Berechnung einiger arithmetischer Funktionen im Zusammenhang mit Drinfeldschen Modulformen

Diplomarbeit

von

Michael Trautwein

Saarbrücken, Dezember 1998

Fachbereich 9, Mathematik

Ich erkläre hiermit an Eides statt, diese Arbeit selbstständig angefertigt und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Inhaltsverzeichnis

Einleitung

Im klassischen Fall der Charakteristik 0 gilt die Potenzreihenidentität

$$\sum_{n\geq 0} p(n)\, X^n \;=\; \left(\prod_{n\geq 1}(1-X^n)\right)^{-1},$$

wobei $p(n)$ die *Partitionsfunktion* ist, d.h. für eine natürliche Zahl n sei $p(n)$ die Anzahl der Darstellungen von n als Summe natürlicher Zahlen $n = k_1 + \cdots + k_r$ mit $k_1 \geq \cdots \geq k_r$. Der Vollständigkeit halber sei $p(0) := 1$. Die Funktion $\eta(z) = q^{\frac{1}{24}} \prod_{n\geq 1}(1-q^n)$ mit $q = e^{2\pi i z}$, die mit der rechten Seite in Verbindung steht, heißt *Dedekindsche η-Funktion.*

Die unendlichen Produkte $\prod_{n\geq 1} \frac{1}{1-z^n}$ und $\prod_{n\geq 1}(1-z^n)$ konvergieren absolut für alle komplexen Zahlen $z \in \mathbb{C}$ mit $|z| < 1$. Weiter gilt die Identität formaler Potenzreihen

$$\prod_{n\geq 1}(1-X^n) \;=\; \sum_{n\geq 0}(-1)^n\, X^{n(3n\pm 1)/2}.$$

Dies ermöglicht die Angabe einer Rekursionsformel zur Berechnung von $p(n)$, die auf den sogenannten *Fünfeckzahlen* $\omega(n) = \frac{n(3n-1)}{2}$, $n \in \mathbb{Z}$, basiert.

Eng mit der Funktion $\prod_{n\geq 1}(1-X^n)$ verwandt ist die *klassische Diskriminantenfunktion*

$$\Delta_{kl}\,(z) \;=\; (2\pi i)^{24}\; q \prod_{n\geq 1}(1-q^n)^{24}$$

mit $q = e^{2\pi i z}$. Sie tritt als Diskriminante (im üblichen Sinne) des Quadrats der Ableitung $(\wp')^2$ der *Weierstraßschen $\wp$-Funktion* auf (Formel von Jacobi), einer elliptischen Funktion auf der komplexen Zahlenebene. Die Koeffizienten von Δ_{kl} sind durch die *Ramanujan-Funktion* $\tau(n)$ gegeben, für die jedoch im Gegensatz zu den Koeffizienten der Funktion $\prod_{n\geq 1}(1-X^n)$ keine explizite Formel bekannt ist.

Sei $A = \mathbb{F}_q[T]$ der Polynomring in der Unbestimmten T über einem endlichen Körper $\mathbb{F}_q$. In gewissem Sinne kann A mit dem Ring $\mathbb{Z}$ der ganzen Zahlen identifiziert werden, denn A ist ebenso wie $\mathbb{Z}$ ein euklidischer Ring. Des Weiteren ist A diskret eingebettet in die Komplettierung K_∞ (bezüglich des zur Gradbewertung gehörenden Betrages) des Quotientenkörpers $K = \mathbb{F}_q(T)$ von A, ebenso wie $\mathbb{Z}$ diskret im Körper der reellen Zahlen $\mathbb{R}$ liegt, also der Komplettierung der rationalen Zahlen $\mathbb{Q}$ bezüglich des üblichen Absolutbetrages. Dem Körper $\mathbb{C}$ der komplexen Zahlen entspricht in dieser Situation die Komplettierung C des algebraischen Abschlusses $\overline{K_\infty}$ (bezüglich der eindeutigen Fortsetzung des oben erwähnten Betrages). Der Satz von Krasner besagt, daß C in der Tat algebraisch abgeschlossen ist.

Die *Drinfeldsche Diskriminantenfunktion*

$$\Delta \;=\; X^{q-1} \prod f_a(X)^{(q^2-1)(q-1)} \;\in A[[X]]$$

kann als Analogon zur klassischen Diskriminantenfunktion Δ_{kl} angesehen werden. Die hierbei vorkommenden *inversen a-ten Kreisteilungspolynome* f_a stehen in Verbindung mit dem *Carlitz-Modul*, einem sogenannten *Drinfeld-Modul* vom Rang 1. Das Polynom $f_a(X) \in A[X]$ entspricht $1 - X^a$, $a \in \mathbb{Z}$. Die Funktion Δ tritt des Weiteren als Modulform im Zusammenhang mit Drinfeld-Moduln vom Rang 2 auf.

Ebenso wie im Fall der klassischen Diskriminantenfunktion Δ_{kl} ist keine explizite Formel für die Koeffizienten von Δ bekannt. Es liegt daher nahe, zunächst die *Produktfunktion* $U = \prod f_a(X)$, die der Funktion $\prod_{n\geq 1}(1 - X^n)$ entspricht, zu untersuchen, um zu Aussagen über Δ zu gelangen.

Dieses ist die Aufgabe der vorliegenden Arbeit. Es sollen einerseits die Potenzreihen U und Δ sowie die „Zwischenstufe“ $h = U^{q^2-1}$ mit Hilfe eines hierzu entwickelten Computerprogramms bis zu möglichst hohen Graden berechnet werden und andererseits auf der Basis der erhaltenen numerischen Daten allgemeine Aussagen über diese Funktionen vermutet und bewiesen werden.

Die Arbeit gliedert sich in Kapitel 1 *Grundlagen*, Kapitel 2 *Berechnung der Funktionen U, h und $\tilde{\Delta}$* und Kapitel 3 *Resultate*.

Kapitel 1 stellt die benötigten Grundlagen bereit. Es ergibt sich, daß die Drinfeldsche Diskriminantenfunktion Δ, die zunächst als Koeffizient von Drinfeld-Moduln des Ranges 2 auftritt und als solcher von einem Parameter $z \in C - K_\infty$ abhängt, nach geeigneter Uniformisierung als Potenzreihe der oben angegebenen Form dargestellt werden kann, die von speziellen Eigenschaften von Drinfeld-Moduln weitgehend unabhängig ist.

Für $0 \neq a \in A$ mit $d = \deg(a)$ ist das inverse a-te Kreisteilungspolynom f_a definiert durch $f_a(X) = \rho_a(X^{-1})\,X^{q^d}$. Hierbei ist ρ_a der Homomorphismus des Carlitz-Moduls, eines Drinfeld-Moduls vom Rang 1. Als „Vorstufe“ zur Diskriminantenfunktion Δ ist zunächst die Produktfunktion $U = \prod f_a \in A[[X]]$ von Interesse, wobei das Produkt alle normierten Polynome a aus A durchläuft. Die Koeffizienten von ρ_a können rekursiv berechnet werden, so daß auch f_a explizit angegeben werden kann. Es stellt sich jedoch heraus, daß vor allem die Polynome der Form f_{T^d}, $d \in \mathbb{N}$, von Bedeutung sind, für die es eine einfachere Berechnungsmöglichkeit als nach der Definition von f_a gibt. Es ergibt sich im gleichen Rahmen, daß die Koeffizienten von

f_{T^d}, die a priori in $\mathbb{F}_q[T]$ liegen, sogar aus $\mathbb{F}_p[T]$ stammen, wobei $\mathbb{F}_p$ der Primkörper von $\mathbb{F}_q$ ist. Hieraus folgt im Verlauf der Arbeit, daß dieses auch auf die Potenzreihen U, h und Δ zutrifft. Des Weiteren ist f_a Polynom in $S := X^{q-1}$, d.h. alle in f_a auftretenden Exponenten sind Vielfache von $q-1$, was dann auch für die darauf aufbauenden Potenzreihen U, h und Δ gilt. Statt der Funktion Δ betrachten wir im Folgenden die Funktion $\tilde{\Delta} := \Delta/(-S) = U^{(q^2-1)(q-1)}$.

Kapitel 2 beschäftigt sich mit der Frage nach der effizienten Berechenbarkeit der gesuchten Potenzreihen sowie der Entwicklung von Algorithmen. Als erstes gilt es die Produktfunktion U zu betrachten, denn die übrigen Funktionen ergeben sich im Wesentlichen als Potenzen von ihr. Zwar ist U als unendliches Produkt definiert, es ist jedoch leicht einzusehen, daß zu jedem festen Koeffizienten von U jeweils nur endlich viele Polynome f_a beitragen können, so daß prinzipiell jeder Koeffizient von U berechenbar ist. Wir zerlegen nun das unendliche Produkt $\prod f_a$ in endliche Teilprodukte, indem wir mit U_d das Produkt all der Polynome f_a, wobei $a \in A$ normiert und vom festen Grad $d \in \mathbb{N}_0$ ist, bezeichnen. Dann ist U_d ein Polynom des Grades $\frac{q^d(q^d-1)}{q-1}$ (bezüglich S).

Es gilt also $U = \prod_{i=0}^{\infty} U_i$. Das Polynom $P_d := \prod_{i=0}^{d} U_i$ muß dann nach Konstruktion bis zu einem gewissen Grad mit der Potenzreihe U übereinstimmen. Es ergibt sich das recht erfreuliche Ergebnis, daß die Übereinstimmung, falls die zugrunde liegende Primzahlpotenz q nicht zwei ist, vollständig bis zum Grad von P_d gilt. Dieser beträgt $\frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)} \approx q^{2d-1}$. Das Polynom P_d stellt also einen Anfangsabschnitt der Potenzreihe U dar. Aufgrund des exponentiellen Wachstums der Grade der Polynome P_d ist allerdings von vorneherein davon auszugehen, daß P_d nicht für allzu große Werte von d ausgerechnet werden kann. Wie „lang“ die zugehörigen Koeffizienten, die selbst Polynome aus $A = \mathbb{F}_q[T]$ (bzw. $\mathbb{F}_p[T]$) sind, maximal werden können, wird in Kapitel 3 untersucht. Nichtsdestoweniger ist das nächste Ziel die Entwicklung von Algorithmen zur Berechnung von P_d. Die Definition von P_d ist zur Berechnung ziemlich ungeeignet.

Sei $H_{d,i}$ für $d \in \mathbb{N},\ 0 \le i \le d-1$, definiert durch

$$H_{d,i} \ := \prod_{(c_0,\dots,c_i)\in\mathbb{F}_q^{i+1}} f_{T^d+c_iT^i+\cdots+c_0}.$$

Dann genügt $H_{d,i}$ der Rekursionsformel

$$H_{d,i} \ = \ H_{d,i-1}^{q} \ - \ H_{d,i-1}\, H_{i,i-1}^{q-1}\, S^{q^i(q^d-q^i)}$$

mit $H_{d,-1} := f_{T^d}$. Dies liefert einen ersten Algorithmus, der in einem Dreicksschema die Werte $U_i = H_{i,i-1},\ i = 1,\dots,d$, liefert. Hieraus kann man durch Multiplikation das Polynom P_d erhalten. Seien weiter

$$V_d \ := \prod_{\substack{a\in A \text{ normiert}\\ \deg(a)=d}} \rho_a, \qquad Q_d \ := \prod_{i=0}^{d} V_i.$$

Dann ist das Polynom Q_d eng mit P_d verwandt – es enthält die gleichen Koeffizienten aus A wie P_d mit anderer Indizierung, insbesondere in gespiegelter Reihenfolge. Für Q_d gilt die Identität

$$Q_d \;=\; \sum_{\sigma \in S_{d+1}} \epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}},$$

wobei S_{d+1} die symmetrische Gruppe der Permutationen von $0, \ldots, d$ ist. Dies liefert einen zweiten Algorithmus zur Berechnung von P_d – man kann Q_d leicht zu P_d konvertieren. Dieser Algorithmus erweist sich als dem ersten deutlich überlegen, wobei er allerdings die Berechnung der Teilprodukte U_d „überspringt“. Ist man an diesen interessiert, so ist die Verwendung des ersten Algorithmus nötig. Die beiden Formeln für $H_{d,i}$ und Q_d wurden von Bartolomé López in der Arbeit [7] bewiesen.

Beide Algorithmen wurden in der Programmiersprache C++ implementiert. Die Berechnungen wurden jeweils für feste Werte von q durchgeführt, und zwar für $q = 2, 3, 4, 5, 7, 8, 9$ (zu Testzwecken in geringem Umfang auch für $q = 11, 13$). Zwar zeigt die Formel für Q_d, daß es auch möglich ist, Q_d und somit P_d symbolisch für allgemeines q darzustellen; dies war jedoch nicht Anliegen der vorliegenden Arbeit, da spätestens die Berechnung der Diskriminantenfunktion $\tilde{\Delta} = U^{(q^2-1)(q-1)}$ feste Werte für q erfordert. Mit dem entwickelten Computerprogramm konnte P_6 für $q = 2$ und ansonsten P_5 berechnet werden. Daraus wurde $\tilde{\Delta}$ abhängig von q bis zu Graden zwischen q^5 und q^{12} berechnet. Im Rahmen der Berechnung von $\tilde{\Delta}$ ergaben sich nebenbei auch die Funktionen U^{-1} und h.

Der Programmcode umfaßt insgesamt ca. 2 000 Zeilen und ist daher nicht in dieser Arbeit zu finden; er kann jedoch im World Wide Web unter der Adresse

http://www.math.uni-sb.de/˜mitr/index.html

betrachtet werden. Dort stehen außerdem Teile der berechneten Daten in Form von komprimierten Binärdateien zur Verfügung, die mit Hilfe des hierzu entwickelten Dateibetrachtungsprogramms *Diskriminante* (deutsche Version) oder *Discriminant* (englische Version) betrachtet oder in Textdateien umgewandelt werden können. Dieses unter Windows 3.1x oder Windows 95/98 lauffähige Programm kann ebenfalls auf dieser Seite heruntergeladen werden.

Eine erste Folgerung aus den Ergebnissen dieses Kapitels ist die Tatsache, daß im Fall $q > 2$ die Potenzreihe U große Lücken besitzt, d.h. Intervalle, in denen alle Koeffizienten verschwinden. Dies beruht darauf, daß U_{d+1} von der Form

$$U_{d+1} \;=\; 1 - S^{q^{2d}(q-1)} + O\big(S^{q^{2d}(q-1)+1}\big)$$

ist, wobei der Wert $q^{2d}(q-1)$ für $q > 2$ bereits größer als der Grad von P_d ist, was in dem Produkt $P_{d+1} = P_d \cdot U_{d+1}$ eine Lücke entstehen läßt. Diese Lückenaussage gilt jedoch einzig und allein für die Produktfunktion U – sie vererbt sich nicht auf die Potenzen $h = U^{q^2-1}$ und $\tilde{\Delta} = U^{(q^2-1)(q-1)}$.

In Kapitel 3 werden schließlich einige Aussagen über die zu untersuchenden Potenzreihen bewiesen, die sich größtenteils aus den Ergebnissen der Berechnungen vermuten ließen. Sei $c_i \in A = \mathbb{F}_q[T]$ der i-te Koeffizient bezüglich der Variablen S einer der Potenzreihen U, h oder $\tilde{\Delta}$. Zunächst möchte man gern das Wachstum der Koeffizienten c_i kontrollieren können, d.h. eine Schranke für deren Grad (bezüglich T) angeben können. Man kann leicht zeigen, daß stets $\deg(c_i) \leq i$ gilt. Dies wirft die Frage auf, ob diese Abschätzung bereits „scharf" ist oder ob sie noch verbessert werden kann. Sie kann sicherlich dann nicht verbessert werden, wenn $\deg(c_i) = i$ für unendlich viele Indizes i gilt. Dies trifft tatsächlich zu. Im Falle der Produktfunktion U wird bewiesen, daß $\deg(c_i) = i$ genau dann gilt, wenn die Zahl i als Summe (beliebiger Länge) von q-Potenzen darstellbar ist, wobei die auftretenden Exponenten alle ungerade und paarweise verschieden sind. In [5] wird weiter bewiesen, daß für die Funktion h bzw. $\tilde{\Delta}$ Gleichheit genau dann gilt, wenn $i \equiv 0 \mod q$ bzw. $i \equiv 0, q \mod q^2$ ist. Also kann die obige Gradschranke nicht verbessert werden.

Die Länge $L(c_i)$ eines Koeffizienten c_i, d.h. die Anzahl seiner von Null verschiedenen Koeffizienten, ist durch diese Gradschranke auf $i+1$ beschränkt. Es gilt aber weiter folgende Kongruenzbedingung: Ist $c_i = \sum b_j T^j$, so gilt für jedes j mit $b_j \neq 0$ die Bedingung $j \equiv i \mod q-1$. Äquivalent hierzu ist die Aussage: $c_i(aT) = a^i\, c_i(T)$ für alle $a \in \mathbb{F}_q^*$. Damit kann die Länge eines jeden c_i höchstens noch $[\frac{i}{q-1}] + 1$ betragen, wobei $[\,.\,]$ der ganzzahlige Anteil sei. Allerdings wird auch diese Schranke i.A. noch weit unterschritten; es scheint $\lim_{i\to\infty} \frac{L(c_i)}{i} = 0$ zu gelten, möglicherweise mit Ausnahme des Falles $q = 2$, der im Übrigen in dieser Arbeit häufiger eine Sonderrolle spielt.

