d}$ auftritt, d. h. alle Koordinaten aus $\mathbb{F}_{q^d}$ sind. Es bezeichne c_d^{prim} die Anzahl derjenigen Punkte der Kurve C, die primitiv vom Grad d sind.

Wir haben also

$$\begin{aligned} c_d^{prim} &= \#\{\text{ Punkte von } C, \text{ primitiv vom Grad } d\,\}, \\ a_d &= \#\{\text{ positive Divisoren vom Grad } d \text{ von } C\,\}, \\ b_d &= \#\{\text{ Bahnen vom Grad } d \text{ von } C \text{ unter } Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)\,\}, \\ N_d &= \#\{\,\mathbb{F}_{q^d}\text{-rationale Punkte der Kurve } C\,\}. \end{aligned}$$

Wegen Lemma (2.3) gilt:

$$N_n = \sum_{d|n} d \cdot b_d .$$

Man macht sich leicht klar, daß zwischen der Anzahl der Bahnen vom Grad d und der Zahl der primitiven Punkte vom Grad d folgender Zusammenhang besteht:

$$b_d = \frac{c_d^{prim}}{d} .$$

Die Anzahl der Bahnen mit d Elementen ist gerade die Anzahl der primitiven Punkte der Kurve in $\mathbb{F}_{q^d}$, geteilt durch die Länge der Bahn. Somit ist

$$N_n = \sum_{d|n} c_d^{prim} .$$

Hat man also bei vorgegebenem n die Zahlen c_d^{prim} oder b_d gegeben, wobei die $d \leq n$ Teiler von n sind, so kann man die Zahl N_n ausrechnen. Eine Umkehrung ist möglich mit Hilfe der *Möbius-Transformation* (siehe z. B. [LN83, KapIII, S.92]):

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) \cdot N_d = c_n^{prim} = n \cdot b_n .$$

Lemma 2.7 *Für die a_d's erhält man aus den entsprechenden Darstellungen der Zeta-Funktion folgende Rekursionsformel:*

$$n \cdot a_n = \sum_{k=0}^{n-1} a_k \cdot N_{n-k} .$$

Beweis: Es ist

$$Z(T) = \sum_{n \geq 0} a_n T^n = \exp\left\{\sum_{n \geq 1} N_n \frac{T^n}{n}\right\}.$$

Wir bilden von beiden Darstellungen die logarithmische Ableitung, und multiplizieren mit T, dann gilt

$$\frac{\sum\limits_{n \geq 0} n \cdot a_n T^n}{\sum\limits_{n \geq 0} a_n T^n} = \sum_{n \geq 1} N_n T^n .$$

Wir bringen $\sum_{n \geq 0} a_n T^n$ auf die rechte Seite, setzen $N_0 := 0$, und erhalten

$$\sum_{n \geq 0} n \cdot a_n T^n = \sum_{n \geq 0} N_n T^n \cdot \sum_{n \geq 0} a_n T^n .$$

Nun können wir auf der rechten Seite das Cauchy-Produkt bilden, dies liefert uns

$$\sum_{n\geq 0} n \cdot a_n T^n \;=\; \sum_{n\geq 0} \left(\sum_{k=0}^{n} a_k \cdot N_{n-k} \right) T^n .$$

Jetzt führen wir noch einen Koeffizientenvergleich für T^n durch, und es ist

$$n \cdot a_n = \sum_{k=0}^{n} a_k \cdot N_{n-k} \; .$$

Für $k = n$ ist $N_{n-k} = N_0 = 0$, man kann also die Obergrenze der Summe auf $n-1$ setzen:

$$n \cdot a_n = \sum_{k=0}^{n-1} a_k \cdot N_{n-k} \; .$$

□

Wir sehen im nächsten Satz, daß die Zeta-Funktion noch eine weitere sehr wichtige Darstellung hat, nämlich als Quotient von zwei Polynomen. Dort spielt zum ersten Mal das Geschlecht einer Kurve eine Rolle. Wir wissen aus Abschnitt (2.1), daß das Geschlecht einer Kurve C definiert über $\mathbb{F}_q$ gleich dem Geschlecht des entsprechenden Funktionenkörpers $\mathbb{F}_q(C)$ ist. Der Begriff des Geschlechts erlaubt uns, die Kurven nach ihrer Komplexität zu klassifizieren. Das Geschlecht einer Kurve wird oft *geometrische* Invariante der Kurve genannt, weil es sich nicht unter Konstantenerweiterungen des Grundkörpers $\mathbb{F}_q$ verändert.
Die Rationalität der Zeta-Funktion zeigt einen komplexen, aber voraussagbaren Zusammenhang zwischen den verschiedenen N_n's auf.

Satz 2.8 (Die Rationalität der Zeta-Funktion). *Sei C eine nicht-singuläre projektive Kurve vom Geschlecht g. Dann ist*

$$Z(T) \;=\; \frac{L(T)}{(1-T)(1-qT)} \; ,$$

wobei $L(T)$ ein Polynom ist.

Beweis: [Lor96, KapVIII, S.285].

Definition 2.9 Das Polynom $L(T) := (1-T)(1-qT)\cdot Z(T)$ nennt man *L-Polynom* der Kurve C.

Genaueres über die Gestalt des L-Polynoms besagt folgender Satz:

Satz 2.10

(i) $L(T) \in \mathbb{Z}[T]$.

(ii) Der Grad des L-Polynoms beträgt $2g$.

(iii) $L(T)$ zerfällt über $\mathbb{C}[T]$ in der Form

$$L(T) \;=\; \prod_{\alpha=1}^{2g} (1 - z_\alpha T) \; .$$

Die Zahlen $z_1, \ldots, z_{2g}$ sind ganze algebraische Zahlen, und können so geordnet werden, daß $z_\alpha z_{g+\alpha} = q$ gilt, für $\alpha = 1, \ldots, g$.

Beweis: [Lor96, KapVIII, S.287].

Bemerkung: Eine komplexe Zahl z nennt man *ganze algebraische Zahl*, wenn sie einer Gleichung $z^m + c_{m-1}z^{m-1} + \cdots + c_1 z + c_0 = 0$ mit Koeffizienten $c_i \in \mathbb{Z}$ genügt.

Nun können wir ein äußerst erstaunliches Korollar formulieren. Aus der Rationalität der Zeta-Funktion folgt nämlich, daß die unendliche Menge $\{ N_n \mid n \geq 1 \}$ vollständig aus einer endlichen Menge an Information, $\{ z_\alpha \mid \alpha = 1, \ldots, 2g \}$, gewonnen werden kann:

Korollar 2.11 *Für jedes $n \geq 1$ gilt*

$$N_n \;=\; q^n + 1 - \sum_{\alpha=1}^{2g} {z_\alpha}^n \;,$$

wobei die $z_1, \ldots, z_{2g}$ die Kehrwerte der Nullstellen von $L(T)$ sind. Speziell haben wir für $N := N_1 = \mid C(\mathbb{F}_q) \mid$

$$N \;=\; q + 1 - \sum_{\alpha=1}^{2g} z_\alpha \;.$$

Beweis: Es gilt

$$Z(T) \;=\; \exp\left\{ \sum_{n\geq 1} N_n \frac{T^n}{n} \right\} \;=\; \frac{\prod\limits_{\alpha=1}^{2g} (1 - z_\alpha T)}{(1-T)(1-qT)} \;. \qquad (*)$$

Nun bilden wir auf beiden Seiten die logarithmische Ableitung und multiplizieren mit T. Dies führen wir zunächst auf der linken Seite durch, und erhalten:

$$T \cdot \frac{d}{dT} \log \left(\exp\left\{ \sum_{n\geq 1} N_n \frac{T^n}{n} \right\} \right) \;=\; \sum_{n\geq 1} N_n T^n.$$

Nun betrachten wir die logarithmische Ableitung der rechten Seite unserer Ausgangsgleichung $(*)$ und multiplizieren mit T:

$$T \cdot \frac{d}{dT} \log \left(\frac{\prod\limits_{\alpha=1}^{2g} (1 - z_\alpha T)}{(1-T)(1-qT)} \right) \;.$$

Wir vereinfachen dies zu

$$T \cdot \frac{d}{dT} \left(\sum_{\alpha=1}^{2g} \log(1 - z_\alpha T) - \log(1-T) - \log(1-qT) \right) \;,$$

und setzen für log wieder die entsprechende Potenzreihe ein:

$$T \cdot \frac{d}{dT} \left(\sum_{\alpha=1}^{2g} \left(- \sum_{n\geq 1} \frac{(z_\alpha T)^n}{n} \right) + \sum_{n\geq 1} \frac{T^n}{n} + \sum_{n\geq 1} \frac{(qT)^n}{n} \right) \;.$$

Die Ableitung des Ausdrucks, anschließend multipliziert mit T, liefert

$$\sum_{n\geq 1} \left(- \sum_{\alpha=1}^{2g} {z_\alpha}^n T^n \right) + \sum_{n\geq 1} T^n + \sum_{n\geq 1} q^n T^n \;.$$

Wir schreiben

$$\sum_{n\geq 1}\left(-\sum_{\alpha=1}^{2g} {z_\alpha}^n + 1 + q^n\right) T^n \ ,$$

und fügen die linke und rechte Seite von $(*)$ wieder zusammen. Dann erhalten wir den Ausdruck

$$\sum_{n\geq 1} N_n T^n \quad = \quad \sum_{n\geq 1}\left(-\sum_{\alpha=1}^{2g} {z_\alpha}^n + 1 + q^n\right) T^n \ .$$

Ein Koeffizientenvergleich für T^n liefert das gewünschte Ergebnis:

$$N_n \ = \ q^n + 1 - \sum_{\alpha=1}^{2g} {z_\alpha}^n \ .$$

□

Das nächste Korollar gibt die Zeta-Funktionen elliptischer Kurven (Kurven vom Geschlecht $g = 1$) an. Wir benutzen die Tatsache, daß nicht-singuläre kubische Kurven elliptisch sind. Für elliptische Kurven sind alle N_n für $n \geq 1$ durch N_1 bestimmt.

Korollar 2.12 (Die Zeta-Funktionen elliptischer Kurven). *Sei F ein homogenes Polynom vom Grad 3 in $\mathbb{F}_q[x_0, x_1, x_2]$. Sei die durch das Polynom gegebene Kurve C nicht-singulär. Sei $N = N_1 = |C(\mathbb{F}_q)|$. Dann ist die Zeta-Funktion der Kurve C gegeben durch*

$$Z(T) \ = \ \frac{1 + (N - q - 1)T + qT^2}{(1-T)(1-qT)} \ .$$

Beweis: Da elliptische Kurven das Geschlecht 1 besitzen, ist das L-Polynom dieser Kurven nach Satz (2.10) gegeben durch

$$L(T) \ = \ (1 - z_1 T)(1 - z_2 T) \, .$$

Nach Korollar (2.11) ist N gegeben durch

$$N \ = \ q + 1 - (z_1 + z_2) \ ,$$

so daß $L(T) \ = \ 1 + (N - q - 1)T + z_1 z_2 T^2$ ist. Nach (2.10) ist $z_1 z_2 = q$. □

An einem Beispiel einer konkreten elliptischen Kurve machen wir uns die Bedeutung des Satzes klar:

Beispiel: *Sei*

$$F(x_0, x_1, x_2) \ = \ {x_0}^3 + {x_1}^3 + {x_2}^3 \ \in \ \mathbb{F}_2[x_0, x_1, x_2]$$

gegeben. Die durch das Polynom F definierte kubische Kurve C ist nicht-singulär, was man leicht sieht, wenn man sich die partiellen Ableitungen von F anschaut. Es ist leicht nachzurechnen, daß $C(\mathbb{F}_2) = \{(0:1:1), (1:0:1), (1:1:0)\}$ und damit $N = 3$ ist. Wir haben $N = 3$ und $q = 2$, damit hat das L-Polynom nach (2.12) die Gestalt

$$L(T) \ = \ 1 + (3 - 2 - 1) \cdot T + 2 \cdot T^2 \ = \ 1 + 2 \cdot T^2 \ .$$

Die beiden Nullstellen sind $\frac{i}{\sqrt{2}}$ *und* $-\frac{i}{\sqrt{2}}$*, die Kehrwerte davon sind* $-i\sqrt{2} = z_1$ *und* $i\sqrt{2} = z_2$*. Also können wir nach (2.11) die* N_n*'s bestimmen:*

$$N_n \;=\; 2^n + 1 - ((-i\sqrt{2})^n + (i\sqrt{2})^n) \;.$$

Speziell gilt für N_2*:*

$$\begin{aligned} N_2 &= 2^2 + 1 - ((-i\sqrt{2})^2 + (i\sqrt{2})^2) \\ &= 5 - (-4) \\ &= 9 \;. \end{aligned}$$

Zur Überprüfung rechnen wir nun die $\mathbb{F}_4$*-rationalen Punkte der Kurve* C *aus. Da* $\mathbb{F}_4^*$ *zyklisch von der Ordnung 3 ist, haben wir sofort*

$$C(\mathbb{F}_4) = \{(a:1:0), (1:0:b), (0:1:c) \mid a,b,c \in \mathbb{F}_4^*\} \;.$$

Also ist $N_2 = 9$*.*

Kapitel 3

Obere Schranken für N

Wie zuvor ist C eine nicht-singuläre projektive Kurve vom Geschlecht g, definiert über $\mathbb{F}_q$.

3.1 Abschätzungen für $N = | C(\mathbb{F}_q) |$

Wir wollen nun explizite Schranken für die Anzahl der $\mathbb{F}_q$-rationalen Punkte N einer Kurve C angeben. Dies erreichen wir, indem wir die sogenannte *Riemannsche Vermutung*, die 1940 von Weil für Kurven über endlichen Körpern bewiesen wurde, benutzen.

Satz 3.1 (Hasse-Weil-Theorem). *Die Kehrwerte der Nullstellen des Polynoms $L(T) = \prod_{\alpha=1}^{2g} (1 - z_\alpha T)$ haben die Eigenschaft*

$$| z_\alpha | = \sqrt{q} \qquad \text{für } \alpha = 1, \ldots, 2g \, .$$

Beweis: [Sti93, KapV, S.169].

Dies liefert direkt eine Möglichkeit der Abschätzung von N:

Satz 3.2 (Hasse-Weil-Schranke). *Die Zahl N der $\mathbb{F}_q$-rationalen Punkte einer Kurve C vom Geschlecht g kann abgeschätzt werden durch:*

$$| N - (q+1) | \leq 2g\sqrt{q} \, .$$

Beweis: Für die $\mathbb{F}_q$-rationalen Punkte N gilt nach (2.11)

$$N - (q+1) = -\sum_{\alpha=1}^{2g} z_\alpha \, .$$

Wir betrachten die Beträge auf beiden Seiten:

$$| N - (q+1) | = \left| \sum_{\alpha=1}^{2g} z_\alpha \right| ,$$

und wenden auf die rechte Seite die Dreiecksungleichung an:

$$\left| \sum_{\alpha=1}^{2g} z_\alpha \right| \leq \sum_{\alpha=1}^{2g} | z_\alpha | \, .$$

An dieser Stelle benutzen wir das Hasse-Weil-Theorem (3.1). Somit gilt

$$\begin{aligned}\sum_{\alpha=1}^{2g} |\, z_\alpha \,| &= \sum_{\alpha=1}^{2g} \sqrt{q} \\ &= 2g\sqrt{q}\,.\end{aligned}$$

Wir haben insgesamt

$$|\, N - (q+1)\,| \leq 2g\sqrt{q}\,.$$

□

Eine einfache Verbesserung dieser Abschätzung erhalten wir, indem wir den ganzzahligen Anteil der rechten Seite betrachten:

$$|\, N - (q+1)\,| \leq [2g\sqrt{q}]\,.$$

Ein besseres Ergebnis liefert die Serre-Schranke:

Satz 3.3 (Serre-Schranke). *Für eine Kurve C vom Geschlecht g ist die Anzahl der $\mathbb{F}_q$-rationalen Punkte beschränkt durch*

$$|\, N - (q+1)\,| \leq g\,[2\sqrt{q}]\,.$$

Beweis: [Sti93, KapV, S.180].