Weiterhin erfüllen die Funktionen U und $\tilde{\Delta}$ die folgende Kongruenzbedingung: Ist wieder c_i ein Koeffizient einer der beiden Funktionen, so kann $c_i \neq 0$ höchstens dann gelten, wenn $i \equiv 0, -1 \mod q$ ist. Dies beschränkt den Anteil nichttrivialer Koeffizienten eines Abschnitts dieser Funktionen bis zu einem festen Grad D auf höchstens $\frac{2}{q}$. Für $q > 2$ wurde im Fall der Produktfunktion U bereits in [7] bewiesen, daß dieser Anteil mit wachsendem D gegen Null strebt. Für $q = 2$ scheint dies nicht der Fall zu sein. (Dann hat auch die obige Kongruenzbedingung wenig Aussagekraft.) Anders als bei der Funktion U, die selbst bei Berücksichtigung ihrer bekannten Lücken und dem Verschwinden aller c_i mit $i \not\equiv 0, -1 \mod q$ noch sehr dünn besetzt ist, sind nur wenige zusätzliche Koeffizienten der Funktion $\tilde{\Delta}$ Null. Das Gleiche gilt auch für die Funktion h, die nicht einmal obige Kongruenzaussage erfüllt. Das Anfangssegment P_5 der Produktfunktion hat (für genügend großes q) etwa 2 300 nichttriviale Koeffizienten, obwohl sein Grad bereits in der Größenordnung q^9 liegt.

Die sicherlich interessanteste Aussage, die im Rahmen dieser Arbeit bewiesen wird, ist eine explizite Formel für diejenigen Koeffizienten der Produktfunktion U, deren Index eine Potenz von q mit ungeradem Exponenten ist. (Der Fall eines geraden Exponenten ist uninteressant – ist $q > 2$, so muß dieser Koeffizient Null sein, da er in eine Lücke der Potenzreihe U hineinfällt; ist $q = 2$, so verhält sich der Koeffizient nicht regelmäßig.) Die Formel lautet wie folgt: Ist u_l der beschriebene Koeffizient, wobei $l = q^m$ mit $m \in \mathbb{N}$ ungerade ist, so gilt

$$u_l \;=\; \sum_{i=0}^{m} \epsilon(i)\, T^{q^{m-i}}$$

mit

$$\epsilon(i) \;:=\; \begin{cases} +1 & \text{für } i \equiv 0,3 \mod 4, \\ -1 & \text{für } i \equiv 1,2 \mod 4. \end{cases}$$

Dieser Koeffizient ist also bis auf Vorzeichen von der Form $T + T^q + \cdots + T^{q^m}$.

Ähnliche Formeln sind auch in der Fällen der Funktionen h und $\tilde{\Delta}$ zu beobachten. Unter den Voraussetzungen $a \in \mathbb{N}$, $k \geq 2$ und $q > a + 1$ gilt für den Koeffizienten $\delta_{a \cdot q^k}$ der Diskriminantenfunktion $\tilde{\Delta}$ scheinbar eine geschlossene Formel, in der genau $2a + 1$ Terme vorkommen (die dann noch von a und k abhängen). Die zugehörigen Koeffizienten aus $\mathbb{F}_p^*$ sind allerdings nur unvollständig bekannt.

Schließlich sind im Anhang statistische Daten zu den Funktionen U_d, U, U^{-1}, h und $\tilde{\Delta}$ zusammengestellt.

Ich möchte mich bei Herrn Prof. Dr. E.-U. Gekeler für die interessante Themenstellung und die sehr gute Betreuung bei der Anfertigung meiner Diplomarbeit bedanken. Ebenso danke ich seinen Mitarbeitern Bodo Wack, Max Gebhardt und Ortwin Scheja für ihre Unterstützung. Schließlich gilt mein Dank Herrn Bartolomé López, dessen Formeln (2.5) und (2.6) mir sehr hilfreich waren, sowie meinen Eltern, die mein Studium finanziert haben.

Saarbrücken, im Dezember 1998 Michael Trautwein

Kapitel 1

Grundlagen

1.1 Notationen

- Im Folgenden sei $q = p^n$ stets eine Potenz der Primzahl p, $n \in \mathbb{N}$.
  Weiter seien
  $\mathbb{F}_q$ der endliche Körper mit q Elementen,
  $A = \mathbb{F}_q[T]$ der Polynomring in der Unbestimmten T über $\mathbb{F}_q$,
  $A[[S]]$ der Ring der formalen Potenzreihen in der Unbestimmten S über A.

- Potenzreihen $f \in A[[S]]$ werden meist in der Form

  $$f = \sum_{i \geq 0} f_i \, S^i$$

  dargestellt; hierbei sei für $i \geq 0$ stets

  $$f_i = f_i(T) \in A.$$

  Sei $k \in \mathbb{N}_0$. Die Aussage

  „k kommt als Exponent in f vor“

  bedeute, daß k in f mit nichttrivialem Koeffizienten vorkommt, daß also $f_k \neq 0$ gilt.

- Sei $f = \sum_{i \geq 0} f_i \, S^i \in A[S]$ ein Polynom. Für $f \neq 0$ sei dann der *Grad* von f sein Grad bezüglich der Variablen S:

  $$\deg(f) \;:=\; \deg_S(f) \;:=\; \max\,\{i \geq 0 \mid f_i \neq 0\}.$$

  Falls $\deg(f) \geq 1$ gilt, sei

  $$E(f) \;:=\; \min\,\{i \geq 1 \mid f_i \neq 0\}$$

der kleinste in f vorkommende von Null verschiedene Exponent. Schließlich sei für ein beliebiges Polynom f die *Länge* von f

$$L(f) \ := \ \#\{i \geq 0 \mid f_i \neq 0\}$$

die Anzahl seiner nichttrivialen Koeffizienten. Analog sei die Länge $L(f)$ auch für Polynome $f \in A = \mathbb{F}_q[T]$ definiert.

- Für $d \in \mathbb{N}$ sei S_d die Gruppe der Permutationen von $0, \ldots, d-1$. Für die Elemente $\sigma \in S_d$ benutzen wir die Schreibweise $\sigma = (\sigma(0), \ldots, \sigma(d-1))$. Das Signum einer Permutation wird mit $\epsilon(\sigma)$ bezeichnet.

- Wie üblich habe die leere Summe stets den Wert 0 und das leere Produkt den Wert 1.

- Für eine reelle Zahl x sei $[x]$ der ganzzahlige Anteil von x.

1.2 Invertierung von Potenzreihen

Sei R ein kommutativer Ring mit Eins. Eine formale Potenzreihe

$$f = \sum_{i \geq 0} f_i\, S^i \in R[[S]]$$

ist genau dann invertierbar, wenn das Absolutglied f_0 Einheit in R ist. In diesem Fall erhält man für die Inverse

$$f^{-1} := \sum_{i \geq 0} g_i\, S^i$$

durch Koeffizientenvergleich folgende Rekursionsformel:

$$\begin{aligned} g_0 &= f_0^{-1}, \\ g_i &= -f_0^{-1} \sum_{j=1}^{i} f_j\, g_{i-j} \quad \text{für } i \geq 1. \end{aligned} \tag{1.1}$$

Im Falle $R = A = \mathbb{F}_q[T]$ ist eine Potenzreihe $f = \sum_{i \geq 0} f_i\, S^i \in A[[S]]$ also genau dann invertierbar, wenn $f_0 \in \mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$ gilt. Bei fast allen in dieser Arbeit auftretenden Potenzreihen wird das Absolutglied Eins sein, so daß die Invertierbarkeit gesichert ist. Die Berechnung der ersten k Koeffizienten der Inversen erfordert dann $\frac{k(k+1)}{2}$ Multiplikationen in A.

1.3 Der Carlitz-Modul

Sei K ein Körper mit einem (nichttrivialen) Ringhomomorphismus $\varphi : A \to K$. Da die Einschränkung $\varphi|_{\mathbb{F}_q}$ injektiv ist, können wir $\mathbb{F}_q$ als Unterkörper von K auffassen. Sei weiter $\tau = X^q$ der Frobenius-Automorphismus (wir unterscheiden nicht zwischen Polynomen und polynomialen Abbildungen) und

$$K\{\tau\} \;:=\; \left\{ \sum_{i=0}^{n} a_i\, \tau^i \;\middle|\; a_i \in K \right\}$$

die Menge der $\mathbb{F}_q$-linearen Polynome über K, d.h. der Polynome $f \in K[X]$ mit $f(X+Y) = f(X) + f(Y)$ und $f(aX) = af(X)$ für alle $a \in \mathbb{F}_q$. Auf dieser sei die (nichtkommutative) Multiplikation $\circ$ durch Einsetzen (Komposition) definiert, oder alternativ: $\circ$ sei diejenige wohlbestimmte assoziative und distributive Multiplikation, die auf Konstanten aus K mit der Multiplikation in K übereinstimmt und der Kommutatorregel

$$\tau\, a = a^q\, \tau$$

für $a \in A$ genügt. Diese Festsetzung macht $K\{\tau\}$ zu einem (nichtkommutativen) Ring mit Einselement $\tau^0 = X$. Dieser Ring $K\{\tau\}$ heißt auch *getwisteter Polynomring in τ*.

In dieser Situation ist ein *Drinfeld-Modul* vom Rang r gegeben durch durch einen Homomorphismus von $\mathbb{F}_q$-Algebren

$$\begin{aligned} \phi :\; A &\longrightarrow K\{\tau\}, \\ a &\longmapsto \phi_a = \varphi(a)\, \tau^0 + \sum_{i=1}^{r} g_i\, \tau^i \end{aligned}$$

mit $g_i \in K$ und $g_r \neq 0$. Dieser liefert eine Modulstruktur auf der additiven Gruppe von K gemäß

$$a \cdot x \;:=\; \phi_a(x), \quad a \in A,\; x \in K.$$

Der Homomorphismus ϕ ist vollständig bestimmt durch ϕ_T, denn für ein beliebiges Polynom $a = \sum c_i\, T^i \in A$ ist

$$\phi_a \;=\; \phi_{\sum c_i\, T^i} \;=\; \sum c_i\, (\phi_T)^i,$$

wobei sich die Potenz $(\phi_T)^i$ auf die modifizierte Multiplikation $\circ$ von $K\{\tau\}$ bezieht.

Wenn auch der Ring $K\{\tau\}$ nichtkommutativ ist, so kommutieren darin doch jedenfalls die Bilder unter dem Homomorphismus ϕ der Elemente des kommutativen Rings A, d.h. es gilt für alle $a, b \in A$

$$\phi_a \circ \phi_b \;=\; \phi_b \circ \phi_a \;=\; \phi_{a \cdot b}.$$

Sei $K = \mathrm{Quot}(A) = \mathbb{F}_q(T)$ und K_∞ die Komplettierung von K „an der unendlichen Stelle", d.h. bezüglich des durch $|T| := q$ normierten Absolutbetrages $|\,.\,|$, der zur Gradbewertung $K \to \mathbb{Z} \cup \{-\infty\}$, $x \mapsto \deg(x)$ gehört. Diese Komplettierung ist explizit gegeben durch $K_\infty = \mathbb{F}_q((T^{-1}))$, den Körper der formalen Laurentreihen in T^{-1}. Sie entspricht dem Körper der reellen Zahlen im Fall der Charakteristik 0. Die Komplettierung C des algebraischen Abschlusses $\overline{K_\infty}$ bezüglich der eindeutigen Fortsetzung von $|\,.\,|$ ist glücklicherweise algebraisch abgeschlossen (Satz von Krasner) und kann mit dem Körper der komplexen Zahlen verglichen werden.

Ein A-*Gitter* in C sei nun ein A-Untermodul von C, der diskret ist, d.h. endlichen Durchschnitt mit jeder Kugel $B \subset C$ von endlichem Radius hat. Zu einem solchen Gitter Λ können wir die Gitterfunktion

$$e_\Lambda(z) \;:=\; z \prod_{\lambda \in \Lambda - \{0\}} (1 - \frac{z}{\lambda})$$

definieren. Aus der Funktion $e_\Lambda(z)$ läßt sich ein Drinfeld-Modul konstruieren. Des Weiteren besitzt $e_\Lambda(z)$ eine inverse Potenzreihe $\log_\Lambda(z)$ (bezüglich Komposition), was zu einer Bijektion zwischen Gittern in C und Drinfeld-Moduln über C führt.

Weiteres zu Drinfeld-Moduln findet man in [3], [4] und [6].

Im einfachsten Fall $K = \mathrm{Quot}(A)$, $\varphi : A \hookrightarrow K$ die Einbettung, ist der sogenannte *Carlitz-Modul* durch

$$\rho_T \;=\; T\,\tau^0 + \tau \;=\; TX + X^q$$

gegeben. Es handelt sich hierbei also um einen Drinfeld-Modul vom Rang 1.

Aus dem Ansatz $\rho_a = \sum_{i=0}^{d} l_i\, X^{q^i}$, $d = \deg(a)$ und der Beziehung $\rho_a \circ \rho_T = \rho_T \circ \rho_a$ erhalten wir für die Koeffizienten $l_i \in A$ von ρ_a die Rekursionsformel

$$\begin{aligned} l_0 &= a, \\ l_i &= \frac{l_{i-1}^q - l_{i-1}}{T^{q^i} - T}, \quad i \geq 1. \end{aligned} \tag{1.2}$$

Sei L das zum Carlitz-Modul gehörende Gitter. (L ist von der Form $L = \overline{\pi} A$ mit einem bis auf Konstanten aus $\mathbb{F}_q^*$ wohlbestimmten Element $\overline{\pi}$.) Dann entspricht die Funktion $t(z) := e_L^{-1}(\overline{\pi} z) = \overline{\pi}^{-1}\, e_A^{-1}(z)$ der klassischen Funktion $e^{2\pi i z}$.

Für $i \in \mathbb{N}_0$ definieren wir die folgenden A-wertigen arithmetischen Funktionen:

$$[\,i\,] \;:=\; T^{q^i} - T, \qquad D_i \;:=\; \prod_{j=1}^{i} [\,j\,]^{q^{i-j}}, \qquad L_i \;:=\; \prod_{j=1}^{i} [\,j\,].$$

Dann ist $[\,i\,]$ das Produkt aller normierten Primelemente von A, deren Grad i teilt, D_i das Produkt aller normierten Polynome vom Grad i aus A und L_i das kleinste gemeinsame Vielfache aller normierten Polynome vom Grad i aus A. Weiterhin gilt

$$e_L(z) \;=\; \sum_{i\geq 0} D_i^{-1}\, z^{q^i} \quad \text{und} \quad \log_L(z) \;=\; \sum_{i\geq 0} (-1)^i\, L_i^{-1}\, z^{q^i}.$$

Drinfeld-Moduln vom Rang 2 sind von der Form

$$\phi_T \;=\; T\,\tau^0 + g\,\tau + \Delta\,\tau^2.$$

Jedes zweidimensionale A-Gitter ist bis auf Skalierung von der Form $\Lambda = A\,z + A$, wobei z ein Element der „oberen Halbebene" $\Omega = C - K_\infty$ ist. Ist ϕ der zugehörige Drinfeld-Modul, so werden die Koeffizienten g und Δ zu Funktionen auf Ω.

Die Funktion $\Delta = \Delta(z)$ wird *Drinfeldsche Diskriminantenfunktion* genannt. Die Untersuchung dieser und einiger weiterer Funktionen ist Gegenstand der vorliegenden Arbeit.

1.4 Inverse a-te Kreisteilungspolynome

Definition 1.1. *Für $0 \neq a \in A$ sei das* inverse a-te Kreisteilungspolynom f_a *definiert durch*

$$f_a(X) \;:=\; \rho_a(X^{-1})\, X^{q^{\deg(a)}}.$$

Dabei sei ρ_a wie im vorigen Abschnitt im Zusammenhang mit dem Carlitz-Modul definiert.

Das Polynom f_a enthält also die Koeffizienten von ρ_a in umgekehrter Reihenfolge. Sei nun $d := \deg(a)$. Aus $\rho_a = \sum_{i=0}^{d} l_i\, X^{q^i}$ folgt

$$f_a \;=\; \sum_{i=0}^{d} l_i\, X^{q^d - q^i} \;=\; \sum_{i=0}^{d} l_i\, X^{q^i(q^{d-i}-1)},$$

wobei $q^{d-i} - 1$ von $q-1$ geteilt wird, d.h. f_a ist Polynom in X^{q-1}. Wir schreiben daher im Folgenden

$$S := X^{q-1}$$

und fassen f_a als Polynom in $A[X^{q-1}] = A[S]$ auf.

Wegen $\rho_a(X) = aX + O(X^q)$ gilt $\deg_X(f_a) = q^d - 1$ und entsprechend $\deg_S(f_a) = \frac{q^d-1}{q-1}$. Das Polynom f_a hat a als Leitkoeffizient und den Leitkoeffizienten von a als Absolutglied (konstanten Term). Es entspricht dem Polynom $1 - X^a$ $(a \in \mathbb{Z})$ im klassischen Fall.

Lemma 1.2. *Seien $a, b \in A$, a normiert, $d = \deg(a) > \deg(b) = d'$. Dann gelten die folgenden Beziehungen:*

(i)

$$f_{a+b} \;=\; f_a \;+\; X^{q^d - q^{d'}}\, f_b, \tag{1.3}$$

(ii)

$$f_{aT} \;=\; f_a^q \;+\; T X^{q^d(q-1)}\, f_a, \tag{1.4}$$

(iii)

$$\prod_{c \in \mathbb{F}_q} f_{a+c} \;=\; f_a^q \;-\; X^{(q^d-1)(q-1)}\, f_a. \tag{1.5}$$

Beweis.