Man kann Kurven nach ihrem Geschlecht klassifizieren. Je größer das Geschlecht einer Kurve ist, umso komplexer ist sie. Wie groß ist nun die maximale Anzahl der $\mathbb{F}_q$-rationalen Punkte, die Kurven von einem bestimmten Geschlecht haben können? Wir führen folgende Bezeichnung ein:

Definition 3.4 Für g und q fest gewählt bezeichne $N_q(g)$ das Maximum von N, wenn C alle Kurven vom Geschlecht g über $\mathbb{F}_q$ durchläuft.

Nach (3.3) haben wir

$$N_q(g) \leq q + 1 + g\,[2\sqrt{q}]\,.$$

Im nächsten Abschnitt wird eine Methode vorgestellt, die eine wesentliche Verbesserung der obigen Abschätzung liefert.

3.2 Die Methode von Serre

Um schärfere Abschätzungen für $N_q(g)$ zu erhalten, benutzt Serre in seinem Artikel [Ser83] die sogenannten *expliziten Formeln* von Weil. Nach dem Hasse-Weil-Theorem (3.1) ist der Betrag der Kehrwerte der Nullstellen des L-Polynoms gleich $\sqrt{q}$, somit lautet die Euler-Darstellung dieser komplexen Zahlen:

$$z_\alpha \;=\; \sqrt{q}\cdot e^{i\Theta_\alpha}\;, \qquad \Theta_\alpha \in \mathbb{R}\,.$$

Satz 3.5 (Explizite Formeln von Weil). *Sei C eine Kurve vom Geschlecht g, definiert über dem Körper $\mathbb{F}_q$. Es sei*

$$f(\Theta_\alpha) \;:=\; 1 + 2\cdot\sum_{r=1}^{m} c_r\cdot\cos\left(r\,\Theta_\alpha\right)\;,$$

und

$$\Psi(t) \;:=\; \sum_{r=1}^{m} c_r\cdot t^r\;,$$

wobei $t\in\mathbb{C}$, $t\neq 0$, $c_1,\ldots,c_m\in\mathbb{R}$ und $\Theta_\alpha\in\mathbb{R}$ wie oben für $\alpha=1,\ldots,g$ sind. Dann gilt

$$N\cdot\Psi\left(\frac{1}{\sqrt{q}}\right) \;=\; \Psi(\sqrt{q}) + \Psi\left(\frac{1}{\sqrt{q}}\right) + g - \sum_{\alpha=1}^{g} f(\Theta_\alpha) - \sum_{r=1}^{m}\left(N_r - N\right)\cdot\frac{c_r}{\left(\sqrt{q}\right)^r}\,.$$

(Explizite Formeln von Weil)

Beweis: Für $N_r = |C(\mathbb{F}_{q^r})|$ gilt nach (2.11)

$$N_r \;=\; q^r + 1 - \sum_{\alpha=1}^{2g} {z_\alpha}^r\,.$$

Die Kehrwerte der Nullstellen des L-Polynoms haben die Euler-Darstellung

$$z_\alpha \;=\; \sqrt{q}\cdot e^{i\Theta_\alpha}\;, \qquad \Theta_\alpha \in \mathbb{R}\,.$$

Damit haben wir

$${z_\alpha}^r \;=\; \left(\sqrt{q}\right)^r\cdot e^{ir\Theta_\alpha}\,.$$

Wegen des Hasse-Weil-Theorems (3.1) und Satz (2.10 (iii)) können wir annehmen, daß gilt

$$z_{\alpha+g} \;=\; \overline{z_\alpha}\,.$$

Also können wir schreiben

$$\begin{aligned}
N_r &= q^r + 1 - \sum_{\alpha=1}^{g}\left({z_\alpha}^r + {z_{\alpha+g}}^r\right)\\
&= q^r + 1 - \sum_{\alpha=1}^{g}\left({z_\alpha}^r + \left(\overline{z_\alpha}\right)^r\right)\\
&= q^r + 1 - \sum_{\alpha=1}^{g}\left(\left(\sqrt{q}\right)^r\cdot e^{ir\Theta_\alpha} + \left(\sqrt{q}\right)^r\cdot e^{-ir\Theta_\alpha}\right)\\
&= q^r + 1 - \left(\sqrt{q}\right)^r\cdot\sum_{\alpha=1}^{g}\left(e^{ir\Theta_\alpha} + e^{-ir\Theta_\alpha}\right)\,.
\end{aligned}$$

Bekanntlich ist $\cos(r\Theta_\alpha) = \frac{1}{2}\left(e^{ir\Theta_\alpha} + e^{-ir\Theta_\alpha}\right)$. Wir benutzen dies, und erhalten

$$N_r = q^r + 1 - (\sqrt{q})^r \cdot 2 \cdot \sum_{\alpha=1}^{g} \cos(r\Theta_\alpha) .$$

Wir multiplizieren beide Seiten dieser Gleichung mit dem Term $\frac{1}{(\sqrt{q})^r}$, dies liefert uns

$$\frac{N_r}{(\sqrt{q})^r} = (\sqrt{q})^r + \frac{1}{(\sqrt{q})^r} - 2 \cdot \sum_{\alpha=1}^{g} \cos(r\Theta_\alpha) .$$

Gegeben seien die reellen Zahlen $c_1, c_2, \dots$. Wir multiplizieren obige Gleichung mit c_r und haben

$$N_r \cdot \frac{c_r}{(\sqrt{q})^r} = c_r \cdot (\sqrt{q})^r + \frac{c_r}{(\sqrt{q})^r} - 2 \cdot \sum_{\alpha=1}^{g} c_r \cdot \cos(r\Theta_\alpha) .$$

Das Aufsummieren dieser Gleichungen für $r = 1, \dots, m$ ergibt

$$\sum_{r=1}^{m} N_r \cdot \frac{c_r}{(\sqrt{q})^r} = \sum_{r=1}^{m} c_r \cdot (\sqrt{q})^r + \sum_{r=1}^{m} \frac{c_r}{(\sqrt{q})^r} - 2 \cdot \sum_{\alpha=1}^{g}\sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha) .$$

Wir definieren

$$\Psi(t) := \sum_{r=1}^{m} c_r \cdot t^r ,$$

wobei $t \in \mathbb{C}$, $t \neq 0$. Für t setzen wir $\sqrt{q}$ beziehungsweise $\frac{1}{\sqrt{q}}$ ein, und erhalten

$$\sum_{r=1}^{m} N_r \cdot \frac{c_r}{(\sqrt{q})^r} = \Psi(\sqrt{q}) + \Psi\left(\frac{1}{\sqrt{q}}\right) - 2 \cdot \sum_{\alpha=1}^{g}\sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha) \qquad (*) .$$

Wir formen den Summanden $-2 \cdot \sum_{\alpha=1}^{g}\sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha)$ etwas um:

$$\begin{aligned}
-2 \cdot \sum_{\alpha=1}^{g}\sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha) &= -\sum_{\alpha=1}^{g}\left(2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha)\right) \\
&= -\sum_{\alpha=1}^{g}\left(-1 + 1 + 2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha)\right) \\
&= -\sum_{\alpha=1}^{g}(-1) - \sum_{\alpha=1}^{g}\left(1 + 2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha)\right) \\
&= g - \sum_{\alpha=1}^{g}\left(1 + 2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha)\right) .
\end{aligned}$$

Wir setzen

$$f(\Theta_\alpha) := 1 + 2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\,\Theta_\alpha) ,$$

und erhalten damit insgesamt für den betrachteten Summanden

$$-2 \cdot \sum_{\alpha=1}^{g}\sum_{r=1}^{m} c_r \cdot \cos(r\Theta_\alpha) = g - \sum_{\alpha=1}^{g} f(\Theta_\alpha) .$$

Dies setzen wir in $(*)$ ein. Damit haben wir

$$\sum_{r=1}^{m} N_r \cdot \frac{c_r}{(\sqrt{q})^r} \;=\; \Psi(\sqrt{q}) \;+\; \Psi\left(\frac{1}{\sqrt{q}}\right) \;+\; g \;-\; \sum_{\alpha=1}^{g} f(\Theta_\alpha)\;.$$

Nun subtrahieren wir $\sum\limits_{r=1}^{m} (N_r \,-\, N) \cdot \frac{c_r}{(\sqrt{q})^r}$ auf beiden Seiten der Gleichnung, dies ergibt die gesuchte Formel

$$N \cdot \Psi\left(\frac{1}{\sqrt{q}}\right) \;=\; \Psi(\sqrt{q}) \;+\; \Psi\left(\frac{1}{\sqrt{q}}\right) \;+\; g \;-\; \sum_{\alpha=1}^{g} f(\Theta_\alpha) \;-\; \sum_{r=1}^{m} (N_r \,-\, N) \cdot \frac{c_r}{(\sqrt{q})^r}.$$

□

Nach [Ser83] erhalten wir aus den expliziten Formeln von Weil eine Abschätzung für N:

Proposition 3.6 *Wir nehmen nun an, daß die Zahlen $c_1, \ldots, c_m$ aus $\mathbb{R}$ den beiden folgenden Bedingungen genügen:*

(i) $c_r \geq 0$ *für $r = 1, \ldots, m$, und nicht alle $c_r = 0$.*

(ii) $f(\Theta) \geq 0$ *für alle $\Theta \in \mathbb{R}$.*

Dann ist die Zahl $N = |C(\mathbb{F}_q)|$ beschränkt durch

$$N \;\leq\; \frac{g}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; \frac{\Psi(\sqrt{q})}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; 1\;.$$

Beweis: Wir haben

$$N \cdot \Psi\left(\frac{1}{\sqrt{q}}\right) \;=\; \Psi(\sqrt{q}) \;+\; \Psi\left(\frac{1}{\sqrt{q}}\right) \;+\; g \;-\; \sum_{\alpha=1}^{g} f(\Theta_\alpha) \;-\; \sum_{r=1}^{m} (N_r \,-\, N) \cdot \frac{c_r}{(\sqrt{q})^r}\;.$$

Es ist klar, daß $N \,=\, N_1 \,\leq\, N_r$ gilt. Zusammen mit den Annahmen (i) und (ii) wissen wir, daß die beiden Summanden $-\sum\limits_{\alpha=1}^{g} f(\Theta_\alpha)$ und $-\sum\limits_{r=1}^{m} (N_r \,-\, N) \cdot \frac{c_r}{(\sqrt{q})^r}$ kleiner als Null sind. Damit können wir $N \cdot \Psi\left(\frac{1}{\sqrt{q}}\right)$ abschätzen durch

$$N \cdot \Psi\left(\frac{1}{\sqrt{q}}\right) \;\leq\; \Psi(\sqrt{q}) \;+\; \Psi\left(\frac{1}{\sqrt{q}}\right) \;+\; g\,.$$

Wir dividieren beide Seiten durch $\Psi\left(\frac{1}{\sqrt{q}}\right)$ und erhalten die gesuchte Abschätzung für N:

$$N \;\leq\; \frac{g}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; \frac{\Psi(\sqrt{q})}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; 1\;.$$

□

Jedes gerade trigonometrische Polynom f, welches in der Form

$$f(\Theta) = 1 + 2 \cdot \sum_{r=1}^{m} c_r \cos(r\Theta)$$

geschrieben werden kann und die beiden Bedingungen (i) und (ii) aus Proposition (3.6) erfüllt, liefert eine obere Abschätzung für N, also auch für $N_q(g)$. Es kommt also darauf an, ein solches f geschickt zu wählen, um eine gute Abschätzung für $N_q(g)$ zu erhalten. Wir wählen zum Beispiel

$$f(\Theta) = 1 + \cos(\Theta)\,.$$

Wir bringen das Polynom f auf die Form

$$f(\Theta) \;=\; 1 + 2 \cdot c_1 \cos(\Theta)\,,$$

indem wir $c_1 = \frac{1}{2} > 0$ setzen. Da auch $f(\Theta) \geq 0$ ist für alle $\Theta \in \mathbb{R}$, können wir Proposition (3.6) anwenden. Wir erhalten mit $\Psi(\sqrt{q}) = \frac{1}{2}\sqrt{q}$ und $\Psi\left(\frac{1}{\sqrt{q}}\right) = \frac{1}{2}\frac{1}{\sqrt{q}}$ die Ungleichung

$$N \leq 2\sqrt{q} \cdot (\, g \,+\, \frac{1}{2}\sqrt{q}\,) \,+\, 1\,.$$

Vereinfachen wir dies, so ergibt sich die Abschätzung von Weil:

$$N \leq q + 1 + 2g\sqrt{q}\,.$$

3.3 Bestimmung von oberen Schranken für $N_q(g)$ mit der Serre-Methode

In diesem Abschnitt suchen wir eine obere Schranke für $N_q(g)$, die maximale Anzahl der $\mathbb{F}_q$-rationalen Punkte der Kurven vom Geschlecht g. Dazu benutzen wir die Methode von Serre. Wir müssen also ein nach Proposition (3.6) passendes trigonometrisches Polynom wählen. Wir verwenden die in dem Artikel [Ser83] angegebene Möglichkeit, da leicht nachzuweisen ist, daß dieses Polynom die Bedingungen aus Proposition (3.6) erfüllt. Das Polynom lautet:

$$\tilde{f}(\Theta) \;:=\; \frac{1}{c} \cdot \left(1 \;+\; 2 \cdot \sum_{j=1}^{n} x_j \cos{(j\Theta)} \right)^2 ,$$

mit $x_j > 0$ für $j = 1, \ldots, n$ und c definiert durch $c \;:=\; 1 \;+\; 2 \cdot \sum\limits_{j=1}^{n} {x_j}^2$.

Wir müssen $\tilde{f}$ zunächst in die Form

$$\tilde{f}(\Theta) \;=\; 1 + 2 \cdot \sum_{r=1}^{m} c_r \cos{(r\,\Theta)}$$

bringen. Dies bedeutet: der Ausdruck

$$\frac{1}{c} \cdot \left(1 \;+\; 2 \cdot \sum_{j=1}^{n} x_j \cos{(j\Theta)} \right)^2$$

muß so umsortiert werden, daß wir

$$1 + 2 \cdot \sum_{r=1}^{m} c_r \cos{(r\,\Theta)}$$

erhalten, wobei sich die Koeffizienten c_r auf noch zu bestimmende Weise aus den x_j zusammensetzen. Um eine solche Darstellung zu erhalten, bedarf es eines umfangreichen sehr technischen Beweises, den wir in mehrere Lemmata aufteilen:

Lemma 3.7 *Es seien $x_j \in \mathbb{R}$ für $j = 1, \ldots, n$, und $\Theta \in \mathbb{R}$, dann gilt*

$$\left(1 + 2 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2 = 1 + 4 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta) + 4 \cdot \sum_{j=1}^{n} {x_j}^2 \cos^2(j\Theta)$$
$$+ 4 \cdot \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cos(j\Theta) \cos(k\Theta).$$

Beweis: Nach der ersten binomischen Formel ist

$$\left(1 + 2 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2 = 1 + 4 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta) + 4 \cdot \left(\sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2.$$

Wir betrachten den Summanden

$$4 \cdot \left(\sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2.$$

Faßt man die quadratischen und die gemischten Terme jeweils zusammen, so erhält man

$$4 \cdot \left(\sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2 = 4 \cdot \sum_{j=1}^{n} {x_j}^2 \cos^2(j\Theta) + 4 \cdot \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cos(j\Theta) \cos(k\Theta).$$

Damit ist die Behauptung bewiesen. □

Wegen Lemma (3.7) können wir für $\tilde{f}$ schreiben

$$\begin{aligned}
\tilde{f}(\Theta) &= \frac{1}{c} \cdot \left(1 + 2 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta)\right)^2 \\
&= \frac{1}{c} \cdot \left(1 + 4 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta)\right. \\
&\qquad + 4 \cdot \sum_{j=1}^{n} {x_j}^2 \cos^2(j\Theta) \\
&\qquad \left. + \; 4 \cdot \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot \cos(j\Theta) \cdot \cos(k\Theta)\right).
\end{aligned}$$

Diese Summanden untersuchen wir im folgenden getrennt.

Lemma 3.8 *Es seien $\Theta \in \mathbb{R}$ und $x_j \in \mathbb{R}$ für $j = 1, \ldots, n$. Es gilt*

$$1 + 4 \cdot \sum_{j=1}^{n} {x_j}^2 \cos^2(j\Theta) = c + 2 \cdot \sum_{j=1}^{n} {x_j}^2 \cos(2j\Theta),$$

wobei $c = 1 + 2 \cdot \sum_{j=1}^{n} {x_j}^2$ ist.