(i)

$$\begin{aligned} f_{a+b} \;&=\; \rho_{a+b}(X^{-1})\, X^{q^{\deg(a+b)}} \;=\; \big(\rho_a(X^{-1}) \;+\; \rho_b(X^{-1})\big)\; X^{q^d} \\ &=\; f_a(X) \;+\; \rho_b(X^{-1})\, X^{q^d} \;=\; f_a(X) \;+\; X^{q^d - q^{d'}}\, f_b(X). \end{aligned}$$

(ii)

$$\begin{aligned} \rho_{aT} \;&=\; \rho_T\, \rho_a \;=\; (T+\tau)\,(\sum_{i \geq 0} l_i\, \tau^i) \;=\; T \sum_{i \geq 0} l_i\, \tau^i \;+\; \tau \sum_{i \geq 0} l_i\, \tau^i \\ &=\; T\rho_a \;+\; \sum_{i \geq 0} l_i^q\, \tau^{i+1} \;=\; T\rho_a \;+\; \rho_a^q. \end{aligned}$$

Also gilt

$$\begin{aligned} f_{aT} \;&=\; \rho_{aT}(X^{-1})\, X^{q^{d+1}} \;=\; T\rho_a(X^{-1})\, X^{q^{d+1}} \;+\; \rho_a(X^{-1})^q\, X^{q^{d+1}} \\ &=\; T\, X^{q^{d+1} - q^d}\, \rho_a(X^{-1})\, X^{q^d} \;+\; \Big(\rho_a(X^{-1})\, X^{q^d}\Big)^q \\ &=\; T\, X^{q^d(q-1)}\, f_a(X) \;+\; f_a(X)^q. \end{aligned}$$

(iii) Zunächst gilt

$$\prod_{c \in \mathbb{F}_q} \rho_{a+c} \;=\; \prod_{c \in \mathbb{F}_q} (\rho_a + \rho_c) \;=\; \prod_{c \in \mathbb{F}_q} (\rho_a + cX) \;=\; -X^q \prod_{c \in \mathbb{F}_q} \Big(-\frac{\rho_a}{X} - c\Big).$$

Da $\mathbb{F}_q$ Zerfällungskörper des Polynoms $X^q - X$ über $\mathbb{F}_p$ ist und gerade aus sämtlichen Nullstellen dieses Polynoms besteht, gilt

$$X^q - X \;=\; \prod_{c \in \mathbb{F}_q} (X - c).$$

Wir erhalten also weiter

$$\prod_{c \in \mathbb{F}_q} \rho_{a+c} \;=\; -X^q \left[\left(-\frac{\rho_a}{X}\right)^q - \left(-\frac{\rho_a}{X}\right) \right] \;=\; \rho_a^q \;-\; \rho_a \, X^{q-1}.$$

Somit gilt schließlich

$$\begin{aligned}
\prod_{c \in \mathbb{F}_q} f_{a+c} \;&=\; \prod_{c \in \mathbb{F}_q} \left(\rho_{a+c}(X^{-1}) \, X^{q^d}\right) \;=\; \left(\prod_{c \in \mathbb{F}_q} \rho_{a+c}(X^{-1}) \right) X^{q^{d+1}} \\
&=\; \left(\rho_a(X^{-1})^q \;-\; \rho_a(X^{-1}) \, X^{1-q}\right) X^{q^{d+1}} \\
&=\; \rho_a(X^{-1})^q \, X^{q^{d+1}} \;-\; \rho_a(X^{-1}) \, X^{q^{d+1}-q+1} \\
&=\; f_a^q \;-\; f_a \cdot X^{q^{d+1}-q+1-q^d} \\
&=\; f_a^q \;-\; X^{(q^d-1)(q-1)} \, f_a.
\end{aligned}$$

□

Von besonderer Bedeutung sind nun die Polynome der Form f_{T^d}, denn von diesen ausgehend kann man mit Hilfe von (1.3) zu beliebigem vorgegebenem $a \in A$ das entsprechende Polynom f_a konstruieren. Diese Methode ist günstiger als die Konstruktion von f_a nach Definition 1.1, denn hierzu müßte zunächst ρ_a nach (1.2) ausgewertet werden.

Der folgende Satz gibt uns die Möglichkeit, f_{T^d} unabhängig von der allgemeinen Definition von f_a zu berechnen.

Satz 1.3. *Für $d \in \mathbb{N}_0$ gilt*

$$f_{T^d} \;=\; \sum_{i=0}^{d} c_{d,i} \cdot S^{D(d,i)} \tag{1.6}$$

mit

$$D(d,i) \;:=\; \frac{q^d - q^{d-i}}{q-1} \;=\; \sum_{j=d-i}^{d-1} q^j, \qquad 0 \le i \le d. \tag{1.7}$$

Die Koeffizienten $c_{d,i} \in A$ genügen der Rekursion

$$\begin{aligned}
c_{d,0} \;&=\; 1, \\
c_{d+1,i} \;&=\; c_{d,i}^q \;+\; T \cdot c_{d,i-1}, \qquad 1 \le i \le d+1.
\end{aligned} \tag{1.8}$$

Hierbei gelte die Konvention $c_{d,i} := 0$ für $i < 0$ oder $i > d$.

Beweis. Vollständige Induktion nach d.
Für $d = 0$ gilt wie behauptet

$$f_1 \;=\; 1 \;=\; c_{0,0} \cdot S^{D(0,0)}.$$

Sei nun unsere Behauptung für d erfüllt. Dann gilt nach (1.4)

$$\begin{aligned}
f_{T^{d+1}} &= f_{T^d \cdot T} \;=\; f_{T^d}^q + T S^{q^d} f_{T^d} \\
&= \sum_{i=0}^{d} c_{d,i}^q \cdot S^{q \cdot D(d,i)} \;+\; \sum_{i=0}^{d} T \cdot c_{d,i} \cdot S^{q^d + D(d,i)} \\
&= \sum_{i=0}^{d} c_{d,i}^q \cdot S^{D(d+1,i)} \;+\; \sum_{i=0}^{d} T \cdot c_{d,i} \cdot S^{D(d+1,i+1)} \\
&= \sum_{i=0}^{d} c_{d,i}^q \cdot S^{D(d+1,i)} \;+\; \sum_{j=1}^{d+1} T \cdot c_{d,j-1} \cdot S^{D(d+1,j)} \\
&= \sum_{i=0}^{d+1} c_{d,i}^q \cdot S^{D(d+1,i)} \;+\; \sum_{j=0}^{d+1} T \cdot c_{d,j-1} \cdot S^{D(d+1,j)} \\
&= \sum_{i=0}^{d+1} (c_{d,i}^q \;+\; T \cdot c_{d,i-1})\, S^{D(d+1,i)}.
\end{aligned}$$

□

Bemerkung 1.4.

(i) Die Rekursion (1.8) liefert für beliebiges d

$$c_{d,1} \;=\; \sum_{i=0}^{d-1} T^{q^i}, \qquad c_{d,d-1} \;=\; \sum_{i=0}^{d-1} T^{iq+d-i-1}, \qquad c_{d,d} \;=\; T^d.$$

(ii) Aus der Rekursion (1.8) folgt weiterhin, daß alle Koeffizienten von $c_{d,i} \in \mathbb{F}_q[T]$ sogar aus dem Primkörper $\mathbb{F}_p$ von $\mathbb{F}_q$ stammen, d.h.

$$f_{T^d} \in \mathbb{F}_p[T][S], \quad p = \mathrm{char}(\mathbb{F}_q),$$

denn die Rekursion beginnt mit dem Wert 1, und $\mathbb{F}_p$ ist als Körper selbstverständlich abgeschlossen unter arithmetischen Operationen.

Dies gilt aber für beliebiges f_a im Allgemeinen nicht, man betrachte etwa $f_c = c$ für $c \in \mathbb{F}_q - \mathbb{F}_p$, q nicht prim.

(iii) Man hätte die Rekursionsformel (1.8) auch erhalten können, indem man in der Gleichung

$$\rho_{T^d} \;=\; \rho_{T^{d-1}} \circ \rho_T$$

einen Koeffizientenvergleich durchführt. Analog erhält man aus der Identität

$$\rho_{T^d} \;=\; \rho_T \circ \rho_{T^{d-1}}$$

die weitere Rekursion

$$c_{d+1,i} \;=\; c_{d,i} \;+\; T^{q^{d-i+1}} \cdot c_{d,i-1}. \tag{1.9}$$

(iv) Aus (1.6) und $f_{T^d}(X) = \rho_{T^d}(X^{-1})\, X^{q^d}$ folgt

$$\rho_{T^d} \;=\; \sum_{i=0}^{d} c_{d,d-i}\, X^{q^i}. \tag{1.10}$$

Beispiel 1.5.

$$\begin{aligned}
f_1 &= 1,\\
f_T &= 1 \;+\; TS,\\
f_{T^2} &= 1 \;+\; (T+T^q)\, S^q \;+\; T^2\, S^{q+1},\\
f_{T^3} &= 1 \;+\; (T+T^q+T^{q^2})\, S^{q^2} \;+\; (T^2+T^{q+1}+T^{2q})\, S^{q^2+q} \;+\; T^3\, S^{q^2+q+1}.
\end{aligned}$$

Korollar 1.6. *Für $d, i \in \mathbb{N}_0$, $0 \le i \le d$ gilt*

$$\deg(c_{d,i}) \;=\; i \cdot q^{d-i}.$$

Beweis. Vollständige Induktion nach d.
Für $d = 0$ ist die Aussage wegen der Voraussetzung $0 \le i \le d$ nur für $i = 0$ zu zeigen. In diesem Fall gilt

$$\deg(c_{0,0}) \;=\; \deg(1) \;=\; 0.$$

Unter der Annahme, unsere Behauptung sei für $d \ge 0$ erfüllt, haben wir

$$\deg(c_{d+1,i}) \;=\; i \cdot q^{d+1-i}$$

für $i = 0, \ldots, d+1$ nachzuweisen.

Im Falle $i = 0$ ergibt sich dies sofort aus $c_{d+1,0} = 1$, ebenso im Falle $i = d+1$ wegen $c_{d+1,d+1} = T^{d+1}$. Sei nun also $0 < i < d+1$. Dann gilt nach (1.8)

$$c_{d+1,i} \;=\; c_{d,i}^{q} \;+\; T \cdot c_{d,i-1},$$

mit

$$\deg(c_{d,i}^{q}) \;=\; i \cdot q^{d+1-i} \qquad \text{und} \qquad \deg(T \cdot c_{d,i-1}) \;=\; (i-1)\, q^{d+1-i} + 1.$$

Wegen $d+1 > i$ ist $q^{d+1-i} > 1$ und somit

$$i \cdot q^{d+1-i} \;>\; (i-1)\, q^{d+1-i} + 1.$$

Hieraus folgt, daß

$$\deg(c_{d+1,i}) \;=\; i \cdot q^{d+1-i}$$

gilt. □

Auf das folgende Korollar werden wir in Kapitel 3 zurückgreifen.

Korollar 1.7. *Für $d \in \mathbb{N}$, $0 \leq i \leq d$ gilt*

(i)

$$\deg(c_{d,i}) \;\leq\; D(d,i),$$

(ii)

$$\deg(c_{d,i}) = D(d,i) \quad \Leftrightarrow \quad i \in \{0,1\}.$$

(Im 1. Fall ist $\deg(c_{d,0}) = D(d,0) = 0$, *im 2. Fall* $\deg(c_{d,1}) = D(d,1) = q^{d-1}$*.)*

Beweis. Nach Korollar 1.6 gilt

$$D(d,i) \,-\, \deg(c_{d,i}) \;=\; \sum_{j=d-i}^{d-1} q^{j} \;-\; i\, q^{d-i} \;=:\; r.$$

(i) Wegen $q^j \geq q^{d-i}$ für $j = d-i, \ldots, d-1$ ist $r \geq 0$.

(ii) Für $i \in \{0,1\}$ gilt offensichtlich $r = 0$; für $i \geq 2$ ist $r > 0$ wegen $q^j > q^{d-i}$ für $j = d-i+1, \ldots, d-1$.

□

1.5 Ziel der Arbeit

Aufbauend auf den inversen Kreisteilungspolynomen f_a definieren wir die folgenden Potenzreihen aus $A[[S]]$:

Definition 1.8.

$$\begin{aligned} U &:= \prod_{a\in A \text{ normiert}} f_a, \\ h &:= U^{q^2-1}, \\ \tilde{\Delta} &:= U^{(q^2-1)(q-1)}, \\ \Delta &:= -S\cdot\tilde{\Delta}. \end{aligned}$$

Wir nennen U die Produktfunktion *und $\tilde{\Delta}$ bzw. Δ* Diskriminantenfunktion. *Für den gesamten Rest der Arbeit seien die Koeffizienten dieser Potenzreihen wie folgt bezeichnet:*

$$U = \sum_{i\geq 0} u_i\,S^i, \qquad h = \sum_{i\geq 0} h_i\,S^i, \qquad \tilde{\Delta} = \sum_{i\geq 0} \delta_i\,S^i.$$

Wollen wir ausdrücken, daß eine Aussage sowohl für die Koeffizienten u_i als auch für h_i als auch für δ_i gilt, so verwenden wir meist die Bezeichung c_i.

Wir fassen dabei U, h, $\tilde{\Delta}$ und Δ als *formale* Potenzreihen auf, d.h. Konvergenzfragen werden bei unseren Betrachtungen keine Rolle spielen.

Wir haben bereits in Abschnitt 1.3 das Symbol Δ für die Drinfeldsche Diskriminantenfunktion verwendet, die dort im Zusammenhang mit Drinfeld-Moduln vom Rang 2 auftrat. Dieses ist aus dem folgenden Grund gerechtfertigt:

Sei wieder $\Omega = C - K_\infty$ die „obere Halbebene“. Drinfeld-Moduln vom Rang 2 sind, wie in Abschnitt 1.3 geschildert, von der Form

$$\phi_T = T\,\tau^0 + g(z)\,\tau + \Delta(z)\,\tau^2,$$

wobei die Funktionen g und Δ von der Wahl des A-Gitters $\Lambda = A\,z + A$, $z\in\Omega$, abhängen. Man führt nun in Analogie zu klassischen Modulformen auf der komplexen oberen Halbebene den Begriff der *Drinfeldschen Modulform* $f:\Omega\to C$ auf Ω vom Gewicht $k\in\mathbb{Z}$ und Typ $m\in\mathbb{Z}/(q-1)\mathbb{Z}$ ein. Hierzu vergleiche man etwa [4]. Einiges zu klassischen Modulformen findet man in [1] und [9].

Der C-Vektorraum M aller Modulformen auf Ω wird dann als Polynomring $C[g,h]$ von den Funktionen g und h erzeugt, wobei $h = P_{q+1,1}$ als *Poincaré-Reihe* definiert ist. Der Untervektorraum M^0 aller Modulformen vom Typ 0 stimmt mit $C[g,\Delta]$ überein. Die Funktionen g und Δ sind in obigem Sinne Modulformen vom Typ 0 und Gewicht $q-1$ bzw. q^2-1; h ist eine Modulform vom Typ 1 und Gewicht $q+1$.

Man kann nun zeigen, daß die Funktion Δ bis auf einen konstanten Faktor mit h^{q-1} übereinstimmt. (Weiterhin gilt der Zusammenhang, daß $h = \partial g$ bezüglich eines geeigneten Differentialoperators ∂ ist, so daß man drei verschiedene Charakterisierungen der Funktion h besitzt.) Es kann weiter die Beziehung

$$\overline{\pi}^{1-q^2}\,\Delta(z) \;=\; -t^{q-1} \prod_{a\in A \text{ normiert}} f_a(t)^{(q^2-1)(q-1)} \tag{1.11}$$

gezeigt werden, wobei die Funktion $t(z) = e_L^{-1}(\overline{\pi}z)$ die Rolle eines uniformisierenden Parameters ähnlich wie die Funktion $q(z) = e^{2\pi iz}$ im klassischen Fall spielt. Dabei sei $L = \overline{\pi}A$ das zum Carlitz-Modul gehörende Gitter. Die Identität (1.11) entspricht der klassischen Formel von Jacobi. Ersetzen wir t durch die Unbestimmte X und schreiben wie bisher $S = X^{q-1}$, so nimmt (1.11) die Form

$$\overline{\pi}^{1-q^2}\,\Delta(z) \;=\; -S \prod_{a\in A \text{ normiert}} f_a(S)^{(q^2-1)(q-1)} \;=\; -S\cdot\tilde{\Delta}$$

an. Somit stimmt die Funktion Δ, wie sie in 1.8 definiert ist, bis auf $\overline{\pi}^{1-q^2}$ mit der in Abschnitt 1.3 betrachteten Funktion Δ überein.

Ziel dieser Arbeit ist es nun, möglichst viel über die Potenzreihen aus Definition 1.8 herauszufinden, indem einerseits ein Computerprogramm zur Berechnung numerischer Daten entwickelt wird und andererseits dabei auffallende Beobachtungen bewiesen werden. Im nächsten Kapitel wollen wir uns mit der Entwicklung von Algorithmen zur Berechnung obiger Potenzreihen beschäftigen, während sich Kapitel 3 dem Beweisen einiger Eigenschaften widmet.

Kapitel 2

Berechnung der Funktionen U, h und $\tilde{\Delta}$

2.1 Vorbemerkungen

Wir wollen uns zunächst mit der Berechnung der Produktfunktion U beschäftigen, denn ist U bekannt, so stellt die Berechnung der übrigen Funktionen, die im Wesentlichen Potenzen von U sind, aus algorithmischer Sicht kein neues Problem mehr dar. Wir werden jedoch sehen, daß sich einige charakteristische Eigenschaften der Produktfunktion U (Lückenhaftigkeit, gewisse Kongruenzbedingungen) nicht zwangsläufig auf ihre Potenzen vererben, so daß jede der Funktionen U, h und $\tilde{\Delta}$ vom theoretischen Standpunkt her von eigenem Interesse ist.

Da U nach Definition eine formale Potenzreihe mit unendlich vielen nichttrivialen, d.h. von Null verschiedenen Koeffizienten ist, kann das Vorhaben der „Berechnung" von U nur bedeuten:

> Berechne möglichst viele Koeffizienten von U, etwa den Anfangsabschnitt von U bis zu einem festen Grad $D \in \mathbb{N}$.