Beweis: Es ist

$$\begin{aligned}\cos(2\Theta) &= \cos^2(\Theta) - \sin^2(\Theta) \\ &= \cos^2(\Theta) - \big(1 - \cos^2(\Theta)\big) \\ &= 2\cos^2(\Theta) - 1\,.\end{aligned}$$

Wir können also schreiben $\cos^2(\Theta) = \frac{1}{2}\cdot(1 + \cos(2\Theta))$. Diese Eigenschaft der Kosinus-Funktion benutzen wir in der folgenden Rechnung:

$$\begin{aligned}1 + 4\cdot\sum_{j=1}^{n} {x_j}^2\cos^2(j\Theta) &= 1 + 4\cdot\sum_{j=1}^{n} {x_j}^2\cdot\left(\frac{1}{2}\cdot(1 + \cos(2j\Theta))\right) \\ &= 1 + 2\cdot\sum_{j=1}^{n} {x_j}^2\cdot(1 + \cos(2j\Theta)) \\ &= \underbrace{1 + 2\cdot\sum_{j=1}^{n} {x_j}^2}_{=c} + 2\cdot\sum_{j=1}^{n} {x_j}^2\cos(2j\Theta)\,.\end{aligned}$$

□

Lemma 3.9 *Für $x_j \in \mathbb{R}$, $(j = 1, \ldots, n)$, und $\Theta \in \mathbb{R}$ gilt*

$$4\cdot\sum_{j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n} x_j x_k \cos(j\Theta)\cos(k\Theta) =$$
$$2\cdot\sum_{j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n} x_j x_k \cdot \big(\cos((j-k)\Theta) + \cos((j+k)\Theta)\big)\ .$$

Beweis: Es ist

$$\cos(\Theta_1 + \Theta_2) = \cos(\Theta_1)\cdot\cos(\Theta_2) - \sin(\Theta_1)\cdot\sin(\Theta_2),$$

und

$$\cos(\Theta_1 - \Theta_2) = \cos(\Theta_1)\cdot\cos(\Theta_2) + \sin(\Theta_1)\cdot\sin(\Theta_2).$$

Wir addieren diese beiden Gleichungen und erhalten

$$\cos(\Theta_1 - \Theta_2) + \cos(\Theta_1 + \Theta_2) = 2\cdot\cos(\Theta_1)\cdot\cos(\Theta_2).$$

Es gilt also

$$\cos(\Theta_1)\cdot\cos(\Theta_2) = \frac{1}{2}\cdot\big(\cos(\Theta_1 - \Theta_2) + \cos(\Theta_1 + \Theta_2)\big) \qquad (*)\ .$$

Wir betrachten die Doppelsumme

$$4\cdot\sum_{j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n} x_j x_k \cos(j\Theta)\cos(k\Theta)\,,$$

und benutzen nun obige Identität $(*)$, dies ergibt

$$4\cdot\sum_{j=1}^{n}\sum_{\substack{k=1\\k\neq j}}^{n} x_j x_k \cdot \frac{1}{2}\cdot\big(\cos(j\Theta - k\Theta) + \cos(j\Theta + k\Theta)\big)\,.$$

Diesen Ausdruck können wir noch vereinfachen zu

$$2 \cdot \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot (\cos((j-k)\Theta) + \cos((j+k)\Theta)) \ .$$

Damit ist die Behauptung gezeigt. □

Wir können nun $\tilde{f}$ in der folgenden Form schreiben:

$$\begin{aligned}
\tilde{f}(\Theta) &= \frac{1}{c} \cdot \left(1 \ + \ 2 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta) \right)^2 \\
&= \frac{1}{c} \cdot \left(4 \cdot \sum_{j=1}^{n} x_j \cdot \cos(j\Theta) \ + \ c \ + \ 2 \cdot \sum_{j=1}^{n} {x_j}^2 \cdot \cos(2j\Theta) \right. \\
&\qquad \left. + \ 2 \cdot \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot (\cos((j-k)\Theta) + \cos((j+k)\Theta)) \right) \\
&= 1 + 2 \cdot \frac{1}{c} \cdot \left(2 \cdot \sum_{j=1}^{n} x_j \cdot \cos(j\Theta) \ + \ \sum_{j=1}^{n} {x_j}^2 \cdot \cos(2j\Theta) \right. \\
&\qquad \left. + \ \sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot (\cos((j-k)\Theta) + \cos((j+k)\Theta)) \right) \ .
\end{aligned}$$

Dies ist noch nicht die gewünschte Form von $\tilde{f}$. Wir müssen die Doppelsumme in der Klammer noch so umsortieren, daß die Faktoren vor Θ in der Kosinus-Funktion nur von einem Index der Doppelsumme abhängen.

Lemma 3.10 *Es seien $x_j \in \mathbb{R}$ für $j = 1, \ldots, n$, und $\Theta \in \mathbb{R}$. Wir setzen*

$$A_n \ := \ \left\{ \begin{array}{c} 2 \cdot \sum\limits_{j=1}^{n} x_j \cdot \cos(j\Theta) \ + \ \sum\limits_{j=1}^{n} {x_j}^2 \cdot \cos(2j\Theta) \\ + \ \sum\limits_{j=1}^{n} \sum\limits_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot (\cos((j-k)\Theta) + \cos((j+k)\Theta)) \end{array} \right\} ,$$

und

$$B_n \ := \ \left\{ \begin{array}{c} \sum\limits_{r=1}^{n} \left(\left(\sum\limits_{i=0}^{r} x_i x_{r-i} \ + \ 2 \cdot \sum\limits_{i=1}^{n-r} x_i x_{r+i} \right) \cdot \cos(r\Theta) \right) \\ + \ \sum\limits_{l=n+1}^{2n} \sum\limits_{i=1}^{l-1} x_i x_{l-i} \cdot \cos(l\Theta) \end{array} \right\} .$$

Dann ist

$$A_n \ = \ B_n \ ,$$

wobei $x_0 := 1$ und $x_l := 0$ für $l \geq n+1$.

Beweis: Zum Beweis der Gleichheit der obigen Ausdrücke betrachten wir A_n und B_n als Polynome in den Unbestimmten $x_1, \ldots, x_n$. Bei dieser Betrachtungsweise können wir die Terme unseres Ausgangsausdrucks A_n in lineare, quadratische und gemischte Terme einteilen, und das Vorkommen dieser Terme in B_n untersuchen:

- lineare Terme: $2 \cdot \sum_{j=1}^{n} x_j \cdot \cos(j\Theta)$ (I),

- quadratische Terme: $\sum_{j=1}^{n} {x_j}^2 \cdot \cos(2j\Theta)$ (II),

- gemischte Terme: $\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k\neq j}}^{n} x_j x_k \cdot \cos((j-k)\Theta)$ (IIIa),

$\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k\neq j}}^{n} x_j x_k \cdot \cos((j+k)\Theta)$ (IIIb).

Wir betrachten den Ausdruck B_n:

$$
\begin{aligned}
B_n &= \sum_{r=1}^{n} \left(\left(\sum_{i=0}^{r} x_i x_{r-i} \; + \; 2 \cdot \sum_{i=1}^{n-r} x_i x_{r+i} \right) \cdot \cos(r\Theta) \right) \\
&\qquad + \sum_{l=n+1}^{2n} \sum_{i=1}^{l-1} x_i x_{l-i} \cdot \cos(l\Theta) \\
&= \sum_{r=1}^{n} \sum_{i=0}^{r} x_i x_{r-i} \cdot \cos(r\Theta) \; + \; 2 \cdot \sum_{r=1}^{n} \sum_{i=1}^{n-r} x_i x_{r+i} \cdot \cos(r\Theta) \\
&\qquad + \sum_{l=n+1}^{2n} \sum_{i=1}^{l-1} x_i x_{l-i} \cdot \cos(l\Theta) \, .
\end{aligned}
$$

Lineare Terme:
Wir sammeln zunächst die linearen Terme von B_n. Nach Definition ist $x_0 = 1$. In der ersten Doppelsumme haben wir für $i = 0$ die Summe

$$\sum_{r=1}^{n} x_r \cos(r\Theta).$$

Für $i = r$ ergibt sich ebenfalls die Summe

$$\sum_{r=1}^{n} x_r \cos(r\Theta).$$

In der zweiten Doppelsumme kann weder i gleich 0, noch i gleich $-r$ sein. Auch in der letzten Doppelsumme von B_n gilt $i \neq 0$ und $i \neq l$ für alle i. Wir haben also insgesamt an linearen Termen:

$$2 \cdot \sum_{r=1}^{n} x_r \cos(r\Theta),$$

was dem Ausdruck (I) aus A_n entspricht.

Wir können also für die erste Doppelsumme schreiben:

$$\sum_{r=1}^{n} \sum_{i=0}^{r} x_i x_{r-i} \cos(r\Theta) \; = \; \sum_{r=1}^{n} \sum_{i=1}^{r-1} x_i x_{r-i} \cos(r\Theta) \; + \; 2 \cdot \sum_{r=1}^{n} x_r \cos(r\Theta).$$

Wir betrachten die nicht-linearen Terme von B_n:

$$\sum_{r=1}^{n} \sum_{i=1}^{r-1} x_i x_{r-i} \cdot \cos(r\Theta) \; + \; 2 \cdot \sum_{r=1}^{n} \sum_{i=1}^{n-r} x_i x_{r+i} \cdot \cos(r\Theta)$$

$$+\sum_{l=n+1}^{2n}\sum_{i=1}^{l-1} x_i x_{l-i}\cdot\cos(l\Theta)\,.$$

Man sieht leicht, daß man die beiden Doppelsummen,

$$\sum_{r=1}^{n}\sum_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta) \quad\text{und}\quad \sum_{l=n+1}^{2n}\sum_{i=1}^{l-1} x_i x_{l-i}\cdot\cos(l\Theta)\,,$$

zu einer Summe zusammenfügen kann:

$$\sum_{r=1}^{2n}\sum_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta)\,.$$

Also haben wir noch

$$\sum_{r=1}^{2n}\sum_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta) \;+\; 2\cdot\sum_{r=1}^{n}\sum_{i=1}^{n-r} x_i x_{r+i}\cdot\cos(r\Theta)\,. \qquad (*)$$

Quadratische Terme:
In der Summe

$$2\cdot\sum_{r=1}^{n}\sum_{i=1}^{n-r} x_i x_{r+i}\cdot\cos(r\Theta)$$

kommen offensichtlich nur gemischte Terme vor. In

$$\sum_{r=1}^{2n}\sum_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta)$$

erhalten wir für $r = 2i$ folgende quadratischen Terme

$$\sum_{i=1}^{n} {x_i}^2\cos(2i\Theta)\,,$$

welche dem Ausdruck (II) von A_n entsprechen.

Wir ziehen die quadratischen Terme aus der Summe $\sum\limits_{r=1}^{2n}\sum\limits_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta)$ heraus, und erhalten

$$\sum_{r=1}^{2n}\sum_{i=1}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta) \;=\; \sum_{r=3}^{2n}\sum_{\substack{i=1\\ i\neq\frac{r}{2}}}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta) \;+\; \sum_{i=1}^{n} {x_i}^2\cos(2i\Theta)\ .$$

Wir subtrahieren $\sum\limits_{i=1}^{n} {x_i}^2\cos(2i\Theta)$ von $(*)$, und erhalten alle nicht-linearen und nicht-quadratischen Terme von B_n:

$$\sum_{r=3}^{2n}\sum_{\substack{i=1\\ i\neq\frac{r}{2}}}^{r-1} x_i x_{r-i}\cdot\cos(r\Theta) \;+\; 2\cdot\sum_{r=1}^{n}\sum_{i=1}^{n-r} x_i x_{r+i}\cdot\cos(r\Theta)\,. \qquad (**)$$

Gemischte Terme:
Wir suchen nun gemischte Terme der Form (IIIa) und (IIIb). Zunächst untersuchen wir das Vorkommen von Termen der Art (IIIa). Wir haben

$$\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot \cos((j-k)\Theta) \qquad \text{(IIIa)}\,.$$

Wir sehen, daß alle gemischten Koeffizienten $x_j x_k$, $j \neq k$, doppelt auftreten. Wir können diese nun zusammenfassen, und somit für (IIIa) schreiben:

$$2 \cdot \sum_{k=1}^{n-1} \sum_{j=1}^{n-k} x_j x_{k+j} \cdot \cos(k\Theta)\,.$$

Dies entspricht genau dem Term

$$2 \cdot \sum_{r=1}^{n} \sum_{i=1}^{n-r} x_i x_{r+i} \cdot \cos(r\Theta)\,,$$

denn es ist

$$\begin{aligned} 2 \cdot \sum_{r=1}^{n} \sum_{i=1}^{n-r} x_i x_{r+i} \cdot \cos(r\Theta) \quad &= \quad 2 \cdot \sum_{r=1}^{n-1} \sum_{i=1}^{n-r} x_i x_{r+i} \cdot \cos(r\Theta) \\ &\quad + \underbrace{\sum_{i=1}^{n-n} x_i x_{n+i} \cdot \cos(n\Theta)}_{=0}\,. \end{aligned}$$

Nun müssen wir noch zeigen, daß

$$\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot \cos((j+k)\Theta)$$

gleich

$$\sum_{r=3}^{2n} \sum_{\substack{i=1 \\ i \neq \frac{r}{2}}}^{r-1} x_i x_{r-i} \cdot \cos(r\Theta)$$

ist. Wir erinnern uns: der Sinn dieser Umsortierung besteht darin, daß der Faktor vor Θ in der Kosinus-Funktion nur von einem Index der Doppelsumme gebildet wird. Offensichtlich entspricht dieser Faktor in beiden Darstellungen der Summe der Indizes der Unbestimmten. Wir brauchen nun eine Möglichkeit, die gemischten Terme so zu ordnen, daß $j+k$ gleich einem Index r ist. Wir haben

$$\begin{matrix} j \in \{1, \dots, n\} \\ k \in \{1, \dots, n\} \end{matrix}\,, \qquad\qquad \text{mit } j \neq k\,.$$

Wir definieren

$$r := (j+k) \in \{2, \dots, 2n\} \;\text{ mit }\; x_r = 0 \;\text{ für }\; r \geq n+1\,,$$

und

$$i := k \in \{1, \dots, r-1\}\,.$$

Außerdem ist $k \neq \frac{j+k}{2}$ da $j \neq k$ für alle j und k gilt. Somit ist auch $i \neq \frac{r}{2}$. Zwischen den Indizes j, k und i, r besteht also folgender Zusammenhang:

$$(k, j) \;=\; (i, r-i).$$

Sei $s \in \{1, \ldots, n\}$. Man stelle sich ein Koordinatensystem aufgespannt von j und k beziehungsweise s und i vor. Die Paare (j,k) beziehungsweise (s,i) liegen dann in einem Gitter der Seitenlänge n. Die Doppelsumme

$$\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot \cos((j+k)\Theta)$$

zählt diese Punkte entlang der Parallelen zur k-Achse für $j = 1, \ldots, n$ von links nach rechts durch, dabei werden die Diagonalelemente weggelassen. Im Fall

$$\sum_{r=3}^{2n} \sum_{\substack{i=1 \\ i \neq \frac{r}{2}}}^{r-1} x_i x_{r-i} \cdot \cos(r\Theta)$$

werden die Punkte entlang der Geraden $s = r - i$ der Steigung -1 mit s-Achsenabschnitt r für $r = 3, \ldots, 2n$ von links oben nach rechts unten durchgezählt. Auch hier werden die Diagonalelemente weggelassen. Die Punkte, die auf diese Weise über das Gitter hinaus gezählt werden, nämlich (s,i) mit $s \geq n+1$ oder $i \geq n+1$, werden ausgelassen. Somit können wir schreiben

$$\sum_{j=1}^{n} \sum_{\substack{k=1 \\ k \neq j}}^{n} x_j x_k \cdot \cos((j+k)\Theta) \;=\; \sum_{r=3}^{2n} \sum_{\substack{i=1 \\ i \neq \frac{r}{2}}}^{r-1} x_i x_{r-i} \cdot \cos(r\Theta)\,.$$