Die Potenzreihe U ist zwar als unendliches Produkt definiert, jedoch können zu jedem festen Koeffizienten von U jeweils nur endlich viele Polynome f_a beitragen, so daß prinzipiell jeder Koeffizient von U berechenbar ist. Genauer gilt:

Zum i-ten Koeffizienten u_i von U können nur diejenigen normierten Polynome f_a beitragen, die $q^{\deg(a)-1} \leq i$ erfüllen.

Denn: Sei $a \in A$ normiert, $d := \deg(a) > 1$. Dann ist ρ_a von der Form

$$\rho_a = \sum_{i=0}^{d} l_i \, X^{q^i} \quad \text{mit } l_i \in \mathbb{F}_q, \; l_d = 1.$$

Somit gilt

$$\begin{aligned} f_a &= \sum_{i=0}^{d} l_i \, X^{q^d - q^i} \\ &= 1 + l_{d-1} \, X^{q^d - q^{d-1}} + O(X^{q^d - q^{d-2}}) \\ &= 1 + l_{d-1} \, S^{q^{d-1}} + O(S^{q^{d-1} + q^{d-2}}). \end{aligned}$$

Also ist $E(f_a) = q^{d-1}$, woraus folgt, daß f_a nur zu Termen u_i mit $q^{d-1} \leq i$ beitragen kann.

Durch die folgende Definition zerlegen wir das Problem der Berechnung von U in endliche Teilprobleme.

Definition 2.1. *Für $d \in \mathbb{N}_0$ sei*

$$U_d \quad := \prod_{\substack{a \in A \text{ normiert} \\ \deg(a) = d}} f_a \quad \in \ A[S].$$

Es gilt also $U = \prod_{i=0}^{\infty} U_i$. Da es genau q^d normierte Polynome des Grades d über $\mathbb{F}_q$ gibt und f_a für $\deg(a) = d$ den Grad $\frac{q^d - 1}{q-1}$ hat, erhalten wir

$$\deg(U_d) \;=\; q^d \, \frac{q^d - 1}{q - 1},$$

d.h. die Grade der Teilprodukte U_d wachsen exponentiell mit d.

Beispiel 2.2.

$$\begin{aligned} U_0 &= 1, \\ U_1 &= 1 - S^{q-1} + (T^q - T) \, S^q. \end{aligned}$$

Statistische Daten zu einigen weiteren U_d findet man im Anhang.

Es wäre im Prinzip möglich, U_d nach obiger Definition berechnen, d.h. man hätte sämtliche q^d normierten Polynome a vom Grad d aus A zu durchlaufen, daraus jeweils die entsprechenden Polynome f_a zu konstruieren und all diese zu multiplizieren. Dieses Vorgehen wäre aber an Ineffizienz kaum zu überbieten. Wir werden hierfür bessere Methoden herleiten, wobei aber noch zu klären sein wird, ob die Berechnung eines Anfangssegments der Potenzreihe U überhaupt die Berechnung solcher Teilprodukte U_d erfordert, oder ob es eventuell einen aus algorithmischer Sicht „kürzeren“ Weg gibt.

Das Produkt der ersten d Polynome U_i wollen wir mit P_d bezeichnen:

Definition 2.3. *Für $d \in \mathbb{N}_0$ sei*

$$P_d \;:=\; \prod_{i=0}^{d} U_i \;=\; \prod_{i=1}^{d} U_i \quad \in \; A[S].$$

Der Grad von P_d beträgt

$$\deg(P_d) \;=\; \sum_{i=0}^{d} \deg(U_i) \;=\; \sum_{i=0}^{d} q^i \,\frac{q^i-1}{q-1} \;=\; \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)}, \tag{2.1}$$

d.h. er liegt in der Größenordnung q^{2d-1}.

Wir interessieren uns nun dafür, bis zu welchem Grad das Polynom P_d mit der Potenzreihe U übereinstimmt. Zunächst gilt

$$P_{d+1} \;\equiv\; P_d \mod S^{E(U_{d+1})},$$

d.h. P_{d+1} und P_d stimmen bis zum Grad $E(U_{d+1})-1$ überein, denn in der Gleichung

$$P_{d+1} \;=\; P_d \cdot U_{d+1}$$

kann U_{d+1} nur zu Termen des Grades $\geq E(U_{d+1})$ beitragen. Es ist bereits zu vermuten, daß $E(U_d)$ mit d streng monoton wächst; wir werden dies in Lemma 2.11 zeigen. In diesem Fall würde P_d nicht nur mit P_{d+1}, sondern sogar mit U bis zum Grad $E(U_{d+1})-1$ übereinstimmen. Es wäre also des Weiteren wünschenswert, $E(U_{d+1})$ zu kennen. Sollte insbesondere zusätzlich stets $E(U_{d+1}) > \deg(P_d)$ gelten – wir werden sehen, daß dies für $q \geq 3$ der Fall ist – so hätten wir insgesamt, daß P_d vollständig mit dem Anfangsabschnitt der Potenzreihe U bis zum Grad $\deg(P_d)$ übereinstimmt. Dies wäre im Hinblick auf eine effiziente Berechnung von U günstig, da sich auf diese Weise keine „Verluste“ ergeben.

Wir wollen uns also im nächsten Abschnitt neben der Entwicklung von Formeln zur effizienten Berechnung von U mit den hier aufgeworfenen Fragen beschäftigen.

2.2 Formeln zur Berechnung von U

Definition 2.4. *Sei $d \in \mathbb{N}_0$. Analog zu den Definitionen von U_d und P_d seien V_d und Q_d definiert durch*

$$\begin{aligned} V_d &:= \prod_{\substack{a \in A \text{ normiert} \\ \deg(a)=d}} \rho_a \quad \in A[X], \\ Q_d &:= \prod_{i=0}^{d} V_i \qquad \in A[X]. \end{aligned}$$

Weiterhin setzen wir

$$\begin{aligned} H_{d,-1} &:= f_{T^d}, \\ H_{d,i} &:= \prod_{(c_0,\ldots,c_i) \in \mathbb{F}_q^{i+1}} f_{T^d + c_i T^i + \cdots + c_0} \quad \in A[S] \quad \textit{für} \quad 0 \le i \le d-1, \end{aligned}$$

sowie

$$\begin{aligned} G_{d,-1} &:= \rho_{T^d}, \\ G_{d,i} &:= \prod_{(c_0,\ldots,c_i) \in \mathbb{F}_q^{i+1}} \rho_{T^d + c_i T^i + \cdots + c_0} \quad \in A[X] \quad \textit{für} \quad 0 \le i \le d-1. \end{aligned}$$

Es gilt also $U_d = H_{d,d-1}$ und $V_d = G_{d,d-1}$. Für die Grade obiger Polynome gilt

$$\deg_X(V_d) = q^{2d}, \qquad \deg_X(Q_d) = \frac{q^{2d+2}-1}{q^2-1},$$

$$\deg_S(H_{d,i}) = q^{i+1}\,\frac{q^d-1}{q-1}, \qquad \deg_X(G_{d,i}) = q^{d+i+1}.$$

Lemma 2.5. *Seien $d \in \mathbb{N}_0$ und $-1 \le i \le d$. Betrachten wir alle folgenden Polynome als solche in der Variablen X, so gelten die Beziehungen*

(i)

$$H_{d,i}(X) = G_{d,i}(X^{-1})\,X^{q^{d+i+1}} \quad \textit{bzw.} \quad G_{d,i}(X) = H_{d,i}(X^{-1})\,X^{q^{d+i+1}}, \tag{2.2}$$

(ii)

$$P_d(X) = Q_d(X^{-1})\,X^{\frac{q^{2d+2}-1}{q^2-1}} \quad \textit{bzw.} \quad Q_d(X) = P_d(X^{-1})\,X^{\frac{q^{2d+2}-1}{q^2-1}}. \tag{2.3}$$

Beweis.

(i)

$$\begin{aligned} H_{d,i}(X) &= \prod_{A \ni a = T^d + c_i T^i + \cdots + c_0} f_a(X) = \prod \left(\rho_a(X^{-1})\, X^{q^d}\right) \\ &= \left(\prod \rho_a(X^{-1})\right) \cdot (X^{q^d})^{q^{i+1}} = G_{d,i}(X^{-1})\, X^{q^{d+i+1}}. \end{aligned}$$

(ii) Nach (i) gilt

$$\begin{aligned} P_d(X) &= \prod_{i=0}^{d} U_i(X) = \prod_{i=0}^{d} \left(V_i(X^{-1})\, X^{q^{2i}}\right) = \prod_{i=0}^{d} V_i(X^{-1}) \cdot \prod_{i=0}^{d} X^{q^{2i}} \\ &= Q_d(X^{-1}) \cdot X^{\sum_{i=0}^{d} q^{2i}} = Q_d(X^{-1})\, X^{\frac{q^{2d+2}-1}{q^2-1}}. \end{aligned}$$

Für die zweiten Formeln ersetze man jeweils X durch X^{-1}. □

Wir wollen uns der Frage nach möglichst effizienten Berechnungsmethoden für die Polynome P_d zuwenden. Die folgenden Aussagen 2.6, 2.7, 2.8 und 2.10 wurden von Bartolomé López bewiesen. Die hier aufgeführten Beweise sind Ausformulierungen der Beweise aus [7].

Betrachten wir die folgenden rekursiv definierten Operatoren β_k :

$$\begin{aligned} \gamma(Y, Z) &:= Y^q - Y Z^{q-1}, \\ \beta_1(X_1, X_0) &:= \gamma(X_1, X_0), \\ \beta_k(X_k, X_{k-1}, \ldots, X_0) &:= \gamma(\beta_{k-1}(X_k, X_{k-2}, \ldots, X_0), \beta_{k-1}(X_{k-1}, X_{k-2}, \ldots, X_0)). \end{aligned}$$

Man sieht durch einfache Induktion nach k, daß diese $\mathbb{F}_q$-linear im ersten Argument sind:

Lemma 2.6. *Für $c \in \mathbb{F}_q$ und $k \geq 1$ gilt*

$$\beta_k(Y + cZ, Y_{k-1}, \ldots, Y_0) = \beta_k(Y, Y_{k-1}, \ldots, Y_0) + c\, \beta_k(Z, Y_{k-1}, \ldots, Y_0).$$

Beweis. Induktion nach k.
Für $k = 1$ haben wir

$$\begin{aligned} \beta_1(Y + cZ, Y_0) &= \gamma(Y + cZ, Y_0) = (Y + cZ)^q - (Y + cZ) Y_0^{q-1} \\ &= Y^q - Y Y_0^{q-1} + cZ^q - cZ Y_0^{q-1} = \gamma(Y, Y_0) + c\,\gamma(Z, Y_0) \\ &= \beta_1(Y, Y_0) + c\, \beta_1(Z, Y_0). \end{aligned}$$

Sei die Behauptung für k erfüllt. Dann gilt

$$\begin{aligned}
&\beta_{k+1}(Y+cZ, Y_k, \ldots, Y_0)\\
&= \gamma(\beta_k(Y+cZ, Y_{k-1}, \ldots, Y_0), \beta_k(Y_k, \ldots, Y_0))\\
&= \beta_k(Y+cZ, Y_{k-1}, \ldots, Y_0)^q - \beta_k(Y+cZ, Y_{k-1}, \ldots, Y_0)\, \beta_k(Y_k, \ldots, Y_0)^{q-1}\\
&= \beta_k(Y, Y_{k-1}, \ldots, Y_0)^q + c\, \beta_k(Z, Y_{k-1}, \ldots, Y_0)^q\\
&\quad - \beta_k(Y, Y_{k-1}, \ldots, Y_0)\, \beta_k(Y_k, \ldots, Y_0)^{q-1} - c\, \beta_k(Z, Y_{k-1}, \ldots, Y_0)\, \beta_k(Y_k, \ldots, Y_0)^{q-1}\\
&= \gamma(\beta_k(Y, Y_k, \ldots, Y_0), \beta_k(Y_k, \ldots, Y_0)) + c\, \gamma(\beta_k(Z, Y_{k-1}, \ldots, Y_0), \beta_k(Y_k, \ldots, Y_0))\\
&= \beta_{k+1}(Y, Y_k, \ldots, Y_0) + c\, \beta_{k+1}(Z, Y_k, \ldots, Y_0).
\end{aligned}$$

□

Weiterhin gilt das folgende

Lemma 2.7. *Sei* $b = T^d + c_{d-1}T^{d-1} + \cdots + c_{i+1}T^{i+1} \in A$. *Dann gilt*

$$\prod_{(c_0,\ldots,c_i)\in\mathbb{F}_q^{i+1}} \rho_{b+c_iT^i+\cdots+c_0} = \beta_{i+1}(\rho_b, \rho_{T^i}, \ldots, \rho_1).$$

Beweis. Induktion nach i.
Für $i = 0$ haben wir zu zeigen:

$$\prod_{c_0\in\mathbb{F}_q} \rho_{b+c_0} = \beta_1(\rho_b, \rho_1).$$

Im Beweis von Lemma 1.2 (iii) haben wir bereits gesehen, daß

$$\prod_{c_0\in\mathbb{F}_q} \rho_{b+c_0} = \rho_b^{q-1} - \rho_b\, X^{q-1}$$

gilt. Die rechte Seite ist gegeben durch

$$\beta_1(\rho_b, \rho_1) = \gamma(\rho_b, X) = \rho_b^{q-1} - \rho_b\, X^{q-1}.$$

Sei also die Behauptung für $i-1$ erfüllt. Dann gilt

$$\begin{aligned}
\prod_{(c_0,\ldots,c_i)\in\mathbb{F}_q^{i+1}} \rho_{b+c_iT^i+\cdots+c_0} &= \prod_{c_i\in\mathbb{F}_q} \left(\prod_{(c_0,\ldots,c_{i-1})\in\mathbb{F}_q^i} \rho_{b+c_iT^i+\cdots+c_0} \right)\\
= \prod_{c_i\in\mathbb{F}_q} \beta_i(\rho_{b+c_iT^i}, \rho_{T^{i-1}}, \ldots, \rho_1) &= \prod_{c_i\in\mathbb{F}_q} \beta_i(\rho_b + c_i\, \rho_{T^i}, \rho_{T^{i-1}}, \ldots, \rho_1).
\end{aligned}$$

Das letzte Produkt ist nach Lemma 2.6 gleich

$$\prod_{c_i \in \mathbb{F}_q} (\beta_i(\rho_b, \rho_{T^{i-1}}, \ldots, \rho_1) \; + \; c_i \, \beta_i(\rho_{T^i}, \rho_{T^{i-1}}, \ldots, \rho_1)).$$

Hierfür erhalten wir wiederum analog zum Beweis von Lemma 1.2 (iii)

$$\begin{aligned} \beta_i(\rho_b, \rho_{T^{i-1}}, \ldots, \rho_1)^q \; - \; \beta_i(\rho_b, \rho_{T^{i-1}}, \ldots, \rho_1) \, \beta_i(\rho_{T^i}, \rho_{T^{i-1}}, \ldots, \rho_1)^{q-1} \\ = \; \beta_{i+1}(\rho_b, \rho_{T^i}, \ldots, \rho_1). \end{aligned}$$

□

Korollar 2.8. *Für $d \in \mathbb{N}, \; 0 \leq i \leq d-1$ gilt*

(i)

$$G_{d,i} \; = \; G_{d,i-1}^q \; - \; G_{d,i-1} \, G_{i,i-1}^{q-1}, \tag{2.4}$$

(ii)

$$H_{d,i} \; = \; H_{d,i-1}^q \; - \; H_{d,i-1} \, H_{i,i-1}^{q-1} \, S^{q^i(q^d - q^i)}. \tag{2.5}$$

Beweis.

(i) Setzen wir in Lemma 2.7

$$c_{i+1} \; := \; c_{i+2} \; := \; \ldots \; := \; c_{d-1} \; := \; 0,$$

so folgt

$$\begin{aligned} G_{d,i} \; &= \prod_{(c_0,\ldots,c_i) \in \mathbb{F}_q} \rho_{T^d + c_i T^i + \cdots + c_0} \\ &= \; \beta_{i+1}(\rho_{T^d}, \rho_{T^i}, \ldots, \rho_1) \\ &= \; \gamma(\beta_i(\rho_{T^d}, \rho_{T^{i-1}}, \ldots, \rho_1), \beta_i(\rho_{T^i}, \ldots, \rho_1)) \\ &= \; \beta_i(\rho_{T^d}, \rho_{T^{i-1}}, \ldots, \rho_1)^q \; - \; \beta_i(\rho_{T^d}, \rho_{T^{i-1}}, \ldots, \rho_1) \, \beta_i(\rho_{T^i}, \ldots, \rho_1)^{q-1} \\ &= \; G_{d,i-1}^q \; - \; G_{d,i} \, G_{i,i-1}^{q-1}. \end{aligned}$$

(ii) folgt durch Einsetzen von (2.2)

$$G_{d,i}(X) \; = \; H_{d,i}(X^{-1}) \, X^{q^{d+i+1}}$$

in (i).

□

Bemerkung 2.9. Nach Bemerkung 1.4 (ii) wissen wir, daß alle Koeffizienten von f_{T^d} in $\mathbb{F}_p[T]$ liegen, $p = \mathrm{char}(\mathbb{F}_q)$. Aufgrund von (2.5) gilt dasselbe nun auch für $H_{d,i}$ und somit ebenso für $U = \prod_{i=0}^{\infty} H_{d,d-1}$, $h = U^{q^2-1}$ und $\tilde{\Delta} = U^{(q^2-1)(q-1)}$.

Satz 2.10. *Für $d \in \mathbb{N}_0$ gilt*

$$Q_d \;=\; \sum_{\sigma \in S_{d+1}} \epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}} \;=\; \det(\rho_{T^i}^{q^j})_{i,j=0,\ldots,d}. \tag{2.6}$$

Beweis. Wir zeigen mittels vollständiger Induktion nach $r := d-(i+1)$ die Gültigkeit von

$$G_{i+1,i}\, G_{i+2,i+1} \cdots G_{d,d-1} \;=\; \begin{vmatrix} G_{i+1,i} & G_{i+1,i}^q & \cdots & G_{i+1,i}^{q^{d-(i+1)}} \\ G_{i+2,i} & G_{i+2,i}^q & \cdots & G_{i+2,i}^{q^{d-(i+1)}} \\ \vdots & \vdots & \ddots & \vdots \\ G_{d,i} & G_{d,i}^q & \cdots & G_{d,i}^{q^{d-(i+1)}} \end{vmatrix} \tag{*}$$

für $i = -1, 0, \ldots, d-1$. Im Falle $i = -1$ entspricht dies unserer Behauptung. Für $r = 0$, d.h. $i = d-1$, nimmt (*) die triviale Form

$$G_{d,d-1} \;=\; \det\left(G_{d,d-1}\right)$$

an. Sei also (*) für $r \geq 0$ erfüllt. Für $r+1$ haben wir die Determinante

$$\begin{vmatrix} G_{i,i-1} & G_{i,i-1}^q & \cdots & G_{i,i-1}^{q^{r+1}} \\ G_{i+1,i-1} & G_{i+1,i-1}^q & \cdots & G_{i+1,i-1}^{q^{r+1}} \\ \vdots & \vdots & \ddots & \vdots \\ G_{d,i-1} & G_{d,i-1}^q & \cdots & G_{d,i-1}^{q^{r+1}} \end{vmatrix}$$

(mit $r+2$ Zeilen und Spalten) zu betrachten. Subtrahieren wir für $j = r+1, r, \ldots, 1$ das $G_{i,i-1}^{q^j - q^{j-1}}$-fache der j-ten Spalte von der $(j+1)$-ten Spalte, so erhalten wir

$$\begin{vmatrix} G_{i,i-1} & 0 & \cdots & 0 \\ G_{i+1,i-1} & G_{i+1,i-1}^{q^1} - G_{i+1,i-1}^{q^0}\, G_{i,i-1}^{q^1-q^0} & \cdots & G_{i+1,i-1}^{q^{r+1}} - G_{i+1,i-1}^{q^r}\, G_{i,i-1}^{q^{r+1}-q^r} \\ \vdots & \vdots & \ddots & \vdots \\ G_{d,i-1} & G_{d,i-1}^{q^1} - G_{d,i-1}^{q^0}\, G_{i,i-1}^{q^1-q^0} & \cdots & G_{d,i-1}^{q^{r+1}} - G_{d,i-1}^{q^r}\, G_{i,i-1}^{q^{r+1}-q^r} \end{vmatrix}.$$

Entwickeln wir nun nach der ersten Zeile und wenden auf die übrigen Einträge (2.4) an, so ergibt sich

$$G_{i,i-1} \begin{vmatrix} G_{i+1,i}^{q^0} & \cdots & G_{i+1,i}^{q^r} \\ \vdots & \ddots & \vdots \\ G_{d,i}^{q^0} & \cdots & G_{d,i}^{q^r} \end{vmatrix} = G_{i,i-1}\, G_{i+1,i} \cdots G_{d,d-1}.$$

□

Die Formeln (2.5) und (2.6) liefern uns Algorithmen zur Berechnung von U_d bzw. P_d. Diesen werden wir uns im nächsten Abschnitt widmen. Eine erste Konsequenz von (2.6) ist, daß P_d unabhängig von q, d.h. mit q als variablem Parameter darstellbar ist, denn in (2.6) benötigt man ausgehend von den Polynomen ρ_{T^i} lediglich Additionen bzw. Subtraktionen, Multiplikationen und q-te Potenzen.

Wir können nun zu den im letzten Abschnitt aufgeworfenen Fragen zurückkehren. Das folgende Lemma liefert uns die ersten vier nichttrivialen Koeffizienten von $H_{d,i}$, also insbesondere auch $E(U_d)$.

Lemma 2.11. *Seien $d, i \in \mathbb{N}_0$ und $i \leq d-1$. Dann hat man folgende Aussagen:*

(i)
$$H_{1,0} = 1 - S^{q-1} + (T^q - T)\, S^q.$$

(ii) *Für $d \geq 2$ gilt*

$$H_{d,0} = 1 - S^{q^d-1} + \Big(\sum_{j=1}^{d} T^{q^j}\Big)\, S^{q^d} - \Big(\sum_{j=0}^{d-1} T^{q^j}\Big)\, S^{q^d+q^{d-1}-1} + O(S^{q^d+q^{d-1}}).$$

(iii) *Für $d \geq 2,\ q = 2$ gilt*

$$H_{d,1} = 1 + S^{2^{d+1}-4} + S^{2^{d+1}-3} + (1+T+T^2)\, S^{2^{d+1}-2} + O(S^k)$$
$$\textit{mit} \quad k = \begin{cases} 7 & \textit{für } d = 2 \\ 2^{d+1} & \textit{für } d \geq 3 \end{cases}.$$

Für $d \geq 2,\ q \geq 3$ gilt

$$H_{d,1} = 1 - S^{q^{d+1}-q^2} - S^{q^{d+1}-q^2+q-1} + (T^q - T)\, S^{q^{d+1}-q^2+q} + O(S^{q^{d+1}-q^2+2q-2}).$$

(iv) *Für $d \geq 3,\ i \geq 2$ gilt*

$$H_{d,i} \;=\; 1 \;-\; S^{q^{d+i}-q^{2i}} \;-\; S^{q^{d+i}-q^{2i-2}\,\frac{q^3+1}{q+1}} \;-\; S^{q^{d+i}-q^{2i-4}\,\frac{q^5+1}{q+1}} \;+\; O(S^k),$$

$$\textit{mit} \quad k = \begin{cases} q^{d+2} - q\,\dfrac{q^4-1}{q+1} & \textit{für } i = 2 \\ q^{d+i} - q^{2i-6}\,\dfrac{q^7+1}{q+1} & \textit{für } i \geq 3 \end{cases}.$$

(v) *In jedem Fall gilt also*

$$E(H_{d,i}) \;=\; q^{d+i} - q^{2i} \;=\; q^i\,(q^d - q^i)$$

und somit für $d \geq 1$

$$E(U_d) \;=\; q^{2d-1} - q^{2d-2} \;=\; q^{2d-2}\,(q-1).$$

Insbesondere ist $E(U_d)$ streng monoton wachsend bezüglich d.

Beweis.

(i) Nach (2.5) gilt

$$\begin{aligned} H_{1,0} &= H_{1,-1}^q \;-\; H_{1,-1}\,H_{0,-1}^{q-1}\,S^{q-1} \\ &= f_T^q - f_T \cdot f_0^{q-1}\,S^{q-1} \\ &= (1+TS)^q \;-\; (1+TS)\cdot 1 \cdot S^{q-1} \\ &= 1 \;+\; T^qS^q \;-\; S^{q-1} \;-\; TS^q \\ &= 1 \;-\; S^{q-1} \;+\; (T^q - T)\,S^q. \end{aligned}$$

(ii) Sei $d \geq 2$. Die Rekursion (2.5) liefert

$$\begin{aligned} H_{d,0} &= H_{d,-1}^q \;-\; H_{d,-1}\,H_{0,-1}^{q-1}\,S^{q^d-1} \\ &= f_{T^d}^q \;-\; f_{T^d}\,S^{q^d-1}. \end{aligned}$$

Nach (1.6) und Bemerkung 1.4 (i) gilt

$$f_{T^d} \;=\; 1 \;+\; (\sum_{j=0}^{d-1} T^{q^j})\,S^{q^{d-1}} \;+\; O(S^{q^{d-1}+q^{d-2}}).$$

Also ergibt sich

$$\begin{aligned} H_{d,0} \;&=\; 1 \;+\; (\sum_{j=1}^{d} T^{q^j})\,S^{q^d} \;+\; O(S^{q^d-q^{d-1}}) \\ &\quad - \left(S^{q^d-1} \;+\; (\sum_{j=0}^{d-1} T^{q^j})\,S^{q^d-q^{d-1}-1} \;+\; O(S^{q^d+q^{d-1}+q^{d-2}-1})\right) \\ &= 1 \;-\; S^{q^d-1} \;+\; (\sum_{j=1}^{d} T^{q^j})\,S^{q^d} \;-\; (\sum_{j=0}^{d-1} T^{q^j})\,S^{q^d-q^{d-1}-1} \;+\; O(S^{q^d-q^{d-1}}). \end{aligned}$$

(iii) Seien $d \geq 2,\ q = 2$. Dann gilt nach (2.5) und den Ergebnissen von (i) und (ii)

$$\begin{aligned} H_{d,1} &= H_{d,0}^2 \;-\; H_{d,0}\, H_{1,0}\, S^{2^{d+1}-4} \\ &= \left(1 + S^{2^d-1} \;+\; O(S^{2^d})\right)^2 \\ &\quad + \left(1 \;+\; O(S^{2^d-1})\right) \cdot \left(1 \;+\; S \;+\; (T+T^2)\, S^2\right)\; S^{2^{d+1}-4} \\ &= 1 \;+\; S^{2^{d+1}-4} \;+\; S^{2^{d+1}-3} \;+\; (1+T+T^2)\, S^{2^{d+1}-2} \;+\; O(S^k) \end{aligned}$$

mit

$$\begin{aligned} k &= \min\,\{2 \cdot 2^d,\ 2^d - 1 + 2^{d+1} - 4\} \\ &= \min\,\{2^{d+1},\ 2^{d+1} + 2^d - 5\} \;=\; \begin{cases} 7 & \text{für } d = 2 \\ 2^{d+1} & \text{für } d \geq 3 \end{cases}. \end{aligned}$$

Seien $d \geq 2,\ q \geq 3$. Dann gilt

$$H_{d,1} \;=\; H_{d,0}^q \;-\; H_{d,0}\, H_{1,0}^{q-1}\, S^{q^{d+1}-q^2}.$$

Dabei ist

$$H_{d,0} \;=\; 1 \;+\; O(S^{q^d-1})$$

und

$$\begin{aligned} H_{1,0}^{q-1} &= \left(1 \;-\; S^{q-1} \;+\; (T^q - T)\, S^q\right)^{q-1} \\ &= 1 \;-\; (q-1)\, S^{q-1} \;+\; (q-1)\,(T^q - T)\, S^q \;+\; O(S^{2(q-1)}) \\ &= 1 \;+\; S^{q-1} \;+\; (T - T^q)\, S^q \;+\; O(S^{2q-2}). \end{aligned}$$

Folglich gilt

$$\begin{aligned} H_{d,1} &= 1 \;+\; O(S^{q^{d+1}-q}) \\ &\quad - \left(1 + O(S^{q^d-1})\right) \cdot \left(1 + S^{q-1} + (T - T^q)\, S^q \;+\; O(S^{2q-2})\right)\; S^{q^{d+1}-q^2} \\ &= 1 \;-\; S^{q^{d+1}-q^2} \;-\; S^{q^{d+1}-q^2+q-1} \;+\; (T^q - T)\, S^{q^{d+1}-q^2+q} \\ &\quad + \; O(S^{q^{d+1}-q^2+2q-2}). \end{aligned}$$

(iv) Wir zeigen die Behauptung mit vollständiger Induktion nach i für festes d, wobei i von 2 bis $d-1$ läuft.
Für $i = 2$ lautet (2.5)

$$H_{d,2} \;=\; H_{d,1}^q \;-\; H_{d,1}\, H_{2,1}^{q-1}\, S^{q^{d+2}-q^4},$$

wobei wir bereits wissen, daß

$$H_{d,1} \;=\; 1 \;+\; O(S^{q^{d+1}-q^2})$$

und

$$\begin{aligned} H_{2,1}^{q-1} &= \left(1 - S^{q^3-q^2} - S^{q^3-q^2+q-1} + O(S^{q^3-q^2+q})\right)^{q-1} \\ &= 1 - (q-1)\,S^{q^3-q^2} - (q-1)\,S^{q^3-q^2+q-1} + O(S^{q^3-q^2+q}) \\ &= 1 + S^{q^3-q^2} + S^{q^3-q^2+q-1} + O(S^{q^3-q^2+q}) \end{aligned}$$

gilt. Somit erhalten wir

$$\begin{aligned} H_{d,2} &= 1 + O(S^{q^{d+2}-q^3}) \\ &\quad - \left(1+O(S^{q^{d+1}-q^2})\right)\left(1+S^{q^3-q^2}+S^{q^3-q^2+q-1}+O(S^{q^3-q^2+q})\right) S^{q^{d+2}-q^4} \\ &= 1 - S^{q^{d+2}-q^4} - S^{q^{d+2}-q^4+q^3-q^2} - S^{q^{d+2}-q^4+q^3-q^2+q-1} \\ &\quad + O(S^{q^{d+2}-q^4+q^3-q^2+q}) \\ &= 1 - S^{q^{d+2}-q^4} - S^{q^{d+2}-q^2\,\frac{q^3+1}{q+1}} - S^{q^{d+2}-\frac{q^5+1}{q+1}} + O(S^{q^{d+2}-q\,\frac{q^4-1}{q+1}}). \end{aligned}$$

Sei unsere Behauptung für $i \geq 2$ erfüllt. Dann gilt

$$H_{d,i+1} = H_{d,i}^{q} - H_{d,i}\,H_{i+1,i}^{q-1}\,S^{q^{d+i+1}-q^{2i+2}}$$

mit

$$H_{d,i} = 1 + O(S^{q^{d+i}-q^{2i}})$$

und

$$\begin{aligned} H_{i+1,i}^{q-1} &= \left(1 - S^{q^{2i+1}-q^{2i}} - S^{q^{2i+1}-q^{2i-2}\,\frac{q^3+1}{q+1}} + O(S^{q^{2i+1}-q^{2i-4}\,\frac{q^5+1}{q+1}})\right)^{q-1} \\ &= 1 + S^{q^{2i+1}-q^{2i}} + S^{q^{2i+1}-q^{2i-2}\,\frac{q^3+1}{q+1}} + O(S^{q^{2i+1}-q^{2i-4}\,\frac{q^5+1}{q+1}}). \end{aligned}$$

Hieraus folgt

$$\begin{aligned} H_{d,i+1} &= 1 + O(S^{q^{d+i+1}-q^{2i+1}}) \\ &\quad - (1 + O(S^{q^{d+i}-q^{2i}})) \\ &\quad \cdot \left(1+S^{q^{2i+2}-q^{2i}}+S^{q^{2i+2}-q^{2i-2}\,\frac{q3+1}{q+1}}+O(S^{q^{2i+1}-q^{2i-4}\,\frac{q^5+1}{q+1}})\right) S^{q^{d+i+1}-q^{2i+2}} \\ &= 1 - S^{q^{d+i+1}-q^{2i+2}} - S^{q^{d+i+1}-q^{2i}\,\frac{q^3+1}{q+1}} - S^{q^{d+i+1}-q^{2i-2}\,\frac{q^5+1}{q+1}} \\ &\quad + O(S^{q^{d+i+1}-q^{2i-4}\,\frac{q^7+1}{q+1}}). \end{aligned}$$

(v) folgt aus (i) – (iv).

$\square$

Lemma 2.12. *Für $d \in \mathbb{N}_0$ und $-1 \leq i \leq d-1$ hat der höchste Term von $H_{d,i}$ die Form*

$$h_{d,i} \cdot S^{q^{i+1}\frac{q^d-1}{q-1}},$$

wobei $h_{d,i} \in A$ der Rekursion

$$\begin{aligned} h_{d,-1} &= T^d, \\ h_{d,i+1} &= h_{d,i}^q - h_{d,i}\, h_{i+1,i}^{q-1} \end{aligned}$$

genügt.

Beweis. Vollständige Induktion nach i für festes d.
Für $i = -1$ ist der höchste Term von $H_{d,-1} = f_{T^d}$ nach (1.6) und Bemerkung 1.4 (i) gegeben durch

$$c_{d,d} \cdot S^{D(d,d)} = T^d\, S^{\frac{q^d-1}{q-1}}.$$

Aus der Gültigkeit der Behauptung für i folgt die Gültigkeit für $i+1$ unmittelbar aus der Rekursion

$$H_{d,i+1} = H_{d,i}^q - H_{d,i}\, H_{i+1,i}^{q-1}\, S^{q^{d+i+1}-q^{2i+2}},$$

wenn gezeigt ist, daß $H_{d,i}^q$ und $H_{d,i}\, H_{i+1,i}^{q-1}\, S^{q^{d+i+1}-q^{2i+2}}$ beide den gleichen Grad $\frac{q^{i+2}\,(q^d-1)}{q-1}$ haben. Dies gilt wegen

$$\left(q^{i+1}\,\frac{q^d-1}{q-1}\right)^q = q^{i+2}\,\frac{q^d-1}{q-1}$$

und

$$q^{i+1}\,\frac{q^d-1}{q-1} + q^{i+1}\,\frac{q^{i+1}-1}{q-1}\cdot(q-1) + q^{d+i+1} - q^{2i+2} = q^{i+2}\,\frac{q^d-1}{q-1}.$$

□

Bemerkung 2.13.