Damit ist die Behauptung $A_n = B_n$ bewiesen. □

Zusammenfassung:

Wir können nun

$$\boxed{\tilde{f}(\Theta) \;=\; \frac{1}{c} \cdot \left(1 \;+\; 2 \cdot \sum_{j=1}^{n} x_j \cos(j\Theta) \right)^2} \;,$$

mit $x_j > 0$ für $j = 1, \ldots, n$, und $c = 1 + 2 \cdot \sum_{j=1}^{n} {x_j}^2$, endlich in der Form

$$\tilde{f}(\Theta) \;=\; 1 + 2 \cdot \sum_{r=1}^{m} c_r \cdot \cos(r\,\Theta)$$

schreiben:

$$\boxed{\begin{aligned} \tilde{f}(\Theta) \;&=\; 1 + 2 \cdot \tfrac{1}{c} \cdot \Bigg(\sum_{r=1}^{n} \Bigg(\Bigg(\sum_{i=0}^{r} x_i x_{r-i} \;+\; 2 \cdot \sum_{i=1}^{n-r} x_i x_{r+i} \Bigg) \cdot \cos(r\Theta) \Bigg) \\ &\qquad + \sum_{l=n+1}^{2n} \sum_{i=1}^{l-1} x_i x_{l-i} \cdot \cos(l\Theta) \Bigg) \end{aligned}} \;,$$

wobei $x_0 = 1$ und $x_{n+1} = x_{n+2} = \ldots = x_{2n} = 0$ ist. Die Koeffizienten c_r mit $r = 1, \ldots, m$, $m := 2n$, sind somit gegeben durch

$$\begin{aligned} c_r \;&=\; \frac{1}{c} \cdot \left(\sum_{i=0}^{r} x_i x_{r-i} \;+\; 2 \cdot \sum_{i=1}^{n-r} x_i x_{r+i} \right) \;, \text{ mit } r = 1, \ldots, n\,, \\ c_l \;&=\; \frac{1}{c} \cdot \sum_{i=1}^{l-1} x_i x_{l-i}\;, \text{ mit } l = n+1, \ldots, 2n\;. \end{aligned}$$

Man sieht an der Darstellung

$$\tilde{f}(\Theta) \;=\; \frac{1}{c}\cdot\left(1 \;+\; 2\cdot\sum_{j=1}^{n} x_j \cos{(j\Theta)}\right)^2$$

direkt, daß $\tilde{f}(\Theta) \geq 0$ ist für alle $\Theta \in \mathbb{R}$. Die Koeffizienten c_r, $r = 1, \ldots, 2n$, sind ebenfalls größer als 0, da sie aus den positiven x_j, $j = 1, \ldots, n$, gebildet werden. Also können wir Proposition (3.6) anwenden. Wir berechnen aus den Koeffizienten c_r, $r = 1, \ldots, 2n$, die Funktion Ψ, die ja gegeben ist durch

$$\Psi(t) \;=\; \sum_{r=1}^{m} c_r \cdot t^r \;,$$

wobei $t \in \mathbb{C}$ und $t \neq 0$ ist. Damit ist

$$\begin{aligned}\Psi(\sqrt{q}) \quad &= \quad \frac{1}{c}\cdot\left(\sum_{r=1}^{n}\left(\sum_{i=0}^{r} x_i x_{r-i} \;+\; 2\cdot\sum_{i=1}^{n-r} x_i x_{r+i}\right)\cdot(\sqrt{q})^r\right.\\ &\qquad\qquad \left. +\; \sum_{l=n+1}^{2n}\sum_{i=1}^{l-1} x_i x_{l-i}\cdot(\sqrt{q})^l\right)\end{aligned}$$

und

$$\begin{aligned}\Psi\left(\frac{1}{\sqrt{q}}\right) \quad &= \quad \frac{1}{c}\cdot\left(\sum_{r=1}^{n}\left(\sum_{i=0}^{r} x_i x_{r-i} + 2\cdot\sum_{i=1}^{n-r} x_i x_{r+i}\right)\cdot\left(\frac{1}{\sqrt{q}}\right)^r\right.\\ &\qquad\qquad \left. +\; \sum_{l=n+1}^{2n}\sum_{i=1}^{l-1} x_i x_{l-i}\cdot\left(\frac{1}{\sqrt{q}}\right)^l\right) .\end{aligned}$$

Wir erhalten

$$N_q(g) \;\leq\; \frac{g}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; \frac{\Psi(\sqrt{q})}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; 1 \;,$$

wobei Ψ von der Wahl der $x_1, \ldots, x_n$ abhängt. Die Funktion

$$M_{q,g}(x_1, \ldots, x_n) \;:=\; \frac{g}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; \frac{\Psi(\sqrt{q})}{\Psi\left(\frac{1}{\sqrt{q}}\right)} \;+\; 1$$

hängt von den Unbestimmten $x_1, \ldots, x_n$, deren Anzahl n, dem Geschlecht g und von dem gewählten q ab. Dabei ist

$$x = (x_1, \ldots, x_n) \in \mathbb{R}^n_{\geq 0} - \{0\} \;.$$

Setzen wir in $M_{q,g}(x_1, \ldots, x_n)$ für x_n die Null ein, so erhalten wir die Funktion $M_{q,g}(x_1, \ldots, x_{n-1})$. In $M_{q,g}(x_1, \ldots, x_n)$ sind also immer die Funktionen der Dimension kleiner als n enthalten.

Wir erhalten eine obere Schranke für $N_q(g)$, indem wir die Funktion $M_{q,g}(x_1, \ldots, x_n)$ für festes g und q minimieren. Im nächsten Kapitel betrachten wir Möglichkeiten zur Minimierung der Funktion für $q = 2$.

Kapitel 4

Minimierung von $M_{2,g}(x_1, \ldots, x_n)$

Wir definieren

$$M_g(x_1, \ldots, x_n) := \frac{g}{\Psi\left(\frac{1}{\sqrt{2}}\right)} + \frac{\Psi(\sqrt{2})}{\Psi\left(\frac{1}{\sqrt{2}}\right)} + 1\,,$$

mit $(x_1, \ldots, x_n) \in \mathbb{R}^n_{\geq 0} - \{0\}$. Diese Funktion $M_g(x_1, \ldots, x_n)$ wollen wir für fest gewählte g's minimieren. Dabei sollten wir noch folgendes beachten: egal wo wir die Funktion M_g auswerten, wir erhalten immer eine obere Schranke für $N_2(g)$. Ob wir nun ein lokales oder das globale Minimum finden, dieses liefert uns auf jeden Fall eine obere Abschätzung.
Es tauchen verschiedene Fragen auf: Wie groß muß die Anzahl der Variablen n für ein bestimmtes Geschlecht gewählt werden? Wie verhalten sich die Funktionen $M_g(x_1)$, $M_g(x_1, x_2)$, $M_g(x_1, x_2, x_3), \ldots, M_g(x_1, \ldots, x_n)$ für $(x_1, \ldots, x_n) \in \mathbb{R}^n_{\geq 0} - \{0\}$?
Um dies zu beantworten, untersuchen wir diese Funktionen zunächst mit Hilfe der Differentialrechnung.

4.1 Anwendung der Differentialrechnung

Wir untersuchen zuerst die einfachste Funktion $M_g(x_1)$ mit $x_1 > 0$. Zunächst schreiben wir die Funktion explizit auf, indem wir die Koeffizienten c_1 und c_2 mit der auf Seite 39 angegebenen Formel ausrechnen, und damit $\Psi(\sqrt{2})$ und $\Psi\left(\frac{1}{\sqrt{2}}\right)$ bestimmen. Wir erhalten

$$\begin{aligned} c_1 &= \frac{2x_1}{1+2{x_1}^2}\,, \\ c_2 &= \frac{{x_1}^2}{1+2{x_1}^2}\,. \end{aligned}$$

Dann ist

$$\begin{aligned} \Psi\left(\sqrt{2}\right) &= \frac{2\sqrt{2}x_1 + 2{x_1}^2}{1+2{x_1}^2}\,, \\ \Psi\left(\frac{1}{\sqrt{2}}\right) &= \frac{2\sqrt{2}x_1 + {x_1}^2}{2+4{x_1}^2}\,. \end{aligned}$$

Damit hat $M_g(x_1)$ folgende Gestalt:

$$\begin{aligned} M_g(x_1) &= \frac{2+4{x_1}^2}{2\sqrt{2}x_1+{x_1}^2}\cdot g+\frac{4\sqrt{2}x_1+4{x_1}^2}{2\sqrt{2}x_1+{x_1}^2}+1 \\ &= \frac{2g+4g{x_1}^2+4\sqrt{2}x_1+4{x_1}^2}{2\sqrt{2}x_1+{x_1}^2}+1\,. \end{aligned}$$

Zur Bestimmung der Extrema von $M_g(x_1)$ leiten wir die Funktion ab.

$$M_g{}'(x_1) = \frac{(8\sqrt{2}g+4\sqrt{2}){x_1}^2-4gx_1-4\sqrt{2}g}{(2\sqrt{2}x_1+{x_1}^2)^2}\,.$$

Wir bestimmen die Nullstellen der ersten Ableitung und erhalten

$$\widetilde{x_1},\widetilde{\widetilde{x_1}} = \frac{g}{4\sqrt{2}g+2\sqrt{2}} \pm \sqrt{\left(\frac{g}{4\sqrt{2}g+2\sqrt{2}}\right)^2+\frac{g}{2g+1}}\,.$$

Da $x_1 > 0$ vorgegeben ist, betrachten wir nur die Lösung $\widetilde{x_1}$. Diese kann als eine Funktion in g interpretiert werden.

$$\widetilde{x_1}(g) := \frac{g}{4\sqrt{2}g+2\sqrt{2}} + \sqrt{\left(\frac{g}{4\sqrt{2}g+2\sqrt{2}}\right)^2+\frac{g}{2g+1}}\,.$$

Bemerkung: Der Fall $g = 0$ ist ein Sonderfall, den wir hier nicht betrachten.

Lemma 4.1 *Für alle $g > 0$ gilt $0 < \widetilde{x_1}(g) < 1$.*

Beweis: Da $g > 0$ ist, ist auch $\widetilde{x_1}(g)$ größer als Null.
Die erste Ableitung von $\widetilde{x_1}$ hat folgende Gestalt:

$$\widetilde{x_1}'(g) = \frac{1}{2\sqrt{2}}\cdot\left(\frac{1}{(2g+1)^2}+\frac{9g+4}{\sqrt{\frac{g(17g+8)}{(2g+1)^2}}(2g+1)^3}\right)\,.$$

Man sieht sofort, daß $\widetilde{x_1}'(g) > 0$ ist für alle $g > 0$. Damit ist die Funktion $\widetilde{x_1}(g)$ monoton wachsend.
Wir untersuchen noch das Verhalten der Funktion $\widetilde{x_1}(g)$ für große g:

$$\begin{aligned} \lim_{g\to\infty}\widetilde{x_1}(g) &= \lim_{g\to\infty}\left(\frac{g}{4\sqrt{2}g+2\sqrt{2}}+\sqrt{\left(\frac{g}{4\sqrt{2}g+2\sqrt{2}}\right)^2+\frac{g}{2g+1}}\right) \\ &= \frac{1}{4\sqrt{2}}+\sqrt{\left(\frac{1}{4\sqrt{2}}\right)^2+\frac{1}{2}} \\ &= \frac{1+\sqrt{17}}{4\sqrt{2}} \\ &\approx 0.905645\,. \end{aligned}$$

Damit ist $\widetilde{x_1}(g) < 1$ für alle $g > 0$. □

Satz 4.2 *Es sei $g > 0$. Es gilt: An der Stelle $\widetilde{x_1}$ hat die Funktion $M_g(x_1)$ ein Minimum.*

Beweis: Die zweite Ableitung von $M_g(x_1)$ lautet

$$M_g''(x_1) \;=\; \frac{-(16\sqrt{2}g+8\sqrt{2})x_1{}^3+12gx_1{}^2+24\sqrt{2}gx_1+32g}{(2\sqrt{2}x_1+x_1{}^2)^3}\,.$$

Ist $M_g''(\widetilde{x_1})$ größer als Null, so liegt ein Minimum vor. Wir müssen also zeigen, daß

$$12g\widetilde{x_1}^2+24\sqrt{2}g\widetilde{x_1}+32g>(16\sqrt{2}g+8\sqrt{2})\widetilde{x_1}^3 \qquad (*)$$

ist. Wir betrachten zuerst den Fall $g=1$. Es ist

$$\widetilde{x_1}(1) \;=\; \frac{1}{\sqrt{2}}\,.$$

Einsetzen in $(*)$ mit $g=1$ liefert

$$12\cdot\frac{1}{2}+24\sqrt{2}\cdot\frac{1}{\sqrt{2}}+32>(16\sqrt{2}+8\sqrt{2})\cdot\left(\frac{1}{\sqrt{2}}\right)^3.$$

Vereinfacht ergibt sich

$$62>12\,.$$

Die Ungleichung gilt also für $g=1$.
Nun untersuchen wir den Fall $g>1$. Da $\widetilde{x_1}$ größer als Null ist für alle g, können wir schreiben

$$12g\widetilde{x_1}^2+24\sqrt{2}g\widetilde{x_1}+32g>32g\,.$$

Weiterhin gilt nach Lemma (4.1), daß $\widetilde{x_1}<1$ ist für alle g. Deshalb ist

$$16\sqrt{2}g+8\sqrt{2}>(16\sqrt{2}g+8\sqrt{2})\widetilde{x_1}^3\,.$$

Die Ungleichung

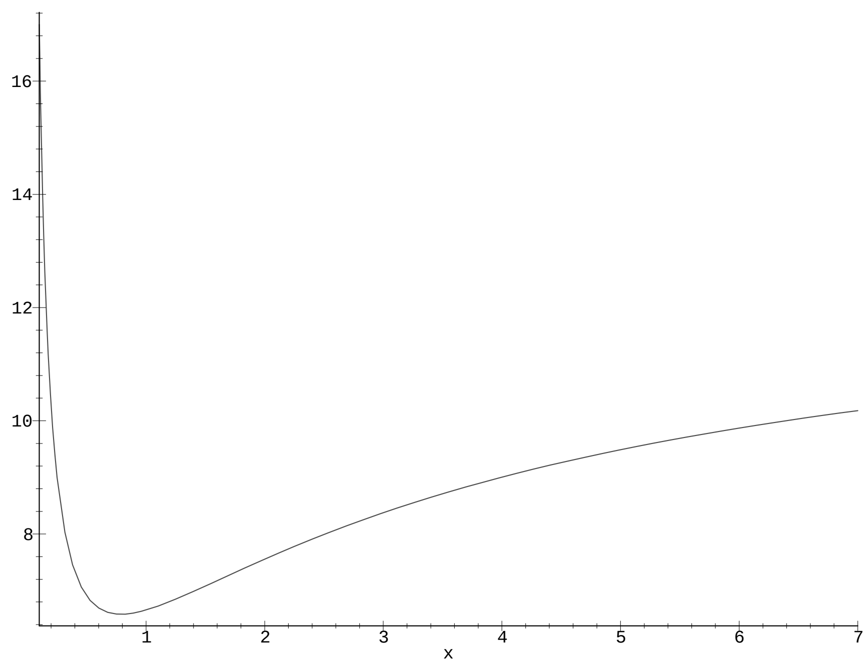
$$32g>16\sqrt{2}g+8\sqrt{2}$$

ist erfüllt für $g>1$. Somit ist $M_g''(\widetilde{x_1})>0$ für $g\geq 1$. Also liegt in $\widetilde{x_1}$ ein Minimum der Funktion $M_g(x_1)$ für alle $g>0$ vor. □

In der folgenden Tabelle sind die Minima der Funktion $M_g(x_1)$ für einige g's aufgeführt.

g	$\widetilde{x_1}$	$M_g(\widetilde{x_1})$
1	$\frac{1}{\sqrt{2}} \approx 0.707106$	5.000000
2	$\frac{1}{5\sqrt{2}}(1+\sqrt{21}) \approx 0.789494$	6.582576
3	0.823243	8.152068
4	0.842069	9.717798
5	0.853794	11.281929
6	0.861867	12.845233
20	0.891873	34.713307
30	0.896400	50.329768
50	0.900066	81.561576
100	0.902844	159.639783
1000	0.905364	1565.037827
5000	0.905589	7811.249124

Wir geben den Graphen der Funktion $M_g(x_1)$ für $g = 2$ an:



Das Minimum liegt an der Stelle $\widetilde{x_1} = 0.789494$ vor.