(i) Die Rekursion aus Lemma 2.12 liefert

- für $d \geq 1,\ i = 0$:
$$h_{d,0} = T^{qd} - T^d,$$
- für $d \geq 2,\ i = 1$:
$$h_{d,1} = T^{q^2 d} - T^{qd} - (T^{qd} - T^d)\sum_{j=1}^{q} T^{(q-1)j}.$$

(ii) Aus der Rekursionsformel folgt weiterhin

$$\deg(h_{d,i}) \;=\; q^{i+1}\, d.$$

Nach Lemma 2.11 (v) ist uns $E(U_d)$ bekannt:

$$E(U_d) \;=\; q^{2d-2}\,(q-1).$$

Wir erinnern daran, daß

$$\deg(P_d) \;=\; \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)}$$

gilt. Hieraus ergibt sich das nützliche

Lemma 2.14. *Sei $d \in \mathbb{N}_0$.*

(i) *Für $q \geq 3$ gilt*

$$E(U_{d+1}) \;>\; \deg(P_d).$$

(ii) *Ist $q = 2$, so gilt noch die schwächere Aussage*

$$E(U_{d+1}) \;>\; \deg(U_d).$$

Beweis.

(i) Sei $q \geq 3$. Dann gilt

$$\begin{aligned}
& E(U_{d+1}) \;-\; \deg(P_d) \\
&= q^{2d}\,(q-1) \;-\; \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)} \\
&= \frac{q}{(q-1)(q^2-1)}\,\left[\,q^{2d+3} + 2\,q^{2d} + q^{d+1} + q^d - 2\,q^{2d+2} - q^{2d+1} - q^{2d-1} - 1\,\right] \\
&= \frac{q}{(q-1)(q^2-1)}\,\left[\,((q-1)^2-2)\,q^{2d+1} \;+\; (2q-1)\,q^{2d-1} \;+\; q^{d+1} \;+\; q^d - 1\,\right] \\
&\geq \frac{q}{(q-1)(q^2-1)}\,\left[\,2\,q^{2d+1} + 5\,q^{2d-1} + q^{d+1} + q^d - 1\,\right] \\
&> 0.
\end{aligned}$$

(ii) Für $q = 2$ gilt

$$E(U_{d+1}) \;-\; \deg(U_d) \;=\; 2^{2d} - 2^d\,(2^d-1) \;=\; 2^d \;>\; 0. \qquad \square$$

Zur Illustration des obigen Lemmas betrachten wir das folgende

Beispiel 2.15. Für $q = 2$ hat man folgende Werte:

d	$E(U_{d+1})$	$\deg(U_d)$	$\deg(P_d)$
0	1	0	0
1	4	2	2
2	16	12	14
3	64	56	70
4	256	240	310
5	1 024	992	1 302

Wie Lemma 2.14 (ii) besagt, gilt stets

$$E(U_{d+1}) \;>\; \deg(U_d),$$

für $d \geq 3$ jedoch *nicht*

$$E(U_{d+1}) \;>\; \deg(P_d),$$

d.h. die Aussage von 2.14 (i) gilt tatsächlich nur, wenn $q \geq 3$ ist.

Fazit:

Wir wissen jetzt nach den vorangehenden Lemmata, daß $E(U_d)$ mit d streng monoton wächst und daß zumindest im Falle $q \geq 3$ stets

$$E(U_{d+1}) \;>\; \deg(P_d)$$

gilt, so daß nach unseren Vorüberlegungen zu Beginn des Kapitels das Polynom P_d komplett mit dem Anfangsabschnitt der Potenzreihe U bis zum Grad

$$\deg(P_d) \;=\; \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)}$$

übereinstimmt. Im Falle $q = 2$ und $d \geq 3$ gilt die Übereinstimmung nur bis zum Grad

$$E(U_{d+1}) - 1 \;=\; 4^d - 1,$$

denn sämtliche Koeffizienten u_i von U mit $i \geq 4^d$ können von U_{d+1} beeinflusst werden.

Eine weitere Konsequenz von Lemma 2.14 ist das folgende Korollar, das eine Aussage über größere Lücken der Potenzreihe U liefert.

Korollar 2.16. *Seien $q \geq 3$ und $d \in \mathbb{N}_0$ beliebig. Dann ist $u_i = 0$ für alle i mit*

$$\deg(P_d) \;<\; i \;<\; E(U_{d+1}).$$

Die „Randstellen“ der Lücken sehen aus wie folgt:

$$\begin{aligned} u_{\deg(P_d)} &= \prod_{i=1}^{d} h_{i,i-1}, \\ u_{E(U_{d+1})} &= -1. \end{aligned}$$

Dabei sei $h_{i,i-1}$ wie in Lemma 2.12 definiert.

Beweis. Die Aussage folgt sofort aus

$$\deg(P_d) \;<\; E(U_{d+1})$$

und

$$U_d \;=\; 1 - S^{E(U_d)} + \cdots + h_{d,d-1}\, S^{\deg(U_d)}.$$

□

Beispiel 2.17. Für $q = 5$, $d = 0, \ldots, 5$ ergeben sich die ersten Lücken der Potenzreihe U im Sinne von Korollar 2.16 wie folgt: Es gilt jeweils $u_i = 0$ in den Bereichen

$$\begin{aligned} 0 &< i < 4, \\ 5 &< i < 100, \\ 155 &< i < 2\,500, \\ 4\,030 &< i < 62\,500, \\ 101\,530 &< i < 1\,562\,500, \\ 2\,542\,155 &< i < 39\,062\,500. \end{aligned}$$

Bemerkung 2.18. In [7] wird die folgende asymptotische Aussage über den Anteil der nicht verschwindenden Koeffizienten der Produktfunktion U bewiesen:

Seien $q > 2$, $C_m := \{i \leq m \mid u_i \neq 0\}$. Dann gilt

$$\lim_{m \to \infty} \frac{\#\, C_m}{m} = 0.$$

Diese Aussage steht im Einklang mit Korollar 2.16, obwohl sie nicht unmittelbar hieraus folgt.

2.3 Algorithmen

Wir haben nun das notwendige Fundament bereitgestellt, um Algorithmen zur Berechnung von U angeben zu können.

Der erste Algorithmus stützt sich auf die Rekursion (2.5), mit deren Hilfe man $U_1, \ldots, U_d$ ausgehend von den Polynomen $f_{T^1}, \ldots, f_{T^d}$ sukzessive berechnen kann. Die Teilprodukte $U_i = H_{i,i-1}$ ergeben sich aus einem Dreiecksschema: Man erhält nacheinander

$$H_{1,0},\ H_{2,0},\ H_{2,1},\ H_{3,0},\ H_{3,1},\ H_{3,2},\ H_{4,0},\ \ldots$$

Den Start der Rekursion bilden die Polynome $H_{i,-1} = f_{T^i}$, für die man mit (1.6) eine „halb-explizite" Formel besitzt – die Exponenten $D(i,j)$ haben eine einfache Gestalt, und die entsprechenden Koeffizienten $c_{i,j}$ erhält man aus der Rekursion (1.8) bzw. (1.9) durch ein zu der Berechnung von $H_{i,j}$ analoges Dreiecksschema.

In der Formel (2.5) ist jedoch $H_{i,i-1} = U_i$ in die $(q-1)$-te Potenz zu erheben. Wir wollen uns überlegen, wie dies möglichst effizient durchzuführen ist, obwohl diese Frage zweitrangig ist, denn in konkreten Rechnungen zeigt sich, daß die Multiplikation $H_{d,i} \cdot U_i^{q-1}$, nicht die Potenzierung U_i^{q-1}, nahezu die gesamte Rechenzeit eines Arbeitsschrittes benötigt. Dennoch wollen wir kurz auf dieses Problem eingehen.

Am angenehmsten ist der Fall $q = 2$. Ansonsten bieten sich zur Berechnung von U_i^{q-1} die folgenden Möglichkeiten an:

1.) Berechne U_i^{q-1} wie üblich über die Binärdarstellung des Exponenten $q-1$, d.h. als Folge von Quadrierungen:
Sei

$$q-1 \;=\; \sum_{j=1}^{k} 2^{e_j}, \qquad e_1 < \cdots < e_k \in \mathbb{N}_0.$$

(D.h. $e_k \;=\; [\,\log_2(q-1)\,]$.)
Berechne dann durch fortgesetztes Quadrieren

$$U_i^2,\ U_i^4,\ \ldots,\ U_i^{2^{e_k}}.$$

Dann ergibt sich U_i^{q-1} als

$$U_i^{q-1} \;=\; U_i^{\sum_{j=1}^{k} 2^{e_j}} \;=\; \prod_{j=1}^{k} U_i^{2^{e_j}}.$$

Es sind also im besten Fall (wenn $q-1$ Zweierpotenz ist) $[\,\log_2(q-1)\,]$ Multiplikationen durchzuführen, im schlechtesten Fall ($q-1 \;=\; \sum_{j=0}^{k} 2^j$ für ein $k \in \mathbb{N}$) doppelt so viele.

2.) Die oben geschilderte Methode 1 kann in unserem Fall noch verfeinert werden. Wegen $U_i \in \mathbb{F}_p[T][S]$, $q = p^n$, sind nicht nur q-te, sondern bereits p-te Potenzen von

U_i sehr leicht zu berechnen:

$$\left(\sum_{i\geq 0}\left(\sum_{j\geq 0} a_{ij}T^j\right) S^i\right)^p \;=\; \sum_{i\geq 0}\left(\sum_{j\geq 0} a_{ij}T^{pj}\right) S^{pi}, \qquad a_{ij}\in\mathbb{F}_p.$$

Wir können daher die p-adische Entwicklung von $q-1$

$$q-1 \;=\; (p-1)\sum_{j=0}^{n-1} p^j,$$

die sich aus der geometrischen Reihe ergibt, ausnutzen und erhalten

$$U_i^{q-1} \;=\; \left(\prod_{j=0}^{n-1} U_i^{p^j}\right)^{p-1}.$$

Für die äußere $(p-1)$-te Potenz wird dann Methode 1 angewendet.

Diese zweite Methode stimmt offensichtlich mit der ersten überein, falls $n=1$, d.h. $q=p$ Primzahl ist. Für $n>1$ wird sie i. A. besser als Methode 1 sein, da die inneren p^j-ten Potenzen praktisch keinen Aufwand darstellen und der verbleibende Exponent $p-1$ kleiner als $q-1$ ist; für $q=2^n$ entfällt er sogar ganz. Dieser Umstand überwiegt den zusätzlichen Aufwand der inneren Multiplikationen.

3.) Eine andersartige Methode als die ersten beiden stellt die folgende dar: Um die Einfachheit einer q-ten Potenz auszunutzen, berechnet man U_i^{q-1} gemäß

$$U_i^{q-1} \;=\; U_i^q\cdot U_i^{-1}.$$

Hierfür ist die Inverse U_i^{-1} nach der Formel (1.1) bis zum Grad

$$\deg(U_i^{q-1}) \;=\; (q-1)\,q^i\,\frac{q^i-1}{q-1} \;=\; q^{2i}-q^i$$

zu bestimmen und bis zum gleichen Grad mit U_i^q zu multiplizieren.

Wie bereits erwähnt ist Methode 2 in der Regel gleich gut oder besser als Methode 1. Methode 3 erwies sich in praktischen Tests für $i\geq 3$ aufgrund des hohen Aufwands der Invertierung und der Tatsache, daß die Inverse i. A. sehr dicht besetzt ist, was den Aufwand der verbleibenden Multiplikation erhöht, stets als ungünstiger als Methode 2, so daß es sich empfiehlt, Methode 2 anzuwenden.

Wir formulieren nun den Algorithmus. Hierbei ist auch angegeben, welche Objekte zu welchem Zeitpunkt – im Hinblick auf Speicherersparnis bei der Implementierung – wieder freigegeben werden sollten.

Algorithmus 1.
Eingabe: $d \in \mathbb{N}$, Primzahlpotenz q
Ausgabe: P_d

1.) Berechnung der Exponenten $D(i,j)$ von f_{T^i} nach (1.7)

Für $i = 1, \ldots, d$:
$D(i,0) \ := \ 0,$
für $j = 1, \ldots, i$:
$D(i,j) \ := \ D(i,j-1) \ + \ q^{i-j}.$

2.) Berechnung der Koeffizienten $c_{i,j}$ von f_{T^i} nach (1.9)

Für $i = 1, \ldots, d$:
$c_{i,0} \ := \ 1,$
für $j = 1, \ldots, i-1$:
$c_{i,j} \ := \ c_{i-1,j-1} \cdot T^{q^{i-j}} \ + \ c_{i-1,j},$
$c_{i,i} \ := \ T^i.$

3.) Zusammensetzen der f_{T^i}

Für $i = 1, \ldots, d$:
$f_{T^i} \ := \ \sum_{j=0}^{i} c_{i,j} \cdot S^{D(i,j)}.$
Lösche alle $c_{i,j}$ und $D(i,j)$.

4.) Berechnung der $H_{d,i}$ nach (2.5)

Für $i = 1, \ldots, d$:
$H_{i,0} \ := \ f_{T^i}^q \ - \ f_{T^i} S^{q^i-1},$
für $j = 1, \ldots, i-1$:
$H_{i,j} \ := \ H_{i,j-1}^q \ - \ H_{i,j-1} \cdot Z_j \cdot S^{q^{i+j}-q^{2j}},$
falls $i \leq d-1$:
$Z_i \ := \ H_{i,i-1}^{q-1}.$
Lösche alle f_{T^i} und Z_i, sowie $H_{i,j}$ für $i = 1, \ldots, d$, $j = 0, \ldots, i-2$.
Speichere, falls benötigt, $U_i \ = \ H_{i,i-1}$ für $i = 1, \ldots, d$.
Falls $q = 2$ ist, so sind die Z_i überflüssig.

5.) Berechnung von P_d

$$
\begin{aligned}
& P_d \;:=\; H_{1,0}, \\
& \text{für } i = 2, \ldots, d : \\
& \quad P_d \;:=\; P_d \cdot H_{i,i-1}, \\
& \quad \text{lösche } H_{i,i-1}. \\
& \text{Falls } q = 2 \text{ und } d \geq 3 \text{ gilt, so berechne man im} \\
& \text{letzten Schritt } P_d \cdot H_{d,d-1} \text{ nur bis zum Grad } 4^d - 1.
\end{aligned}
$$

Die Formel (2.6) liefert uns einen weiteren Algorithmus, der im Gegensatz zu Algorithmus 1 sofort $P_d = \prod_{i=0}^{d} U_i$ und nicht zuerst $U_1, \ldots, U_d$ berechnet. Analog zur Konstruktion der Polynome f_{T^i} in Algorithmus 1 werden hier die Polynome ρ_{T^i} gemäß (1.10) dargestellt. Hiervon ausgehend kann Q_d berechnet werden, indem die Produkte

$$\epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}}$$

für alle Permutationen $\sigma \in S_{d+1}$ summiert werden. Man erhält also $Q_d(X)$, welches mittels (2.3) leicht zu $P_d(S)$ konvertiert werden kann. (Beide Polynome besitzen die gleichen Koeffizienten aus A mit lediglich verschiedener Indizierung.)

Auch im Falle $q = 2$ sind hier trotz der Tatsache, daß P_d mit U nur bis zum Grad $4^d - 1$ übereinstimmt, sämtliche Operationen vollständig durchzuführen, denn es wird hier zunächst Q_d konstruiert, welches die Koeffizienten von P_d in gespiegelter Reihenfolge enthält, so daß es nicht möglich ist, die oberen Koeffizienten von Q_d „abzuschneiden“. Erst bei der Konvertierung von $Q_d(X)$ zu $P_d(S)$ können die überflüssigen Koeffizienten verworfen werden. Der Algorithmus lautet folgendermaßen:

Algorithmus 2.
Eingabe: $d \in \mathbb{N}$, Primzahlpotenz q
Ausgabe: P_d

1.) Berechnung der Koeffizienten $r_{i,j} = c_{i,i-j}$ von ρ_{T^i} nach (1.10)

$$
\begin{aligned}
& \text{Für } i = 0, \ldots, d : \\
& \quad r_{i,0} \;:=\; T^i, \\
& \quad \text{für } j = 1, \ldots, i-1 : \\
& \quad\quad r_{i,j} \;:=\; r_{i-1,j} \cdot T^{q^j} \;+\; r_{i-1,j-1}, \\
& \quad r_{i,i} \;:=\; 1.
\end{aligned}
$$

2.) Zusammensetzen der ρ_{T^i}

Für $i = 0, \ldots, d$:

$\rho_{T^i} \;:=\; \sum_{j=0}^{i} r_{i,j}\, X^{q^j}.$

Lösche alle $r_{d,i}$.

3.) Berechnung von Q_d nach (2.6)

$Q_d \;:=\; 0,$

Für alle $\sigma \in S_{d+1}$:

$\mathit{Summand} \;:=\; 1,$

für $i = 0, \ldots, d$:

$\mathit{Summand} \;:=\; \mathit{Summand} \cdot \rho_{T^i}^{q^{\sigma(i)}},$

$Q_d \;:=\; Q_d \;+\; \epsilon(\sigma) \cdot \mathit{Summand}.$

4.) Konvertierung von $Q_d(X)$ zu $P_d(S)$ nach (2.3)

Das berechnete Polynom Q_d habe die Form

$$Q_d(X) \;=\; \sum_{i=1}^{L(Q_d)} q_i\, X^{e_i} \quad \text{mit } q_i \neq 0 \text{ für alle } i.$$

Setze für $i = 1, \ldots, L(Q_d)$

$p_i \;:=\; q_{L(Q_d)-i},$

$f_i \;:=\; \left(\frac{q^{2d+2}-1}{q-1} \;-\; e_{L(Q_d)-i} \right) \;/\; (q-1).$

Dann gilt

$$P_d(S) \;=\; \sum_{i=1}^{L(Q_d)} p_i\, S^{f_i}.$$

Im Fall $q = 2$ und $d \geq 3$ brauchen nur diejenigen i mit

$$f_i \leq 4^d - 1 \quad \text{bzw.} \quad e_{L(Q_d)-i} \geq 4^{d+1}$$

berücksichtigt zu werden.

Vergleich der Algorithmen:

Vom Hauptgesichtspunkt der Effizienz her ist eindeutig Algorithmus 2 vorzuziehen. Beispielsweise benötigte Algorithmus 2 zur Berechnung von P_6 für $q = 2$ (auf einer Unix-Umgebung gestartet über ein DQS-Warteschlangensystem) ca. 3 Stunden gegenüber ca. 2 Tagen bei Algorithmus 1. Die Berechnung von P_5 für Werte von q im Bereich von 2 bis 9 benötigte bei Verwendung von Algorithmus 2 jeweils zwischen 2 und 18 Minuten; P_4 war in diesem Fällen stets praktisch in Nullzeit berechnet. Hingegen war es mit Algorithmus 1 nicht mehr möglich, P_5 für $q > 2$ oder P_4 für $q > 4$ zu berechnen, da entweder die Rechenzeit oder der Speicherbedarf gewisse systembedingte Grenzen überstieg. (Möglich waren etwa zwei Wochen Rechenzeit und maximal 512 MB Arbeitsspeicher.)

Dieses Ergebnis wirkt zunächst überraschend, da beim 2. Algorithmus $(d+1)!$ Summanden zu berechnen sind, die jeweils wieder d Multiplikationen benötigen. Dem steht jedoch gegenüber, daß ρ_{T^i} lediglich $i + 1$ von Null verschiedene Koeffizienten besitzt, d.h. der Aufwand einer einzelnen Multiplikation ist sehr gering. Die geringe Effizienz von Algorithmus 1 rührt wohl daher, daß die Teilprodukte U_i gewissermaßen „zuviel“ Information enthalten, denn bei deren Multiplikation treten massive Auslöschungen auf. Zumindest für kleine Werte von q und i scheint der Anteil der nichttrivialen Koeffizienten von U_i in der Größenordnung $\frac{1}{q}$ zu liegen, was ein exponentielles Wachstum der Länge der U_i mit dem Parameter i bedeutet, denn der Grad eines U_i beträgt ca. q^{2i-1}. Demgegenüber ist P_d wesentlich dünner besetzt. Wir hatten bereits erwähnt, daß P_d unabhängig von q dargestellt werden kann, also ist auch für feste, genügend große Werte von q die Länge von P_d unabhängig von q; es können lediglich für kleine Charakteristiken p von $\mathbb{F}_q$ einige zusätzliche Koeffizienten verschwinden oder für sehr kleine q einige Koeffizienten identisch sein, wie etwa q^3+q-1 und q^3+q^2-q-1 für $q = 2$. (In diesem Fall addieren sich die entsprechenden Terme.) So hat beispielsweise P_5 etwa 2 300 nichttriviale Koeffizienten, obwohl der Grad von P_5 bereits in der Größenordnung q^9 liegt, für $q = 9$ gilt z.B. $\deg(P_5) = 441\,287\,847$. Diese dünne Besetzung der Produktfunktion U ist zum Teil durch die größeren Lücken nach Korollar 2.16 und die Kongruenzaussage von Satz 3.9 aus dem nächsten Kapitel erklärbar, jedoch verschwinden selbst innerhalb dieser Beschränkungen noch viele zusätzliche Koeffizienten von U. Somit hält sich bei Algorithmus 2 auch der Speicherbedarf noch in Grenzen, wohingegen er bei Algorithmus 1 durch die notwendige Speicherung von $U_1, \ldots, U_d$ ebenso wie der Rechenaufwand hoch ist.

Neben der deutlich höheren Effizienz hat Algorithmus 2 den bereits angedeuteten Vorteil, daß er sich auch für symbolische Rechnungen mit variablem Parameter q eignet. Dies ist jedoch nicht Anliegen der vorliegenden Arbeit, da spätestens die Berechnung der Diskriminantenfunktion $\tilde{\Delta} = U^{(q^2-1)(q-1)}$ feste Werte für q erfordert.

Abschließend kann man also sagen, daß die einzige Daseinsberechtigung von Algorithmus 1 darin liegt, daß er im Gegensatz zu Algorithmus 2 auch die Teilprodukte U_i liefert, denn letzterer berechnet bekanntlich sofort deren Produkt.

Berechnung der Potenzen h und $\tilde{\Delta}$:

Nehmen wir nun an, die Potenzreihe U sei bis zum Grad $D \in \mathbb{N}$ berechnet. Um $\tilde{\Delta} = U^{(q^2-1)(q-1)}$ aus U zu erhalten, nutzt man für $q \geq 3$ zweckmäßigerweise die Identität

$$U^{(q^2-1)(q-1)} \;=\; U^{q^3-q^2-q+1} \;=\; U^{q^3} \cdot U^{-q^2} \cdot U^{-q} \cdot U,$$

d.h. man berechnet die Inverse U^{-1} gemäß der Rekursion (1.1) bis zum Grad $[\frac{D}{q}]$, erhält hieraus praktisch ohne weiteren Aufwand U^{-q} und U^{-q^2} mindestens bis zum Grad D und berechnet dann das Produkt $U^{q^3} \cdot U^{-q^2} \cdot U^{-q} \cdot U$ bis zum Grad D.

Dieses Vorgehen bietet die folgenden Vorteile:

- Es sind unabhängig von q neben der Invertierung lediglich drei Multiplikationen durchzuführen. Hierbei ist U – wie oben erwähnt – dünn besetzt, und für U^{-q}, U^{-q^2} und U^{q^3} muß dies ebenfalls gelten, da hierin höchstens solche Koeffizienten nicht verschwinden, deren Index Vielfaches von q bzw. q^2 bzw. q^3 ist.

- Die Berechnung der Inversen U^{-1} ist nur bis zum Grad $[\frac{D}{q}]$ erforderlich, was gegenüber einer Invertierung bis zum Grad D eine immense Ersparnis bedeutet, denn in letzterem Fall wäre etwa die q^2-fache Anzahl von Multiplikationen aus A notwendig, wobei die neu hinzukommenden Multiplikationen sogar noch aufwendiger würden, da die Länge der Koeffizienten u_i von U mit steigendem Index i im Mittel wächst. (Vergleiche hierzu auch die Abschätzung (3.2) aus dem nächsten Kapitel sowie die statistischen Daten im Anhang.)

- Man erhält nebenbei auch die Inverse U^{-1} bis zum Grad $[\frac{D}{q}]$ und hat auch die Möglichkeit, mit einer weiteren Multiplikation die Funktion $h = U^{q^2-1} = U^{q^2} \cdot U^{-1}$ bis zum Grad $[\frac{D}{q}]$ zu berechnen.

Im Falle $q = 2$ ist es einfacher, statt obigem Vorgehen $\tilde{\Delta}$ gemäß

$$U^{(q^2-1)(q-1)} \;=\; U^3 \;=\; U^2 \cdot U$$

zu berechnen, wobei die Quadrierung in Charakteristik 2 nahezu nichts kostet, d.h. man kommt mit einer Multiplikation aus. Die Funktion $h = U^{q^2-1}$ stimmt in diesem Fall mit der Funktion $\tilde{\Delta} = U^{(q^2-1)(q-1)}$ überein. Interessiert man sich auch im Falle $q = 2$ für die Inverse U^{-1}, so muß diese gesondert berechnet werden.

2.4 Bemerkungen zur Implementierung

Die Algorithmen des vorigen Abschnitts wurden in der Programmiersprache C++ implementiert. Der Programmcode umfaßt ca. 2 000 Zeilen und ist daher nicht in dieser Arbeit abgedruckt, kann jedoch im World Wide Web unter der Addresse

http://www.math.uni-sb.de/˜mitr/index.html

betrachtet werden. Ebenso stehen dort die berechneten Daten (in reduziertem Umfang) in Form von komprimierten Binärdateien zur Verfügung, die mit Hilfe des hierzu entwickelten Dateibetrachtungsprogramms *Diskriminante* (deutsch) oder *Discriminant* (englisch) betrachtet oder in Textdateien umgewandelt werden können. Dieses unter Windows 3.1x oder Windows 95/98 lauffähige Programm kann ebenfalls auf dieser Seite heruntergeladen werden. Insgesamt belegen die berechneten Daten etwa 120 MB. Die auf der oben angegebenen Seite befindlichen Daten belegen unkomprimiert ca. 53 MB, komprimiert ca. 15 MB.

Wir wollen nun etwas näher auf die Implementierung eingehen. Der Rest dieses Abschnitts richtet sich großteils an Leser mit Kenntnissen der Programmiersprache C++.

Nach Bemerkung 2.9 wissen wir, daß sämtliche in dieser Arbeit auftretenden Potenzreihen Koeffizienten aus $\mathbb{F}_p[T]$ haben, wobei $p = \mathrm{char}(\mathbb{F}_q)$ ist. Zur Darstellung der endlichen Körper kann man sich also auf die Primkörper $\mathbb{F}_p$ beschränken, deren Arithmetik prinzipiell durch die Arithmetik in $\mathbb{Z}$ und Rechnen modulo p realisierbar ist; eine geringe Beschleunigung läßt sich jedoch erreichen, indem man die Rechenregeln der Addition und Multiplikation in Tabellen (zweidimensionalen Feldern) speichert und hierauf direkt (ohne Funktionsaufruf) zugreift. Des Weiteren kann man auch die additiven und eventuell auch die multiplikativen Inversen der Elemente von $\mathbb{F}_p$ in eindimensionalen Feldern speichern.

Polynome $f \in \mathbb{F}_p[T]$ werden durch eine Klasse *TPoly* repräsentiert. Diese merkt sich in einer Variablen *Anzahl* die Anzahl der von Null verschiedenen Koeffizienten von f, und falls *Anzahl* > 0 ist, stehen in zwei dynamisch erzeugten Feldern *exp* und *koeff* der Länge *Anzahl* die in f vorkommenden Exponenten in aufsteigender Reihenfolge sortiert und die entsprechenden Koeffizienten.

Polynome aus $\mathbb{F}_p[T][S]$ werden durch eine weitere Klasse *SPoly* repräsentiert, die sehr ähnlich zu *TPoly* aufgebaut ist, mit dem einzigen Unterschied, daß die Koeffizienten eines solchen Polynoms selbst Polynome aus $\mathbb{F}_p[T]$ sind, d.h. die Klasse *SPoly* besitzt unter ihren privaten Daten ein dynamisch erzeugtes Feld *koeff*, in dem Instanzen der Klasse *TPoly* gespeichert werden.

In beiden Klassen werden nur von Null verschiedene Koeffizienten abgespeichert, sonst wäre die Speicherung von beispielsweise P_5 kaum durchführbar. Aus Effizienzgründen wurde des Weiteren die Klasse *SPoly* zum Freund (*friend*) der Klasse *TPoly* erklärt, d.h. *member*-Funktionen der Klasse *SPoly* dürfen direkt auf die privaten Daten der Klasse *TPoly* zugreifen, so daß Funktionen, die auf der Klasse *SPoly* definiert sind, die Koeffizienten des entsprechenden Polynoms ohne weitere Funktionsaufrufe ändern können. Ebenfalls aus Effizienzgründen wurde auf eine Darstellung von Polynomen mit beliebigem Koeffizientenbereich mittels *template*-Mechanismen verzichtet – hierfür hätten einige spezielle Optimierungen weggelassen werden müssen.

Die benötigten arithmetischen Operationen werden nun durch Funktionen oder Operatoren auf diesen Klassen implementiert. Auf der Basis dieser Implementierung können die Algorithmen aus dem letzten Abschnitt sehr einfach (als Hauptprogramm) übernommen werden.

Sicherlich sind auch andere Repräsentierungen der benötigten Polynome denkbar. So hätte man anstatt der Speicherung der Koeffizienten in Feldern auch verkettete Listen verwenden können. Diese bieten den Vorteil der flexibleren Handhabung, denn Einfügen, Anhängen oder Löschen von Termen ist hiermit problemlos möglich. Des Weiteren kommt diese Methode auch besser mit stark fragmentiertem Speicher zurecht, obwohl sie auch leichter zur Fragmentierung des Speichers führen kann. Die Nachteile dieser Methode liegen in dem etwas höheren Speicherbedarf durch die zusätzlichen *pointer*-Variablen sowie vor allem dem langsameren Zugriff als bei Feldern. Eine Alternative wäre es auch, sich statt der Unterscheidung der Klassen *TPoly* und *SPoly* einen Datentyp *Monom* zu schaffen, der Monome der Form cT^mS^n ($c \in \mathbb{F}_q^*$) darstellt, die dann entweder in einem Feld oder einer verketteten Liste gespeichert werden. Diese Art der Darstellung sollte weder wesentlich besser noch wesentlich schlechter als die hier verwendete sein – die oben geschilderte Darstellung wurde bevorzugt, da sie eher dem in dieser Arbeit eingenommenen Standpunkt entspricht, die zu berechnenden Potenzreihen als solche in $A[[S]] = (\mathbb{F}_q[T])[[S]]$, nicht $\mathbb{F}_q[[T, S]]$, aufzufassen. Der Zugriff auf einen bestimmten Koeffizienten (aus A) bezüglich S ist bei der hier verwendeten Art der Darstellung einfacher.

Das Programm wurde auf einem PC-Rechner mit Pentium 200 MMX Prozessor, 64 MB RAM und dem (etwas älteren) Compiler *Turbo C++ 3.1 für Windows* entwickelt, jedoch nur zu Testzwecken auf diesem System ausgeführt. Die eigentlichen Berechnungen wurden auf UNIX-Rechenanlagen der Universität des Saarlandes mit Hilfe des Warteschlangensystems DQS (*Distributed Queueing System*) durchgeführt, so daß gewährleistet war, daß jede Berechnung als einzelner Prozeß oder parallel mit höchstens ein bis zwei weiteren Prozessen von einer CPU bearbeitet wurde. Somit sind auch die verschiedenen Berechnungszeiten einigermaßen vergleichbar.

Sämtliche Berechnungen wurden für $q = 2, 3, 4, 5, 7, 8, 9$ durchgeführt, zu Testzwecken in geringem Umfang auch für $q = 11, 13$. Für $q = 2$ wurde P_6 berechnet, ansonsten P_5. Die Diskriminantenfunktion $\tilde{\Delta}$ wurde bis zu „vernünftigen" Grenzen berechnet, jeweils Grade zwischen q^5 und q^{12}. Im Anhang findet man weitere Angaben zur Berechnungsdauer und statistische Daten.

Die meisten dort zu findenden Berechnungszeiten sind relativ kurz – meist nicht mehr als einige Stunden, was vermuten läßt, daß es auch möglich sein sollte, die entsprechenden Funktionen noch bis zu höheren Graden zu berechnen. Man beachte hierzu jedoch, daß der Rechenaufwand extrem schnell wächst, so wie etwa die Grade von U_d und P_d bezüglich d von exponentieller Ordnung sind. Es sind daher wohl von vorneherein an die Größenordnungen, bis zu denen die Berechnungen noch mit erträglichen Mengen an Ressourcen durchführbar sind, gewisse Grenzen gesetzt. In der Tat scheiterten einige Berechnungen bis zu höheren Größenordnungen vor allem am Speicherbedarf; der zur Verfügung stehende Speicher belief sich in der Regel auf 32-128 MB, absolute Obergrenze waren 512 MB. Die kurzen Berechnungszeiten kann man daher wohl (positiv) so interpretieren, daß das Programm die möglichen Berechnungen in vernünftiger Zeit bewältigt, der immense Aufwand noch größerer Rechnungen ist wohl inhärent.

Zum Abschluß dieses Kapitels seien dem an Algorithmen und Computeralgebra interessierten Leser als Literatur [2] und [8] empfohlen. Zur Arithmetik endlicher Körper ist [10] empfehlenswert. Ein umfassendes Standardwerk zur Programmiersprache C++ stellt [11] dar.

Kapitel 3

Resultate

3.1 Gradaussagen

Es wäre wünschenswert, Schranken für die Grade der Koeffizienten $c_i \in A = \mathbb{F}_q[T]$ der Potenzreihen U, h und $\tilde{\Delta}$ in Relation zum Index i zu besitzen, um deren Wachstum kontrollieren zu können. Hier wird sich eine sehr einfache Aussage ergeben. Dazu folgende

Definition 3.1. *Eine Potenzreihe* $f = \sum_{i\geq 0} f_i(T)\, S^i \ \in\ \mathbb{F}_q[T][[S]]$ *habe die* Eigenschaft (G), *falls für alle* $i \geq 0$ *gilt*

$$\deg_T(f_i) \ \leq\ i.$$

Satz 3.2. *Die Funktionen* f_a, $H_{d,i}$, U, h, $\tilde{\Delta}$ *und alle dazugehörigen Inversen besitzen die Eigenschaft* (G).

Beweis.
(1) Zunächst sehen wir, daß (G) stabil unter Addition, Multiplikation und Inversenbildung ist ist, denn sind $f = \sum_{i\geq 0} f_i\, S^i$, $\ g = \sum_{i\geq 0} g_i\, S^i \ \in A[[S]]$ zwei Potenzreihen mit der Eigenschaft (G) und $f_0 \in \mathbb{F}_q^*$, so gilt für die Summe $f + g = \sum_{i\geq 0}(f_i + g_i)\, S^i$

$$\deg(f_i + g_i) \ \leq\ \max\left(\deg(f_i), \deg(g_i)\right) \ \leq\ i,$$

für das Produkt $f \cdot g = \sum_{k\geq 0} \left(\sum_{i+j=k} f_i \cdot g_j\right) S^k$

$$\deg\left(\sum_{i+j=k} f_i\, g_j\right) \ \leq\ \max_{i,j}\left\{\deg(f_i\, g_j)\right\} \ =\ \max_{i,j}\left\{\deg(f_i) + \deg(g_j)\right\} \ \leq\ i + j \ =\ k$$

und für die Inverse $f^{-1} = \sum_{i\geq 0} w_i\, S^i \quad (w_0 = f_0^{-1},\ w_i = -f_0^{-1} \sum_{j=1}^{i} f_j\, w_{i-j})$

$$\deg(f_j\, w_{i-j}) \ \leq\ j + i - j \ = i \ \text{ für alle } i.$$

(2) Wir haben in Korollar 1.7 (i) gesehen, daß f_{T^d} die Eigenschaft (G) besitzt. Nach (1) gilt dies dann auch für die folgenden Funktionen:

- f_a wegen (1.3)
- $H_{d,i}$ wegen (2.5),
- U wegen $U = \prod f_a$,
- h und $\tilde{\Delta}$ wegen $h = U^{q^2-1}$, $\tilde{\Delta} = U^{(q^2-1)(q-1)}$.