Als nächstes untersuchen wir die Funktion $M_g(x_1, x_2)$. Wir konstruieren die Funktion aus den Koeffizienten $c_1, \ldots, c_4$, die wir nach der Formel auf Seite 39 berechnen: Wir erhalten

$$\begin{aligned} c_1 &= \frac{2x_1 + 2x_1x_2}{1 + 2{x_1}^2 + 2{x_2}^2}, \\ c_2 &= \frac{2x_2 + {x_1}^2}{1 + 2{x_1}^2 + 2{x_2}^2}, \\ c_3 &= \frac{2x_1x_2}{1 + 2{x_1}^2 + 2{x_2}^2}, \\ c_4 &= \frac{{x_2}^2}{1 + 2{x_1}^2 + 2{x_2}^2}. \end{aligned}$$

Daraus ergibt sich

$$\begin{aligned} \Psi\left(\sqrt{2}\right) &= \frac{2\sqrt{2}x_1 + 2\sqrt{2}x_1x_2 + 4x_2 + 2{x_1}^2 + 4\sqrt{2}x_1x_2 + 4{x_2}^2}{1 + 2{x_1}^2 + 2{x_2}^2}, \\ \Psi\left(\frac{1}{\sqrt{2}}\right) &= \frac{4\sqrt{2}x_1 + 4\sqrt{2}x_1x_2 + 4x_2 + 2{x_1}^2 + 2\sqrt{2}x_1x_2 + {x_2}^2}{4(1 + 2{x_1}^2 + 2{x_2}^2)}. \end{aligned}$$

Insgesamt hat $M_g(x_1, x_2)$ die Form

$$\begin{aligned} M_g(x_1, x_2) &= \frac{4(1 + 2{x_1}^2 + 2{x_2}^2)}{4\sqrt{2}x_1 + 6\sqrt{2}x_1x_2 + 4x_2 + 2{x_1}^2 + {x_2}^2} \cdot g \\ &\quad + \frac{8\sqrt{2}x_1 + 24\sqrt{2}x_1x_2 + 16x_2 + 8{x_1}^2 + 16{x_2}^2}{4\sqrt{2}x_1 + 6\sqrt{2}x_1x_2 + 4x_2 + 2{x_1}^2 + {x_2}^2} + 1\,. \end{aligned}$$

Wir suchen das Minimum der Funktion $M_g(x_1, x_2)$ mit Hilfe des Computeralgebrasystems Maple. Zuerst berechnen wir die partiellen Ableitungen $\frac{\partial}{\partial x_1} M_g(x_1, x_2)$ und $\frac{\partial}{\partial x_2} M_g(x_1, x_2)$. Wir wählen ein festes g. Dann bestimmen wir die Lösungen des Gleichungssystems

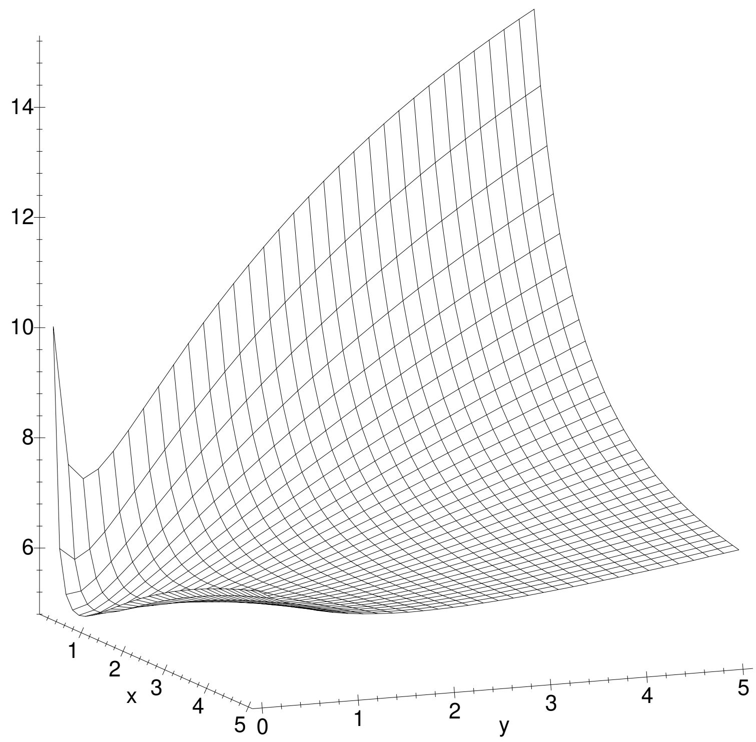
$$\begin{aligned} \frac{\partial}{\partial x_1} M_g(x_1, x_2) &= 0 \\ \frac{\partial}{\partial x_2} M_g(x_1, x_2) &= 0\,. \end{aligned}$$

Wir erhalten genau eine Lösung für $(x_1, x_2) \in \mathbb{R}^2_{\geq 0} - \{0\}$. An dieser Stelle liegt das Minimum der Funktion $M_g(x_1, x_2)$. Ein Beispiel für die Bestimmung des Minimums mit Maple ist im Anhang beigefügt. Auf diese Weise gehen wir auch bei den Funktionen $M_g(x_1, x_2, x_3)$, $M_g(x_1, \ldots, x_4)$ und $M_g(x_1, \ldots, x_5)$ vor.

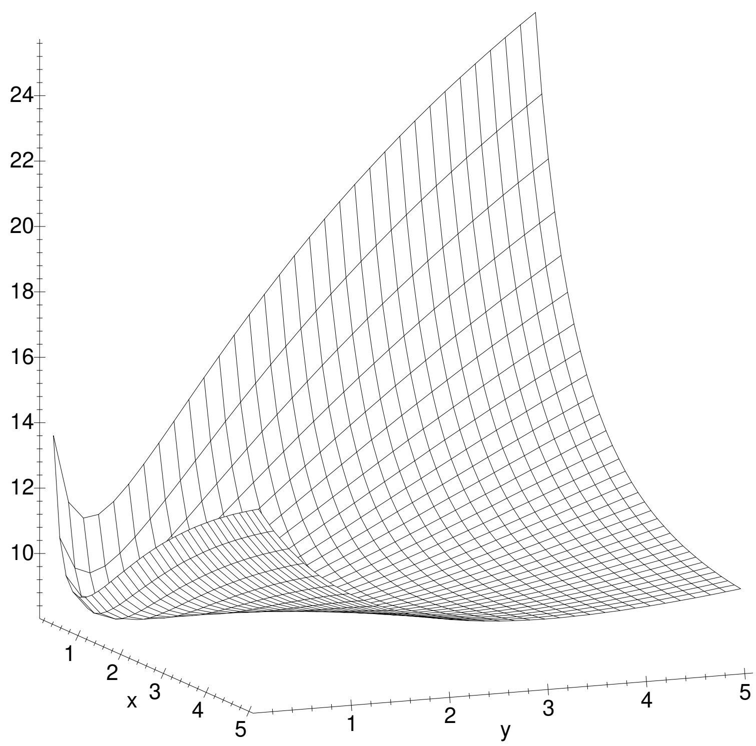
Mit Hilfe von Maple erhalten wir folgende Minima der Funktion $M_g(x_1, x_2)$ für fest gewählte g's:

g	$\widetilde{x} = (\widetilde{x_1}, \widetilde{x_2})$	$M_g(\widetilde{x})$
1	(0.707106 , 0)	5.000000
2	(0.792538 , 0.256232)	6.276905
3	(0.831845 , 0.383932)	7.337431
4	(0.855048 , 0.462196)	8.339441
5	(0.870444 , 0.515346)	9.316462
6	(0.881439 , 0.553870)	10.280404
20	(0.925626 , 0.713567)	23.482117
30	(0.932814 , 0.740286)	32.852398
50	(0.938752 , 0.762513)	51.573987
100	(0.943321 , 0.779711)	98.355418
500	(0.947051 , 0.793810)	472.536271
1000	(0.947516 , 0.795594)	940.253431

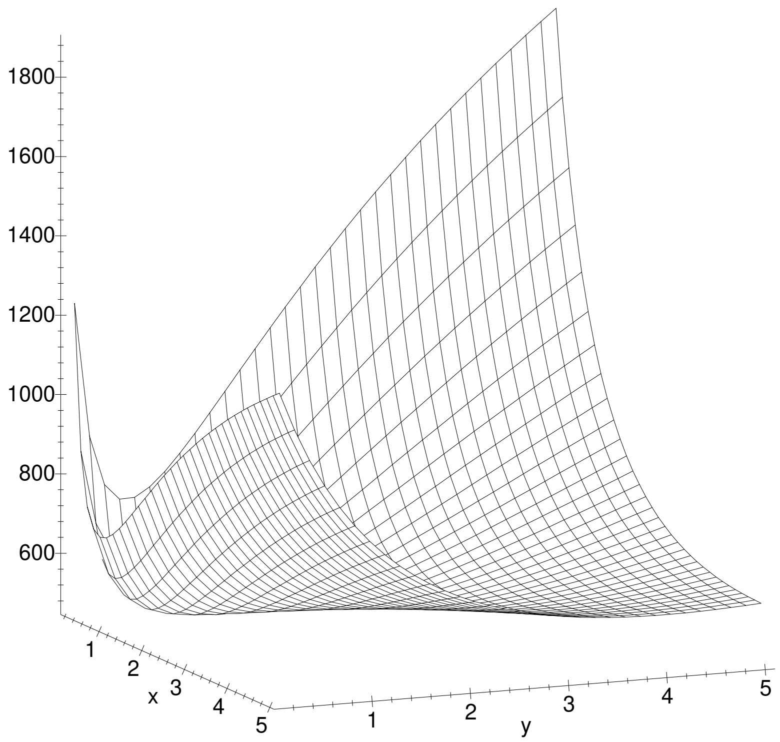
Wir vergleichen die Minima, die die Funktionen $M_g(x_1)$ und $M_g(x_1, x_2)$ bezüglich der einzelnen g's besitzen. Es gibt eine Übereinstimmung zwischen dem Minimum von $M_1(x_1)$ und demjenigen von $M_1(x_1, x_2)$ (unten ist der Graph von $M_1(x_1, x_2)$ angegeben). Außerdem sehen wir, daß die Funktion $M_g(x_1, x_2)$, bis auf den Wert für $g = 1$, ausschließlich bessere Ergebnisse als $M_g(x_1)$ liefert. Je größer das Geschlecht ist, umso größer ist die Differenz zwischen den entsprechenden Minima von $M_g(x_1)$ und $M_g(x_1, x_2)$. Weiter ist zu beobachten, daß auch bei $M_g(x_1, x_2)$ die Koordinaten der Minimumstellen $\widetilde{x_1}, \widetilde{x_2}$ für alle g's kleiner als Eins sind. Zusätzlich ist für alle g $\widetilde{x_1} > \widetilde{x_2}$.



Graph von $M_1(x_1, x_2)$. Das Minimum wird an der Stelle $\widetilde{x} = (0.707106\ ,\ 0)$ angenommen.



Graph von $M_4(x_1, x_2)$. Wir erhalten für $\widetilde{x} = (0.855048\ ,\ 0.462196)$ ein Minimum.



Graph von $M_{500}(x_1, x_2)$. An der Stelle $\widetilde{x} = (0.947051\ ,\ 0.793810)$ liegt das Minimum der Funktion.

Anhand der Tabelle der Funktion $M_g(x_1, x_2)$ erkennen wir: je kleiner das g ist, desto kleiner ist der Wert von $\widetilde{x_2}$. Dies sieht man auch an den Graphen für $g = 1$, $g = 4$ und $g = 500$: das Minimum für kleine g's liegt näher bei der x_1-Achse. Für $g = 1$ ist $\widetilde{x_2}$ gleich Null, es genügt also für $g = 1$ die Dimension von M_g um Eins kleiner zu wählen.
Aufgrund der folgenden Betrachtungen sehen wir, daß dies auch in höheren Dimensionen von M_g auftritt. Zum Beispiel liefert die Funktion $M_g(x_1, x_2, x_3)$ für $g = 1, \ldots, 4$ die selben Minima wie die Funktion $M_g(x_1, x_2)$. Ab $g = 5$ erhalten wir andere Ergebnisse, die aber ohne Ausnahme besser als die von $M_g(x_1, x_2)$ sind:

g	$\widetilde{x} = (\widetilde{x_1}, \widetilde{x_2}, \widetilde{x_3})$	$M_g(\widetilde{x})$
5	(0.870481 , 0.515475 , 0.026941)	9.312546
6	(0.881910 , 0.555531 , 0.097947)	10.225756
20	(0.934166 , 0.745334 , 0.453867)	21.169526
30	(0.943898 , 0.781887 , 0.532147)	28.599796
50	(0.952263 , 0.813610 , 0.597279)	43.331080
100	(0.958915 , 0.839038 , 0.650218)	80.002874
1000	(0.965207 , 0.863251 , 0.701227)	738.912147

Die Minima für $g = 1, \ldots, 14$ der Funktion $M_g(x_1, \ldots, x_4)$ sind die selben wie die der Funktion $M_g(x_1, x_2, x_3)$. Die nächste Tabelle gibt einige Werte für $g > 14$ an.

g	$\widetilde{x} = (\widetilde{x_1}, \ldots, \widetilde{x_4})$	$M_g(\widetilde{x})$
20	(0.934665 , 0.747198 , 0.462095 , 0.116610)	21.039894
30	(0.945869 , 0.789337 , 0.547351 , 0.246108)	27.884882
50	(0.956383 , 0.829338 , 0.629947 , 0.375603)	40.995155
100	(0.965399 , 0.863994 , 0.702800 , 0.492972)	73.023661
1000	(0.974522 , 0.899389 , 0.778428 , 0.617802)	643.575851

Setzt man $g = 1, \ldots, 37$, so erhält man für $M_g(x_1, \ldots, x_5)$ die selben Minimumstellen wie für $M_g(x_1, \ldots, x_4)$. Deshalb geben wir in der folgenden Tabelle Werte für $g > 37$ an.

g	$\widetilde{x} = (\widetilde{x_1}, \ldots, \widetilde{x_5})$	$M_g(\widetilde{x})$
50	(0.956629 , 0.830279 , 0.631911 , 0.378729 , 0.092696)	40.858029
100	(0.967292 , 0.871309 , 0.718329 , 0.518360 , 0.284482)	71.052349
1000	(0.979909 , 0.920445 , 0.823997 , 0.694440 , 0.536979)	591.414981

Zusammenfassung: Wir können aufgrund unserer Beobachtungen der Funktionen $M_g(x_1), \ldots, M_g(x_1, \ldots, x_5)$ folgende Vermutungen anstellen:

- Jede Funktion $M_g(x_1, \ldots, x_n)$, mit fest gewähltem g und bestimmter Dimension n, hat genau ein Minimum.
- Die Koordinaten $\widetilde{x_1}, \ldots, \widetilde{x_n}$ der Minimumstellen sind immer kleiner als Eins. Zusätzlich ist sogar $\widetilde{x_1} > \widetilde{x_2} > \ldots > \widetilde{x_n}$ in allen Funktionen erfüllt.
- Für jedes g gibt es eine Funktion $M_g(x_1, \ldots, x_n)$ mit einer für dieses g optimalen Dimension n. Das heißt: wählt man eine Funktion, deren Vektorlänge von x kleiner als n ist, so ist das Minimum dieser Funktion immer schlechter als das der Funktion mit n Variablen. Wählt man umgekehrt eine Funktion mit mehr als n Variablen, so liefert diese keinen besseren Wert, sondern sie hat das selbe Minimum. Zum Beispiel ist für $g = 20$ die Vektorlänge $n = 4$ optimal:

n	$M_{20}(\widetilde{x})$
1	34.713307
2	23.482117
3	21.169526
4	21.039894
5	21.039894

- Die optimalen Vektorlängen einiger g's bis $n = 5$ sind in folgender Tabelle aufgeführt:

g	n
1	1
$2, 3, 4$	2
$5, \ldots, 14$	3
$15, \ldots, 37$	4
$38, \ldots, 91$	5

Wir können demzufolge annehmen: je größer das Geschlecht gewählt ist, umso komplexer muß die optimale Funktion $M_g(x)$ sein. Wählen wir eine Vektorlänge, die kleiner als die optimale Länge n ist, so gilt: je größer der Abstand zu n ist, umso weiter ist das Minimum vom optimalen Wert entfernt. Außerdem erkennen wir, daß die Dimension n viel langsamer wächst als g.

4.2 Entwurf eines Computerprogramms

Wenn wir nun solche Minima für große g's bestimmen wollen, müssen wir Funktionen mit entsprechend großer optimaler Dimension benutzen. Die Methode der Differentialrechnung mit Maple stößt dort an ihre Grenzen. Mit Maple kann man die Minima von Funkionen M_g auf die auf Seite 45 beschriebene Weise bis zur Dimension $n = 9$ berechnen. Für $n > 9$ ist die Funktion 'fsolve', welche Gleichungssysteme numerisch löst, überfordert. Deshalb gehen wir anders vor. Wir nehmen den vorangegangenen Betrachtungen zufolge an, daß die Koordinaten der Minimumstellen aller Funktionen zwischen Null und Eins liegen. Daher suchen wir das Minimum von $M_g(x_1, \ldots, x_n)$ durch Auswertung dieser Funktion an Punkten im Bereich $[0\,,\,1]^n - \{0\}$ mit Hilfe eines Computerprogramms. Dazu betrachten wir zunächst folgendes Testprogramm:

Testprogramm: Wir setzen die Dimension $n = 5$. Das Programm durchläuft alle Punkte $(x_1, \ldots, x_5) \in [0\,,\,1]^5 - \{0\}$ mit der Eigenschaft $x_1 > x_2 > \ldots > x_5$ in 0.01-er Schritten. Die Funktion $M_g(x_1, \ldots, x_5)$ wird an jedem dieser Punkte für $g = 1$ bis $g = 100$ ausgewertet. Dabei wird der jeweils kleinste Wert mit dem entsprechenden Punkt gespeichert.
Wir vergleichen einige Werte, die das Programm ausgegeben hat, mit den mit Maple berechneten Werten:

g	Wert des Testprogramms	n	$M_g(\widetilde{x})$
4	$8.3394\underline{86}$	2	$8.3394\underline{41}$
5	$9.312\underline{674}$	3	$9.312\underline{546}$
10	$13.537\underline{427}$	3	$13.537\underline{320}$
15	$17.401\underline{290}$	4	$17.401\underline{114}$
20	$21.0\underline{40184}$	4	$21.0\underline{39894}$
60	$47.055\underline{348}$	5	$47.055\underline{129}$
90	$65.12\underline{4117}$	5	$65.12\underline{3870}$

Diejenigen Dezimalstellen, in denen sich die Werte unterscheiden, sind unterstrichen.

Diskussion der Ergebnisse:

- Aus der Tabelle ersehen wir, daß die Unterteilung des Bereiches $[0\,,\,1]^5 - \{0\}$ in 0.01-er Schritte schon sehr genau ist. Wir interessieren uns ja nur für den ganzzahligen Anteil der Werte. Deshalb empfiehlt es sich, eine Steuerung für die erforderliche Genauigkeit einzuführen. Das heißt, es soll nur dann genauer gerechnet werden, falls eine Chance für die Verbesserung des ganzzahligen Anteils besteht.

- Wir vergleichen die Minimumstelle der jeweiligen Funktion $M_g(x)$ mit dem von dem Testprogramm ermittelten Punkt, der zu dem kleinsten Wert für dieses g führt. Wie erwartet, stimmt die Dimension n der jeweiligen Funktion $M_g(x)$ mit der Anzahl der Koordinaten des Punktes, welche ungleich Null sind, überein.
  Zum Beispiel haben wir für $g = 10$:

Differentialrechnung	Testprogramm
$\widetilde{x} = (0.908898\,,\ 0.652191\,,\ 0.276653)$	$x = (0.91\,,\ 0.65\,,\ 0.28\,,\ 0\,,\ 0)$

  Wir haben also im Testprogramm für viele g's in einer höheren Dimension als der jeweiligen optimalen gerechnet. Sinnvoller wäre es, die optimale Dimension eines g's zu finden und dann abzubrechen, also eine Steuerung der Dimension in das Programm einzubauen. Erhöhen wir für ein festes g schrittweise die Dimension der Funktion $M_g(x)$ und vergleichen die Minima, so wird die Differenz zwischen diesen Werten immer kleiner, je näher wir der optimalen Dimension für dieses g kommen. Siehe zum Beispiel auf Seite 50 die Tabelle für $g = 20$. Wir können also sukzessive die Dimensionen durchprobieren. Wir testen dann jedesmal die Differenz zwischen dem Minimum der aktuellen Dimension und der Dimension davor. Ist die Differenz kleiner als eine bestimmte Schranke, so brechen wir ab.

- In dem Testprogramm wird die Funktion M_g an allen Punkten des 5-dimensionalen Gitters ausgewertet. Da wir annehmen, daß M_g nur ein Minimum besitzt, liegt es nahe, dieses etwas systematischer aufzuspüren. Wir können das Gebiet, in dem sich das Minimum befindet, auf folgende Weise eingrenzen: im ersten Schritt durchlaufen wir den Bereich $[0\,,1]^n - \{0\}$ in 0.25-er Schritten und werten die Funktion M_g an diesen $5^n - 1$ Punkten aus. Wir speichern die 2^n besten Werte mit ihren zugehörigen Vektoren. Dann überprüfen wir, ob die Differenz zwischen dem schlechtesten und dem besten Wert kleiner als eine gewisse Schranke ist. Ist dies der Fall, so liegen die Werte genügend dicht beeinander. Dann speichern wir den besten Wert. Ist die Differenz größer als die Schranke, so legen wir um die 2^n Punkte ein neues Gitter. Die Anzahl der Punkte entspricht genau der Anzahl der Ecken des Gitters. Bei der Konstruktion des neuen Gitters lassen wir noch einen gewissen Abstand zwischen dem Gitterrand und den äußeren der 2^n Punkte zu. Dann verfeinern wir das Raster, indem wir die Schrittweite halbieren. Dieses neue Gitter ist nun unser Ausgangsgitter, in dem wir wieder die 2^n besten Werte suchen, usw.. Da es nur ein Minimum für jede Funktion M_g gibt, laufen wir nicht Gefahr, in der falschen Ecke des Gitters zu landen und nur ein lokales Minimum zu finden.

Unser Ziel ist es nun, ein Programm zu erarbeiten, das bei Eingabe von g möglichst effektiv eine kleinste obere Schranke findet, und die oben gemachten Überlegungen berücksichtigt. Wir betrachten folgende Möglichkeit:

Programm:
g bekommt einen Wert zugewiesen.
Die Genauigkeitsschranke $FINE$ wird zunächst auf 1 gesetzt.
Die Vektorlänge n erhält den Wert 2 .

- Die $FINE$-Schleife.
  Dies ist die äußerste Schleife, sie steuert die erforderliche Genauigkeit. Wir beginnen mit $FINE = FINE * 0.1$, im ersten Durchlauf hat $FINE$ also den Wert 0.1 .
  - Die $LONG$-Schleife.
    Sie steuert die Vektorlänge. Hier wird $n = n+1$ gesetzt. Die Vektorlänge n ist im ersten Durchlauf gleich 3. Die Schranke $LONG$ erhält den Wert 0.1 .
    * Die Funktion $Minimierung$.
      Beim ersten Aufruf wird die Funktion $M_g(x_1 \ldots, x_n)$ für das jeweilige n zunächst an allen Gitterpunkten aus dem Bereich $[0\,,\,1]^n - \{0\}$ mit der Schrittweite $sw = 0.25$ (das sind $5^n - 1$ Punkte) ausgewertet. Dabei werden die 100 besten Werte mit ihren Gitterpunkten bestimmt.
      · Ist die Differenz zwischen dem größten und dem kleinsten dieser 100 Werte größer als $FINE$, so wird ein neues Gitter gleicher Dimension um die 100 Punkte gelegt. Das Gitter wird so erzeugt, daß keiner dieser 100 Punkte auf dem Rand des Gitters liegt, sondern ein Abstand von mindestens sw zum Rand besteht. Dann wird die Schrittweite halbiert. Wir gehen wieder zum Anfang der Funktion $Minimierung$, wo die 100 besten Werte dieses neuen verfeinerten Gitters bestimmt werden.
      · Liegen die Werte sehr dicht beeinander, d. h. ist nun die Differenz zwischen dem größten und dem kleinsten Wert kleiner als $FINE$, so gibt die Funktion den kleinsten Wert als besten Wert bei dieser Vektorlänge an das Hauptprogramm zurück.
  - ($LONG$) Von der Funktion $Minimierung$ erhalten wir den kleinsten Wert für die vorgegebene Vektorlänge. Diesen vergleichen wir nach dem ersten Durchlauf mit dem Wert, den die Weil-Schranke (3.2) liefert. Bei allen weiteren Durchläufen wird getestet, ob die Differenz zwischen dem Wert für $n-1$ und dem Wert für n noch größer als $LONG$ ist. Ist dies nicht mehr der Fall, so verlassen wir die $LONG$-Schleife.
- ($FINE$) Hier wird nun getestet, ob der ganzzahlige Anteil des von der $LONG$-Schleife zurückgegebenen Wertes noch verbessert werden kann. Falls bei der Genauigkeit $FINE$ der Nachkommateil des Wertes kleiner als $2 * FINE$ ist, gehen wir wieder zum Anfang der Schleife, wo wieder mit $n = 2$ begonnen wird. Dort wird $FINE = FINE * 0.1$ gesetzt. Beim zweiten Durchlauf hat $FINE$ den Wert 0.01 . Ist $FINE = 10^{-7}$, so brechen wir ab.

Bemerkung zur $LONG$-Schranke: Es erwies sich nach einigen Testläufen als sinnvoll, für $LONG$ den Wert 0.1 zu wählen. Bei der Wahl einer kleineren Schranke rechnet der Computer über die für das jeweilige g optimale Dimension hinaus. Dort berechnet er das selbe Minimum wie bei der Dimension vorher, und erhält dann als Differenz die Null. Dieser Überlauf ist unnötig und kostet, vor allem bei größeren g's, viel Rechenzeit.

Bemerkung zur Anzahl der gespeicherten Punkte: Ursprünglich wurden 2^n Punkte gespeichert, was genau der Anzahl der Ecken eines n-dimensionalen Gitters entspricht. Da dies sich als zu zeitaufwendig erwies, wurde getestet, ob eine Speicherung von 100 Werten genügt. Wir nehmen ja an, daß die Funktion M_g für jedes g nur ein Minimum im positiven Bereich hat. Es zeigte sich, daß man mit 100 Werten schneller genau die selben Minima bekommt.

Einzelheiten der Funktionsweise des Programms sind im Progamm selbst, welches sich im Anhang befindet, an entsprechender Stelle dokumentiert. Weiter findet man im Anhang Tabellen für die Werte $g = 1$ bis $g = 600$ und für größere Werte bis $g = 10000$.

Wir vergleichen die von dem Programm errechneten Minima mit den Ergebnissen von Maple:

g	Wert des Programms	n	$M_g(\tilde{x})$
4	$8.3394\underline{62}$	2	$8.3394\underline{41}$
5	$9.312\underline{637}$	3	$9.312\underline{546}$
10	$13.5373\underline{95}$	3	$13.5373\underline{20}$
15	$17.4011\underline{95}$	4	$17.4011\underline{14}$
20	$21.039\underline{974}$	4	$21.039\underline{894}$
60	$47.0551\underline{96}$	5	$47.0551\underline{29}$
90	$65.123\underline{973}$	5	$65.123\underline{870}$

Diejenigen Dezimalstellen, in denen sich die Werte unterscheiden, sind unterstrichen.

Wir sehen, daß die vom Programm gelieferten Werte sehr nahe bei den von Maple berechneten Minima liegen.

Nun führen wir noch folgende Bezeichnung ein:

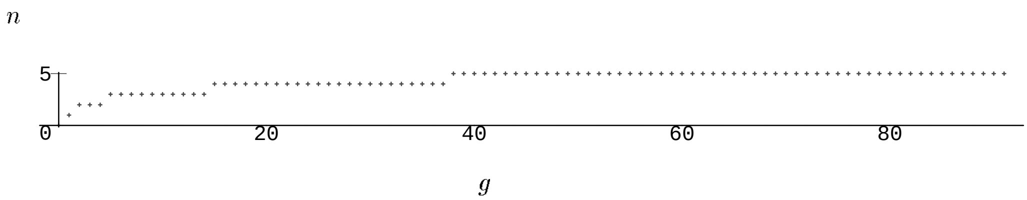
Definition 4.3 Seien g und q fest gewählt. Den ganzzahligen Anteil des von dem oben beschriebenen Programm berechneten Minimums der Funktion M_g bezeichnen wir mit

$$\mathcal{M}_q(g) \, .$$

Wir geben einige Minima für größere g's an:

g	$\mathcal{M}_q(g)$	n
100	71	6
200	127	6
400	235	7
500	287	8
700	390	8
1000	543	9
2000	1038	9
4000	2006	10
7000	3430	11
10000	4839	12

Im nächsten Schaubild ist das Geschlecht g gegen die von dem Programm benötigte Variablenzahl n aufgetragen. Man erkennt leicht, daß n sich ungefähr wie $\log(g)$ verhält.



Mit Hilfe des Programms können wir noch die Frage untersuchen, wie sich die Werte $\mathcal{M}_q(g)$ für wachsendes g verhalten.

Unter Benutzung der Serre-Methode zur Abschätzung von $N_q(g)$, vergleiche Proposition (3.6) auf Seite 31, kann man eine asymptotische Schranke für $N_q(g)$ beweisen.

Definition 4.4 Wir definieren

$$A(q) := \lim\sup_{g \longrightarrow \infty} \frac{N_q(g)}{g} .$$

Eine obere Schranke für $A(q)$ liefert dann der folgende Satz:

Satz 4.5 (Drinfeld-Vladut-Schranke).

$$A(q) \leq \sqrt{q} - 1 .$$

Beweis: [Sti93, KapV, S.184].

Man vermutet, daß sogar $A(q) = \sqrt{q} - 1$ gilt. In unserem Fall hieße das $\mathrm{A}(2) = \sqrt{2} - 1 \approx 0.4142$.

Da der oben zitierte Beweis mit Hilfe der Methode der expliziten Formeln durchgeführt wird, können wir annehmen, daß die asymptotische Schranke $A(2)$ für die Werte die unser Programm liefert, ebenfalls erfüllt ist. Wir betrachten das Verhältnis $\frac{\mathcal{M}_q(g)}{g}$ für einige g's:

g	$\frac{\mathcal{M}_q(g)}{g}$
10	1.3
100	0.71
1000	0.543
10000	0.4839

Die von dem Programm berechneten Ergebnisse deuten darauf hin, daß wir für größere g's die asymptotische Schranke $A(2)$ erreichen.

Wir haben nun ein Programm entworfen, das es uns erlaubt, obere Schranken für die Anzahl der rationalen Punkte von Kurven mit sehr großem Geschlecht zu bestimmen. Die Tabellen dazu befinden sich im Anhang.

Symbolverzeichnis

$\mathbf{A}^n$	n-dimensionaler affiner Raum	16
a_d	Anzahl der positiven Divisoren der Kurve C, die den Grad d besitzen	21
b_d	Anzahl der Primdivisoren $[P] \in C/Gal(\bar{\mathbb{F}}_q/\mathbb{F}_q)$ vom Grad d	20
$\mathbb{C}$	Körper der komplexen Zahlen	23
C	projektive algebraische Kurve	18
c_d^{prim}	Punkte von C, die primitiv vom Grad d sind	22
$C(\mathbb{F}_{q^n})$	Menge der $\mathbb{F}_{q^n}$-rationalen Punkte von C	19
D	Divisor aus $\mathcal{D}_F$	9
$deg\, D$	Grad des Divisors D	9
$\mathcal{D}_F$	Divisorgruppe von F/K	9
$dim\, D$	Dimension des Divisors D	10
$e(P' \mid P)$	Verzweigungsindex von P' über P	13
F/K	algebraischer Funktionenkörper über K	7
F'/K'	algebraische Erweiterung von F/K	12
F_P	Restklassenkörper von P	8
$\mathbb{F}_q$	endlicher Körper mit q Elementen	19
g	Geschlecht von F/K	11
$K(x)$	rationaler Funktionenkörper über K	7
$K(C)$	Körper der K-rationalen Funktionen auf C	18
$\bar{K}(C)$	Körper der rationalen Funktionen auf C	18
$\bar{K}(V)$	Funktionenkörper der Varietät V	17
$L(T)$	L-Polynom der Kurve C	23
$\mathcal{L}(A)$	$\mathcal{L}$-Raum des Divisors A	10
$M_{q,g}(x_1, \ldots, x_n)$	die zu minimierende Funktion	40
$M_g(x_1, \ldots, x_n)$	die zu minimierende Funktion im Fall $q = 2$	41
$\mathcal{M}_q(g)$	ganzzahliger Anteil des vom Progamm berechneten Minimums von M_g	54

Literaturverzeichnis

[Che51] C. Chevalley. *Introduction to the Theory of Algebraic Functions of one Variable.* American Mathematical Society, New York, 1951.

[Ful69] W. Fulton. *Algebraic Curves.* Benjamin, New York, 1969.

[LN83] R. Lidl-Niederreiter. *Encyclopedia of Mathematics and its Applications - Finite Fields.* Addison-Wesley Publishing Company, London-Amsterdam-Don Mills, 1983.

[Lor96] D. Lorenzini. *An Invitation to Arithmetic Geometry.* American Mathematical Society, Rhode Island, 1996.

[Ser83] J.-P. Serre. *Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini.* C. R. Acad. Sc. Paris, t. 296, Sér. I, 397 - 402, 1983.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin-Heidelberg-New York, 1993.

Anhang

Exemplarische Maple-Sitzung:

```
> d:=2;
> for i from d+1 to 2*d do x[i]:=0 od;
```

$$d := 2$$
$$x_3 := 0$$
$$x_4 := 0$$

```
> x[0]:=1;
```

$$x_0 := 1$$

```
> c:=1+2*sum('x[j]^2','j'=1..d);
```

$$c := 1 + 2\,x_1{}^2 + 2\,x_2{}^2$$

```
> p1:=(sum('(sum('x[i]*x[r-i]','i'=0..r)
+sum('2*x[i]*x[r+i]','i'=1..d-r)) *sqrt(2)^r','r'=1..d)
+sum('sum('x[i]*x[l-i]*sqrt(2)^l', 'i'=1..l)','l'=d+1..2*d))/c;
```

$$p1 := \frac{(2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2} + 4\,x_2 + 2\,x_1{}^2 + 4\,x_1\,x_2\,\sqrt{2} + 4\,x_2{}^2}{1 + 2\,x_1{}^2 + 2\,x_2{}^2}$$

```
> p2:=(sum('(sum('x[i]*x[r-i]','i'=0..r)
+sum('2*x[i]*x[r+i]','i'=1..d-r)) *sqrt(1/2)^r','r'=1..d)
+sum('sum('x[i]*x[l-i]*sqrt(1/2)^l', 'i'=1..l)','l'=d+1..2*d))/c;
```

$$p2 := \frac{\frac{1}{2}\,(2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2} + x_2 + \frac{1}{2}\,x_1{}^2 + \frac{1}{2}\,x_1\,x_2\,\sqrt{2} + \frac{1}{4}\,x_2{}^2}{1 + 2\,x_1{}^2 + 2\,x_2{}^2}$$

```
> M:=g/p2+p1/p2+1;
```

$$M := 3\,\frac{1 + 2\,x_1{}^2 + 2\,x_2{}^2}{\frac{1}{2}\,(2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2} + x_2 + \frac{1}{2}\,x_1{}^2 + \frac{1}{2}\,x_1\,x_2\,\sqrt{2} + \frac{1}{4}\,x_2{}^2} + \frac{(2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2} + 4\,x_2 + 2\,x_1{}^2 + 4\,x_1\,x_2\,\sqrt{2} + 4\,x_2{}^2}{\frac{1}{2}\,(2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2} + x_2 + \frac{1}{2}\,x_1{}^2 + \frac{1}{2}\,x_1\,x_2\,\sqrt{2} + \frac{1}{4}\,x_2{}^2} + 1$$

```
> for i from 1 to d do d[i]:=diff(M,x[i]) od;
```

$$d_1 := -3\,\frac{(1 + 2\,x_1{}^2 + 2\,x_2{}^2)\,(\frac{1}{2}\,(2 + 2\,x_2)\,\sqrt{2} + x_1 + \frac{1}{2}\,x_2\,\sqrt{2})}{\%3^2} + 12\,\frac{x_1}{\%3} + \frac{(2 + 2\,x_2)\,\sqrt{2} + 4\,x_1 + 4\,x_2\,\sqrt{2}}{\%3} - \frac{(\%2 + 4\,x_2 + 2\,x_1{}^2 + 4\,\%1 + 4\,x_2{}^2)\,(\frac{1}{2}\,(2 + 2\,x_2)\,\sqrt{2} + x_1 + \frac{1}{2}\,x_2\,\sqrt{2})}{\%3^2}$$

$$\%1 := x_1\,x_2\,\sqrt{2}$$
$$\%2 := (2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2}$$
$$\%3 := \frac{1}{2}\,\%2 + x_2 + \frac{1}{2}\,x_1{}^2 + \frac{1}{2}\,\%1 + \frac{1}{4}\,x_2{}^2$$

$$d_2 := -3\,\frac{(1 + 2\,{x_1}^2 + 2\,{x_2}^2)\,(\frac{3}{2}\,x_1\,\sqrt{2} + 1 + \frac{1}{2}\,x_2)}{\%3^2} + 12\,\frac{x_2}{\%3} + \frac{6\,x_1\,\sqrt{2} + 4 + 8\,x_2}{\%3}$$
$$- \frac{(\%2 + 4\,x_2 + 2\,{x_1}^2 + 4\,\%1 + 4\,{x_2}^2)\,(\frac{3}{2}\,x_1\,\sqrt{2} + 1 + \frac{1}{2}\,x_2)}{\%3^2}$$
$$\%1 := x_1\,x_2\,\sqrt{2}$$
$$\%2 := (2\,x_1 + 2\,x_1\,x_2)\,\sqrt{2}$$
$$\%3 := \frac{1}{2}\,\%2 + x_2 + \frac{1}{2}\,{x_1}^2 + \frac{1}{2}\,\%1 + \frac{1}{4}\,{x_2}^2$$

```
> g:=3;fsolve({d[1]=0,d[2]=0},{x[1],x[2]},{x[1]=0..1,x[2]=0..1});
```

$$g := 3$$
$$\{x_1 = .8318452320,\ x_2 = .3839329801\}$$

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
1	5	26	25	51	41	76	56
2	6	27	25	52	42	77	57
3	7	28	26	53	42	78	57
4	8	29	27	54	43	79	58
5	9	30	27	55	43	80	59
6	10	31	28	56	44	81	59
7	11	32	29	57	45	82	60
8	11	33	29	58	45	83	60
9	12	34	30	59	46	84	61
10	13	35	31	60	47	85	62
11	14	36	31	61	47	86	62
12	15	37	32	62	48	87	63
13	15	38	33	63	48	88	63
14	16	39	33	64	49	89	64
15	17	40	34	65	50	90	65
16	18	41	35	66	50	91	65
17	18	42	35	67	51	92	66
18	19	43	36	68	51	93	66
19	20	44	37	69	52	94	67
20	21	45	37	70	53	95	68
21	21	46	38	71	53	96	68
22	22	47	38	72	54	97	69
23	23	48	39	73	54	98	69
24	23	49	40	74	55	99	70
25	24	50	40	75	56	100	71

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
101	71	126	86	151	100	176	114
102	72	127	86	152	100	177	114
103	72	128	87	153	101	178	115
104	73	129	87	154	101	179	115
105	73	130	88	155	102	180	116
106	74	131	88	156	103	181	117
107	75	132	89	157	103	182	117
108	75	133	90	158	104	183	118
109	76	134	90	159	104	184	118
110	76	135	91	160	105	185	119
111	77	136	91	161	105	186	119
112	78	137	92	162	106	187	120
113	78	138	92	163	106	188	120
114	79	139	93	164	107	189	121
115	79	140	94	165	108	190	122
116	80	141	94	166	108	191	122
117	80	142	95	167	109	192	123
118	81	143	95	168	109	193	123
119	82	144	96	169	110	194	124
120	82	145	96	170	110	195	124
121	83	146	97	171	111	196	125
122	83	147	97	172	112	197	125
123	84	148	98	173	112	198	126
124	84	149	99	174	113	199	127
125	85	150	99	175	113	200	127

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
201	128	226	141	251	155	276	169
202	128	227	142	252	156	277	169
203	129	228	143	253	156	278	170
204	129	229	143	254	157	279	170
205	130	230	144	255	157	280	171
206	130	231	144	256	158	281	171
207	131	232	145	257	158	282	172
208	132	233	145	258	159	283	172
209	132	234	146	259	159	284	173
210	133	235	146	260	160	285	173
211	133	236	147	261	161	286	174
212	134	237	147	262	161	287	175
213	134	238	148	263	162	288	175
214	135	239	149	264	162	289	176
215	135	240	149	265	163	290	176
216	136	241	150	266	163	291	177
217	137	242	150	267	164	292	177
218	137	243	151	268	164	293	178
219	138	244	151	269	165	294	178
220	138	245	152	270	165	295	179
221	139	246	152	271	166	296	179
222	139	247	153	272	166	297	180
223	140	248	153	273	167	298	180
224	140	249	154	274	168	299	181
225	141	250	155	275	168	300	182

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
301	182	326	195	351	209	376	222
302	183	327	196	352	209	377	223
303	183	328	197	353	210	378	223
304	184	329	197	354	210	379	224
305	184	330	198	355	211	380	224
306	185	331	198	356	211	381	225
307	185	332	199	357	212	382	225
308	186	333	199	358	212	383	226
309	186	334	200	359	213	384	226
310	187	335	200	360	214	385	227
311	187	336	201	361	214	386	227
312	188	337	201	362	215	387	228
313	189	338	202	363	215	388	228
314	189	339	202	364	216	389	229
315	190	340	203	365	216	390	229
316	190	341	203	366	217	391	230
317	191	342	204	367	217	392	231
318	191	343	205	368	218	393	231
319	192	344	205	369	218	394	232
320	192	345	206	370	219	395	232
321	193	346	206	371	219	396	233
322	193	347	207	372	220	397	233
323	194	348	207	373	220	398	234
324	194	349	208	374	221	399	234
325	195	350	208	375	222	400	235

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
401	235	426	248	451	262	476	275
402	236	427	249	452	262	477	275
403	236	428	250	453	263	478	276
404	237	429	250	454	263	479	276
405	237	430	251	455	264	480	277
406	238	431	251	456	264	481	277
407	238	432	252	457	265	482	278
408	239	433	252	458	265	483	278
409	239	434	253	459	266	484	279
410	240	435	253	460	266	485	279
411	241	436	254	461	267	486	280
412	241	457	254	462	267	487	280
413	242	438	255	463	268	488	281
414	242	439	255	464	268	489	282
415	243	440	256	465	269	490	282
416	243	441	256	466	269	491	283
417	244	442	257	467	270	492	283
418	244	443	257	468	271	493	284
419	245	444	258	469	271	494	284
420	245	445	258	470	272	495	285
421	246	446	259	471	272	496	285
422	246	447	260	472	273	497	286
423	247	448	260	473	273	498	286
424	247	449	261	474	274	499	287
425	248	450	261	475	274	500	287

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
501	288	526	301	551	314	576	327
502	288	527	301	552	314	577	327
503	289	528	302	553	315	578	328
504	289	529	302	554	315	579	328
505	290	530	303	555	316	580	329
506	290	531	303	556	316	581	329
507	291	532	304	557	317	582	330
508	291	533	304	558	317	583	330
509	292	534	305	559	318	584	331
510	292	535	305	560	318	585	331
511	293	536	306	561	319	586	332
512	294	537	307	562	319	587	332
513	294	538	307	563	320	588	333
514	295	539	308	564	320	589	333
515	295	540	308	565	321	590	334
516	296	541	309	566	322	591	334
517	296	542	309	567	322	592	335
518	297	543	310	568	323	593	335
519	297	544	310	569	323	594	336
520	298	545	311	570	324	595	337
521	298	546	311	571	324	596	337
522	299	547	312	572	325	597	338
523	299	548	312	573	325	598	338
524	300	549	313	574	326	599	339
525	300	550	313	575	326	600	339

g	$\mathcal{M}_2(g)$	g	$\mathcal{M}_2(g)$
600	339	850	467
610	344	860	472
620	349	870	477
630	355	880	482
640	360	890	487
650	365	900	492
660	370	910	497
670	375	920	502
680	380	930	507
690	385	940	512
700	390	950	518
710	396	960	523
720	401	970	528
730	406	980	533
740	411	990	538
750	416	1000	543
760	421	2000	1038
770	426	3000	1525
780	431	4000	2006
790	436	5000	2483
800	441	6000	2948
810	447	7000	3430
820	452	8000	3901
830	457	9000	4371
840	462	10000	4839

```
#include <stdio.h>
#include <math.h>
#include <time.h>

#define DR 3
#define QQ 2                  /*Der Koerper, ueber dem die Kurven
                                definiert sind.*/
#define XX 20                 /*Maximale Laenge des x-Vektors +1.*/
#define ECK 101               /*Anzahl der gespeicherten Punkte +1.*/
#define GG_UNTEN 200          /*Fuer g = 200 bis g = 300 sollen Minima*/
#define GG 300                /*bestimmt werden.*/
#define SS 0.25               /*Schrittweite.*/
#define FINE  1               /*Die Genauigkeit wird mit 1 initialisiert.*/
#define LONG 0.1              /*Schranke zur Steuerung der Vektorlaenge.*/

double mini(int n, int l, int g, double fine, int B[], double xwert[],
            double xv[XX][DR], double ss, int ec, double xmatr[ECK][XX]);


main()
{
        FILE *dat_ptr;
        double xwert[2*XX-1], xv[XX][DR], M[XX], xmatr[ECK][XX];
        double ss, w, fine;
        int B[ECK], i, k, sq, g, n, st, l, ec, inte;

        xwert[0] = 1;

/*G: Aeusserste Schleife, die alle g's im oben gewaehlten Bereich
  durchlaeuft.*/

/*G*/   for (g = GG_UNTEN; g < GG + 1; g++){
        printf("g = %d\n",g);
        n = 3;        /*Die Vektorlaenge ist zunaechst gleich 2.*/
        sq = 2*sqrt(QQ);
        M[n-1] = QQ + 1 + (g*sq);  /*Erster Vergleichswert aus
                                     der Weil-Abschaetzung.*/

/*FI:diese Schleife erhoeht die Genauigkeit fine, falls der
  ganzzahlige Anteil des von der N-Schleife zurueckgegebenen
  Wertes noch verbessert werden kann. Das heisst, falls bei fine=0.1
  der Nachkommateil des Wertes kleiner als 0.2 ist, wird die Rechnung
  mit einer Genauigkeit von 0.01 wiederholt. Dann wird geprueft, ob
  der Nachkommateil des Wertes kleiner als  0.02 ist usw. . Bei 10
  hoch minus 7 wird abgebrochen.*/

        fine = FINE;
/*FI*/  do{
        fine = fine * 0.1;
        n = 3;

/*LO: hier wird die Vektorlaenge gesteuert. Die Vektorlaenge n wird
  solange erhoeht, bis die Schranke LONG unterschritten wird.*/

/*LO*/  do{
                n++;
                ss = SS;
                ec = ECK;
                l = 2*n-1;
                for (i = 1; i < 2*XX-1; i++)
                        xwert[i] = 0;           /*Initialisierung von xwert*/
                for (i = 1; i < ECK; i++)       /*Initialisierung von B*/
                        B[i] = i;
                for (i = 1; i < XX; i++){       /*Initialisierung von xv*/
                        xv[i][1] = 1;
                        xv[i][2] = 0;
                }

                /*Die Funktion mini gibt fuer festes g und n den mit
                  Genauigkeit fine optimalen Funktionswert samt
                  zugehoerigem Vektor aus.*/

                w = mini(n, l, g, fine, B, xwert, xv, ss, ec, xmatr);
                M[n-1] = w;

                /*Diese Ausgabe kann in eine Datei umgeleitet werden,
                  sie liefert die Zwischenergebnisse fuer die
                  einzelnen Vektorlaengen.*/
```

```
printf("\nM[%d] = %lf\n", n-1, M[n-1]);
                printf("(M[%d] - M[%d]) = %lf\n", n-2, n-1, (M[n-2] - M[n-1]));
                printf("Vektor zu M[%d]:\n", n-1);
                for(i=1; i<n; i++)
                  printf(" %lf", xmatr[B[1]][i]);
                fflush(stdout);
/*LO*/  }while((M[n-2] - M[n-1]) > LONG);
        inte = M[n-1];
        if((M[n-1] - inte) < 0.0000001)
          inte = M[n-1] - 1;
/*FI*/      }while((M[n-1] - inte) < (2*fine));

        st = B[1]; /*Die Stelle in xmatr, wo der Loesungsvektor steht.*/

        /*Das Endergebins fuer das entsprechende g wird in folgende Datei
          geschrieben.*/

/*DAT*/ dat_ptr = fopen("func200_300","a");
        fprintf(dat_ptr,"\ng = %d ", g);
        fprintf(dat_ptr,"   Wert: %lf\n", M[n-1]);
        for (i = 1; i < n; i++)
          fprintf(dat_ptr,"%lf  ", xmatr[st][i]);
/*DAT*/ fclose(dat_ptr);

/*G*/ }
        return 0;
}

/*Ende des Hauptprogramms.*/

/*Die Minimierungsfunktion gibt fuer ein festes n und festes g
  den optimalen Funktionswert samt zugehoerigem Vektor xwert
  aus.*/

double mini(int n, int l, int g, double fine, int B[], double xwert[],
          double xv[XX][DR], double ss, int ec, double xmatr[ECK][XX])
{
        double gitter(int n, double ss, double xv[XX][DR]);
        double punkt(double xwert[], double ss, double xv[XX][DR], int n);
        double auswertung(double xwert[], int n, int l, int g);
        double ordnung(double MM[], int B[], int ec, double xwert[],
           int n, double mm, double xmatr[ECK][XX], int gp);
        double feld(double xmatr[ECK][XX], double xv[XX][DR],
            double ss, int ec, int n);
        double  d, mm;
        double MM[ECK];
        int   j, k, r, s, h, t;
        unsigned long int gp;

/*S: Innerhalb dieser Schleife werden die Punkte eines n-dim. Gitters
  ausgewertet. Die 100 besten Werte werden gespeichert, ein neues
  Gitter wird um diese Werte gelegt. Es ist das neue Ausgangsgitter,
  in dem dann mit halbierter Schrittweite weitergerechnet wird. Am
  Ende der Schleife wird geprueft, ob die Differenz zwischen dem
  groessten und dem kleinsten Wert groesser als fine ist. Solange dies
  erfuellt ist, wird mit einem jeweils neuen Gitter weiterverfahren
  wie zuvor. Ist die Bedingung nicht mehr erfuellt, so wird der
  kleinste der 100 Werte an das Hauptprogramm zurueckgegeben.*/

/*S*/   do{
        d = gitter(n, ss, xv);       /*Anzahl der Gitterpunkte.*/
        xwert[1] = xv[1][2] - ss;    /*Initialisierung fuer die
                                       Funktion punkt.*/
        if(xwert[1] < 0){            /*Der Nullpunkt wird ausgenommen.*/
                xwert[1] = 0;
                d = d-1;
        }

        /*Die Funktion punkt erhaelt den ersten Gitterpunkt, woraus
          sie alle weiteren berechnet.*/

        for (s = 2; s < XX; s++)
                xwert[s] = xv[s][2];

        /*Alle Gitterpunkte gp werden durchlaufen.*/

/*gp*/  for (gp = 1; gp < d+1; gp++){
```

```
        /*punkt berechnet bei jedem Aufruf einen Gitterpunkt.
          punkt(Vektor, Schrittweite, Gittergrenzen, Vektorlaenge).*/

                punkt(xwert, ss, xv, n);

                /*auswertung berechnet zu gegebenem Vektor und
                  Geschlecht den Funktionswert.
                  auswertung(Vektor, Vektorlaenge, Geschlecht).*/

                mm = auswertung(xwert, n, l, g);

                /*Die ersten 100 Funktionswerte und ihre Punkte werden
                  gespeichert,...*/

                if (gp < ec){
                        MM[gp] = mm;
                        for (r = 1; r < XX; r++)
                        xmatr[gp][r] = xwert[r];
                }

                /*...dann werden sie geordnet. Alle weiteren Werte
                  werden in die Reihe eingefuegt. ordnung(Werte,
                  Hilfsvektor, x-Vektor, Vektorlaenge, x-Matrix,
                  #Gitterpunkte).*/

                if (gp >= ec){
                        ordnung(MM, B, ec, xwert, n, mm, xmatr, gp);
                }
/*gp*/   }

        /*Alle Gitterpunkte sind nun ausgewertet, die 100 besten Werte
          sind gespeichert in MM[ECK], die zugehoerigen Vektoren in
          xmatr[ECK][XX]. Die Funktion feld erzeugt nun anhand der
          x-Martrix ein neues Gitter. Der Bereich, in dem der optimale
          Wert der Funktion fuer vorgegebenes n und g liegt, wird
          somit eingegrenzt. Durch Halbieren der Schrittweite wird das
          Netz verfeinert. feld(x-Matrix, Gittergrenzen, Schrittweite,
          #Eckpunkte, Vektorlaenge).*/


         feld(xmatr, xv, ss, ec, n);
         ss = ss/2;                             /*Schrittweite/2*/

         /*Die Differenz zwischen dem groessten und dem kleinsten Wert
           wird gebildet. Ist diese < fine, wird das neu errechnete
           Gitter nicht weiter verfeinert, sondern n um 1
           hochgesetzt.*/

/*S*/    }while((MM[ec-1] - MM[1]) > fine);

        /*Der beste Wert fuer fuer festes n und g wird zurueckgegeben.*/

         return MM[1];
}

/*Ende der Funktion mini.*/

/*Die Funktion Gitter gibt die Anzahl der neuen Gitterpunkte aus. Die
  Matrix xv enthaelt in der ersten Spalte alle maximalen Koordinaten
  jeder Komponente der Gittervektoren, in der zweiten alle
  minimalen. Die Anzahl der Gitterpunkte erhaelt man, indem man fuer
  jede Komponente die Differenz max-min durch die Schrittweite teilt,
  die 1 addiert, und alle Ergebnisse
  multipliziert. gitter(Vektorlaenge, Schrittweite, Gittergrenzen).*/

double gitter (int n, double ss, double xv[XX][DR])
{
        int k;
        double en;

        en = 1;
        for (k = 1; k < n; ++k)
                en = (((xv[k][1]-xv[k][2])/ss)+1) * en;
        return en;
}
```

```
/*Die Funktion punkt berechnet den naechsten Vektor xwert.*/

double punkt(double xwert[], double ss, double xv[XX][DR], int n)
{
        int i;
        i = 1;

        while (((xwert[i] + ss ) > xv[i][1] + 0.000000001) && i < n-1){
                xwert[i] = xv[i][2];
                i++;
        }
        xwert[i] = xwert[i] + ss;
        return 0;
}

/*Die Funktion Auswertung berechnet den naechsten
  Funktionswert. auswertung(x-Vektor, Vektorlaenge, Geschlecht).*/

double auswertung(double xwert[], int n, int l, int g)
{
        double psi (double koeff[], double w, int l);
        double doppels (double xwert[], double cmine, double cvec[], int l);
        double koeff[2*XX-1];
        double p1, p2, cmin, cmine, aa;
        int k;

        cmin = 0;
        for (k = 1; k < n; ++k)
                cmin = pow(xwert[k], 2) + cmin;
        cmine = 1 + 2 * cmin;
        doppels(xwert, cmine, koeff, l);
        p1 = psi(koeff,sqrt(QQ), l);
        p2 = psi(koeff, 1/sqrt(QQ), l);
        aa = ((1/p2) * g) + (1+(p1/p2));
        return aa;
}

/*Die Funktion Psi.*/

double psi(double koeff[], double w, int l)
{
        int i;
        double h;
        h = 0;
        for (i = 1; i < l; ++i)
                h = (koeff[i] * pow( w, i)) + h;
        return h;
}

/*Die Funktion doppels.*/

double doppels (double xwert[], double cmine, double cvec[], int l)
{
        int t, i, s;
        double zz, yy, bb;
        cvec[0] = 0;
        for (t = 1; t < (l+1)/2; ++t){
                yy = zz = 0;
                for (i = 0; i <= t; ++i)
                        zz = (xwert[i] * xwert[t-i]) + zz;
                for (s = 1; s < (((l+1)/2)-t); ++s)
                        yy = (2 * (xwert[s] * xwert[t+s])) + yy;
                cvec[t] = pow(cmine, -1) * (zz + yy);
                /*Dies sind die Koeffizienten von 1 bis n*/
        }
        for (t = (l+1)/2; t < l; ++t){
                bb = 0;
                for (s = 1; s < t; ++s){
                        bb = (xwert[s] * xwert[t-s]) + bb;
                        cvec[t] = pow(cmine, -1) * bb;
                        /*Dies sind die Koeffizienten von n+1 bis 2n*/
                }
        }
        return 0;
}
```

```
/*Die Funktion ordnung sortiert die 2 hoch n Funktionswerte
  aufsteigend, und ordnet hinzukommende ein.*/

double ordnung(double MM[], int B[], int ec, double xwert[],
               int n, double mm, double xmatr[ECK][XX], int gp)
{
        int i, j, k, y, t, p, q, ende, low, right, left;
        double binsearch(double MM[], int ec, double mm);
        void q2sort (double MM[], double xmatr[ECK][XX], int left,
                     int right, int n);

        left = 1;
        right = ec-1;

        /*Die Funktion qsort ordnet im Falle gp=100 die 100
          Funktionswerte aufsteigend, und bringt auch die zugehoerigen
          Vektoren in die entsprechende Reihenfolge.*/

        if (gp-1 < ec){
                q2sort(MM, xmatr, left, right, n);
              }

        /*Im Falle gp > 100 werden die hinzukommenden Werte nebst
          Vektoren einsortiert,...*/

/*GP*/  if (gp-1 >= ec){

        /*...falls der neu errechnete Funktionswert kleiner als der
          groesste Wert in der Liste ist.*/

/*M*/     if (mm < MM[ec-1]){

        /*binsearch ermittelt die passende Einfuegestelle(low).*/

                low = binsearch(MM, ec, mm);

                /*Werte von bereits berechneten Gitterpunkten sollen
                  nicht in die Reihe eingefuegt werden.*/
                y = 0;
/*IF*/          if(fabs(MM[low] - mm) <= 0.0000000001){
                  for(t = 1; t < XX; t++){
                    if(fabs(xmatr[B[low]][t] - xwert[t]) <= 0.00000000001)
                      y++;
                    else
                       ;
                  }
/*IF*/ }
                if(y == XX)
                  ;

                /*Sonst ordne den Funktionswert samt x-Vektor in die
                  Reihe ein. Im Vektor B[ECK] ist die Anordnung der
                  Zeilen in der x-Matrix kodiert. Steht z. B. an der
                  Stelle B[2] der Eintrag 4, so bedeutet dies: in der
                  4.Zeile der x-Matrix steht der Vektor, der zu dem
                  Wert MM[2] gehoert. Einfuegevorgang: i wird auf ec-1
                  gesetzt, und ende erhaelt den Eintrag von
                  B[ec-1]. An der Stelle ec-1 in MM[] bzw. B[] seht ja
                  der schlechstest Wert bzw. Vektor. Die Werte B[low] bzw.
                  MM[low] bis B[ec-2] bzw. MM[ec-2] rutschen jeweils eine
                  Stelle nach hinten. Der schlechteste Wert wird so
                  geloescht. Die Einfuegestellen B[low] bzw. MM[low] sind
                  freigegeben.  MM[low] erhaelt den Funktionswert m,
                  ende wird in B[low] geschrieben, in die Zeile ende
                  der x-Matrix wird der Vektor, der zu dem Wert
                  MM[low] gehoert, eingefuegt.*/

                else{
                  i = ec-1;
                  ende = B[ec-1];
                  while (i > low){
                        MM[i] = MM[i-1];
                        B[i] = B[i-1];
                        i--;
                      }
                  MM[low] = mm;
                  B[low] = ende;
                  for (k = 1; k < n; k++)
                        xmatr[ende][k] = xwert[k];
                  /*ELSE*/ }
```

```
/*M*/      }
/*GP*/ }
        return 0;
}



/*q2sort: rekursive Funktion, die MM[left] ... MM[right] in
  aufsteigender Reihenfolge sortiert.*/

void q2sort (double MM[], double xmatr[ECK][XX], int left, int right, int n)
{
        int i, last;
        void s2wap(double MM[], double xmatr[ECK][XX], int i, int j, int n);

        if (left >= right) /*wenn der Vektor weniger als 2 Elemente enthaelt*/
        return;
        s2wap(MM, xmatr, left, ((left+right)/2), n); /*Bewege gewaehltes*/
                                                     /*Element nach MM[1].*/
        last = left;
        for (i = left+1; i <= right; i++)
                if (MM[i] < MM[left])
                s2wap(MM, xmatr, ++last, i, n);
        s2wap(MM, xmatr, left, last, n);
        q2sort(MM, xmatr, left, last-1, n);
        q2sort(MM, xmatr, last+1, right, n);
}

/*s2wap: vertauscht MM[i] und MM[j] und die entsprechenden Zeilen in
  der x-Matrix.*/

void s2wap(double MM[], double xmatr[ECK][XX], int i, int j, int n)
{
        double temp, te[XX];
        int m;

        temp = MM[i];                /*Vertauscht die Funktionswerte.*/
        MM[i] = MM[j];
        MM[j] = temp;

        for (m = 1; m < XX; m++){
        te[m] = xmatr[i][m];         /*Vertauscht die entsprechenden*/
        xmatr[i][m] = xmatr[j][m];   /*Zeilen in der x-Matrix.*/
        xmatr[j][m] = te[m];
        }
}

/*Binaere Suche der Einfuegestelle mittels binsearch.*/

double binsearch(double MM[], int ec, double m)
{
        int low, high, mid;
        low = 1;
        high = ec-1;
        while (low <= high){
                mid = (low+high)/2;
                if (m < MM[mid])
                        high = mid - 1;
                else if (m > MM[mid])
                        low = mid + 1;
                else
                        return mid;
        }
        return low;
}

/*Die Funktion feld erzeugt aus den 100 Gitterpunkten ein neues Suchfeld.*/

double feld(double xmatr[ECK][XX], double xv[XX][DR], double ss, int ec, int n)
{
        int f, r;
        double xsort[ECK], lleft, rlight;
        void extremwerte(double xsort[], int ec, double* unten, double* oben);
        for (f = 1; f < n; ++f){
                for(r = 1; r < ec; r++){
                        xsort[r] = xmatr[r][f];
                }
```

```
                extremwerte(xsort, ec, &lleft, &rlight);
                xv[f][1] = rlight + ss;
                if(xv[f][1] > 1)
                        xv[f][1] = 1;
                xv[f][2] = lleft - ss;
                if( xv[f][2] < 0)
                        xv[f][2] = 0;
        }
        return 0;
}

/*Die Funktion extremwerte sucht den groessten und den kleinsten Wert
  von xsort.*/

void extremwerte(double xsort[], int ec, double* unten, double* oben)
{
  int i;
  double hoch, tief;

  hoch = xsort[1];
  tief = xsort[1];

  for(i = 2; i < ec; i++){
    if(xsort[i] < tief)
      tief = xsort[i];
    if(xsort[i] > hoch)
      hoch = xsort[i];
  }
  *unten = tief;
  *oben  = hoch;
}
```