□

Die Gültigkeit der Eigenschaft (G) liefert uns eine, wenn auch noch sehr grobe, Beschränkung der Längen aller Koeffizienten c_i:

$$L(c_i) \ \leq\ i + 1.$$

Eine schon etwas bessere Abschätzung hierfür werden wir später mit der Ungleichung (3.2) erhalten.

Zunächst aber drängt sich die Frage auf, ob die Gradschranke (G) „scharf“ ist oder ob sie noch verbessert werden kann. Sie kann sicher dann nicht verbessert werden, wenn sie unendlich oft angenommen wird, also in (G) in unendlich vielen Fällen Gleichheit gilt. Im Falle der Produktfunktion U werden wir beweisen, daß dies der Fall ist; ebenso trifft dies aber auch für die Funktionen h und $\tilde{\Delta}$ zu.

Wir wollen nun also untersuchen, an welchen Stellen (d.h. bei welchem Index j der Koeffizienten c_j) die Aussage $\deg(c_j) = j$ gilt. Wir beginnen mit den Polynomen $H_{d,i}$.

Lemma 3.3. *Seien $d \in \mathbb{N}$, $-1 \leq i \leq d-1$, $H_{d,i} = \sum_{j\geq 0} g_j\, S^j$. Dann gilt*

$$\deg(g_j) = j \ \Leftrightarrow\ j \in \{0,\ q^{d+i}\}.$$

Beweis. Vollständige Induktion nach i für festes d, wobei i von -1 bis $d-1$ läuft. Für $i = -1$ ist

$$H_{d,-1} \ = \ f_{T^d} \ = \ \sum_{j=0}^{d} c_{d,j}\, S^{D(d,j)}.$$

Hierfür gilt nach Korollar 1.7 (ii) die Äquivalenz

$$\deg(c_{d,j}) = D(d,j) \quad \Leftrightarrow \quad j \in \{0,1\},$$

wobei $\deg(c_{d,0}) = D(d,0) = 0$ und $\deg(c_{d,1}) = D(d,1) = q^{d-1}$ ist.
Nehmen wir also an, die Behauptung sei für i richtig. Für $i+1$ gilt dann nach (2.5)

$$H_{d,i+1} \;=\; H_{d,i}^q \;-\; H_{d,i}\, H_{i+1,i}^{q-1}\, S^{q^{i+1}(q^d - q^{i+1})}.$$

Seien

$$\begin{aligned} H_{d,i+1} \;&:=\; \sum_{j\geq 0} g_j\, S^j, \\ H_{d,i}^q \;&:=\; \sum_{j\geq 0} a_j\, S^j, \\ H_{d,i}\cdot H_{i+1,i}^{q-1}\cdot S^{q^{i+1}(q^d-q^{i+1})} \;&:=\; \sum_{j\geq 0} b_j\, S^j. \end{aligned}$$

Wegen $\deg(b_j) \leq j - q^{i+1}(q^d - q^{i+1}) < j$ für alle $j \geq 0$ nimmt kein b_j den maximal möglichen Grad j an, so daß folgt

$$\deg(g_j) = j \quad \Leftrightarrow \quad \deg(a_j) = j.$$

Nach Induktionsannahme gilt des Weiteren

$$\deg(a_j) = j \quad \Leftrightarrow \quad j \in \{0,\ q^{d+i+1}\}.$$

□

Die für uns interessanten Teilprodukte $U_d = H_{d,d-1}$ nehmen also genau an den Stellen 0 und q^{2d-1} den maximal möglichen Grad an. Das folgende Lemma gibt uns Auskunft darüber, inwieweit sich solche Gradaussagen bei der Multiplikation von Potenzreihen kontrollieren lassen.

Lemma 3.4.

(i) *Seien* $M_1, M_2 \subset \mathbb{N}_0,\ f = \sum_{i\geq 0} f_i\, S^i,\ g = \sum_{i\geq 0} g_i\, S^i \in A[[S]]$ *mit*

$$\deg(f_i),\ \deg(g_i) \;\leq\; i \quad \textit{für alle } i \geq 0$$

und

$$\begin{aligned} \deg(f_i) = i \quad &\Leftrightarrow \quad i \in M_1, \\ \deg(g_i) = i \quad &\Leftrightarrow \quad i \in M_2. \end{aligned}$$

Dann gilt für $f \cdot g := \sum_{i\geq 0} l_i\, S^i$ *die Implikation*

$$\deg(l_i) = i \quad \Rightarrow \quad i = r + s \quad \textit{mit } r \in M_1,\ s \in M_2.$$

(ii) *Falls in* (i)

$$M_1 = \{i_1, \ldots, i_n\} \quad und \quad M_2 = \{I_1, \ldots, I_m\}$$

mit $i_1 < \cdots < i_n$ *und* $I_1 < \cdots < I_m$ *gilt, so folgt zusätzlich*

$$\deg(l_{i_n+I_m}) = i_n + I_m.$$

(iii) *Falls in* (i)

$$M_1 = \{0, i_1, \ldots, i_n\} \quad und \quad M_2 = \{0, I\}$$

mit $0 < i_1 < \cdots < i_n < I$ *gilt, so folgt*

$$\deg(l_i) = i \quad \Leftrightarrow \quad i = r + s \quad mit\ r \in M_1,\ s \in M_2.$$

Beweis.

(i) Für das Produkt

$$f \cdot g \ = \ \sum_{k \geq 0} \left(\sum_{i+j=k} f_i \cdot g_j \right) S^k$$

kann $\deg(l_k) = \deg(\sum_{i+j=k} f_i\, g_j) = k$ höchstens dann gelten, wenn es mindestens ein Paar von Indizes $(i_0, j_0) \in \mathbb{N}_0^2$ mit

$$\deg(f_{i_0} \cdot g_{j_0}) \ = \ \deg(f_{i_0}) + \deg(g_{j_0}) \ = \ i_0 + j_0 \ = \ k$$

gibt. Dies ist nach Voraussetzung genau für $k = r + s$ mit $r \in M_1,\ s \in M_2$ der Fall.

(ii) Wegen $i_n \in M_1,\ I_m \in M_2$ ist

$$\deg(f_{i_n} \cdot g_{I_m}) \ = \ i_n + I_m.$$

Da außerdem $i_1 < \cdots < i_n$ und $I_1 < \cdots < I_m$ gilt, ist für alle übrigen Paare von Indizes $(\tilde{i}, \tilde{j}) \in (M_1 - \{i_n\}) \times (M_2 - \{I_m\})$

$$\deg(f_{\tilde{i}}) + \deg(g_{\tilde{j}}) \ \leq \ \tilde{i} + \tilde{j} \ < \ i_n + I_m,$$

so daß zum Koeffizienten $l_{i_n+I_m}$ keine weiteren Terme mit maximalem Grad $i_n + I_m$ beitragen können, die eventuell für Auslöschungen sorgen könnten. Somit gilt

$$\deg(l_{i_n+I_m}) \ = \ i_n + I_m.$$

(iii) Die Implikation „⇒“ gilt bereits nach (i). Zum Nachweis der Umkehrung sei $i = r + s$ mit $r \in M_1$ und $s \in M_2$. Dann gilt $\deg(f_r \cdot g_s) = r + s$. Nehmen wir an, es gäbe weitere Indizes $\tilde{r} \in \{0, i_1, \ldots, i_n\} - \{r\}$ und $\tilde{s} \in \{0, I\} - \{s\}$ mit $\tilde{r} + \tilde{s} = r + s$. Falls $s = 0$ ist, so muß $\tilde{s} = I$ sein. Dann gilt aber

$$\tilde{r} + \tilde{s} \ \geq \ I \ > \ r = r + s.$$

Falls aber $s = I$, also $\tilde{s} = 0$ gilt, so folgt

$$\tilde{r} + \tilde{s} \ < \ I = s \ \leq \ r + s.$$

In beiden Fällen ergibt sich ein Widerspruch zur Annahme $\tilde{r} + \tilde{s} = r + s$, also tragen zum Koeffizienten $l_i = l_{r+s}$ keine weiteren Terme vom Grad $r + s$ bei, woraus

$$\deg(l_i) = i$$

folgt.

$\square$

Bemerkung 3.5.

(i) In Lemma 3.4 (i) gilt i. A. *nicht* die Implikation

$$i = r + s \ \text{ mit } \ r \in M_1, \ s \in M_2 \quad \Rightarrow \quad \deg(l_i) = i,$$

selbst dann nicht, wenn gilt

$$M_1 = \{i_1, \ldots, i_n\}, \ M_2 = \{I_1, \ldots, I_m\} \subset \mathbb{N}_0$$

und

$$i_1 < \cdots < i_n < I_1 < \cdots < I_m.$$

Gegenbeispiel: Seien $f := TS + T^2S^2$, $g := T^3S^3 + T^4S^4 - T^5S^5$. Dann kommt S^6 in $f \cdot g = T^4S^4 + 2\,T^5S^5 - T^7S^7$ gar nicht vor, obwohl $i = 6 = 1 + 5 = 2 + 4$ obige Voraussetzung erfüllt.

(ii) In Lemma 3.4 (iii) ist die Voraussetzung

$$i_1 < \cdots < i_n < I$$

wesentlich, wie schon das einfache Gegenbeispiel $q = 2$, $f = g = 1 + TS$ zeigt. Es ist jedoch unerheblich, ob wie angegeben tatsächlich in beiden Mengen der Wert Null enthalten ist oder ob eine oder beide Nullen entfallen. Die im Lemma angegebene Form ist aber genau diejenige, die unserer Situation im Beweis von Satz 3.6 entsprechen wird.

Wir wissen nach Lemma 3.3, daß die Polynome U_d die Gradschranke (G) genau an den Stellen 0 und q^{2d-1} annehmen, d.h. daß dort Gleichheit gilt. Mit Hilfe von Lemma 3.4 können wir hieraus schließen, wann dieses für $P_d = \prod_{i=0}^{d} U_d$ der Fall ist.

Satz 3.6. *Für* $P_d = \sum_{i \geq 0} p_i S^i$ $(d \in \mathbb{N})$ *und* $i \geq 0$ *sind äquivalent:*

(i) $\deg(p_i) = i$.

(ii) *Die Zahl* i *ist von der Form* $i = \sum_{k=1}^{n} q^{i_k}$ *mit* $n \geq 0$, $i_k \in \mathbb{N}$ *ungerade für* $k = 1, \ldots, n$ *und* $i_1 < \cdots < i_n \leq 2d-1$.

Beweis. Vollständige Induktion nach d.
Für $d = 1$ trifft die Behauptung zu, denn es gilt nach Lemma 2.11 (i)

$$P_1 \;=\; U_1 \;=\; H_{1,0} \;=\; 1 - S^{q-1} + (T^q - T)\, S^q.$$

Zum Schluß $d \to d{+}1$ benutze man Lemma 3.4 (iii) mit

$$f := P_d, \quad g := U_{d+1},$$

$$M_1 \;:=\; \left\{ \sum_{k=1}^{n} q^{i_k} \;\middle|\; i_1 < \cdots < i_n \leq 2d{-}1 \text{ alle ungerade, } n \geq 0 \right\},$$

$$M_2 \;:=\; \{0,\, q^{2d+1}\}.$$

□

Nach unseren Überlegungen zu Ende des Abschnitts 2.2 stimmt das Polynom P_d mit der Potenzreihe U bis zum Grad $q^{2d}\,(q-1)$ überein (für $q \geq 3$ ist dieser Wert bereits größer als der Grad von P_d – im Zwischenraum sind alle Koeffizienten Null), so daß wir für genügend großes $d \in \mathbb{N}$ die Potenzreihe U bis zu beliebigen Größenordnungen durch P_d ausschöpfen können. Daher folgt aus Satz 3.6 das folgende

Korollar 3.7. *Für die Koeffizienten der Produktfunktion* U *und* $i \geq 0$ *sind äquivalent:*

(i) $\deg(u_i) = i$.

(ii) *Die Zahl* i *ist von der Form* $i = \sum_{k=1}^{n} q^{i_k}$ *mit* $n \geq 0$, $i_k \in \mathbb{N}$ *ungerade für* $k = 1, \ldots, n$ *und* $i_1 < \cdots < i_n$.

Für die Potenzreihen h und $\tilde{\Delta}$ hat man ähnliche Aussagen:

$$\deg(h_i) = i \quad \Leftrightarrow \quad i \equiv 0 \mod q,$$
$$\deg(\delta_i) = i \quad \Leftrightarrow \quad i \equiv 0, q \mod q^2.$$

Einen Beweis hierzu findet man in [5]. Bei sämtlichen drei Potenzreihen U, h und $\tilde{\Delta}$ gilt also in der Abschätzung $\deg(c_i) \leq i$ unendlich oft Gleichheit, so daß diese Gradschranke nicht verbessert werden kann.

3.2 Kongruenzaussagen

Wie wir schon in Abschnitt 2.3 angedeutet haben, fällt bei der Betrachtung der Produktfunktion U auf, daß diese sehr dünn besetzt ist, beispielsweise gilt $L(P_5) \approx 2\,300$, obwohl bereits $\deg(P_5) \approx q^9$ ist. Dies ist einerseits eine Konsequenz von Korollar 2.16, welches eine Aussage über große Lücken der Potenzreihe U liefert, andererseits sind aber auch die von Korollar 2.16 nicht betroffenen Abschnitte von U keineswegs dicht besetzt. Dieser Sachverhalt kann zum Teil durch die folgende Kongruenzbedingung erklärt werden.

Definition 3.8. *Seien $x_1, \ldots, x_n \in \mathbb{Z}$, $n \geq 1$. Eine Potenzreihe $f = \sum_{i\geq 0} f_i Y^i \in A[[Y]]$ habe die* Eigenschaft $(\mathrm{K}_{x_1,\ldots,x_n})$ *(bezüglich der Variablen Y), falls für alle $i \geq 0$ die Implikation*

$$f_i \neq 0 \quad \Rightarrow \quad i \equiv x_j \mod q \quad \textit{für ein } j \in \{1, \ldots, n\}$$

gilt.

Diese Eigenschaft ist selbstverständlich nicht stabil unter Multiplikation. Dennoch werden wir zeigen können:

Satz 3.9. *Die Produktfunktion U besitzt die Eigenschaft* $(\mathrm{K}_{0,-1})$ *bezüglich S.*

Wenn dies bewiesen ist, so folgt unmittelbar das folgende

Korollar 3.10. *Die Diskriminantenfunktion*

$$\tilde{\Delta} \;=\; U^{(q^2-1)(q-1)} \;=\; \left(U^{q^2-q-1}\right)^q \cdot U$$

besitzt ebenfalls die Eigenschaft $(\mathrm{K}_{0,-1})$ *bezüglich S.*

Zum Beweis von Satz 3.9 benötigen wir den folgenden

Hilfssatz 3.11. Sei $x \equiv 0 \mod q-1$ und $x \equiv k \mod q$, $\; x, k \in \mathbb{Z}$.
Dann ist $\frac{x}{q-1} \equiv -k \mod q$.

Beweis. Sei $x = c\,(q-1)$, $c \in \mathbb{Z}$. Dann gelten die folgenden Äquivalenzen:

$$\begin{array}{lll} & x & \equiv k \mod q \\ \Leftrightarrow & c\,(q-1) & \equiv k \mod q \\ \Leftrightarrow & cq - c & \equiv k \mod q \\ \Leftrightarrow & -c & \equiv k \mod q \\ \Leftrightarrow & c & \equiv -k \mod q. \end{array}$$

□

Beweis von Satz 3.9. Wir fassen zunächst alle betrachteten Potenzreihen als solche in der Variablen X auf. Nach (1.10) gilt

$$\rho_{T^d} \;=\; \sum_{i=0}^{d} c_{d,d-i}\, X^{q^i}.$$

Der kleinste Exponent von ρ_{T^d} ist $q^0 = 1 \equiv 1 \mod q$, die übrigen auftretenden Exponenten sind $\equiv 0 \mod q$, d.h. ρ_{T^d} besitzt (bezüglich X) die Eigenschaft $(\mathrm{K}_{0,1})$. Nach (2.6) gilt weiter

$$Q_d \;=\; \prod_{i=0}^{d} V_i \;=\; \sum_{\sigma \in S_{d+1}} \epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}}.$$

Betrachten wir ein festes $\sigma \in S_{d+1}$ und den zugehörigen Summanden

$$\epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}},$$

wobei $\sigma(k) = 0$ sei $(0 \le k \le d)$. Dann erfüllt

$$\prod_{\substack{i=0\\ i\neq k}}^{d} (\rho_{T^i})^{q^{\sigma(i)}}$$

die Eigenschaft (K_0) und

$$(\rho_{T^k})^{q^{\sigma(k)}} \;=\; \rho_{T^k}$$

die Eigenschaft $(\mathrm{K}_{0,1})$. Also besitzt jeder solche Summand und somit auch die Summe

$$\sum_{\sigma \in S_{d+1}} \epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}} \;=\; Q_d$$

die Eigenschaft $(\mathrm{K}_{0,1})$. Nach (2.3) gilt der Zusammenhang

$$P_d(X) \;=\; Q_d(X^{-1})\, X^{\frac{q^{2d+2}-1}{q^2-1}}.$$

Da $Q_d(X^{-1})$ die Eigenschaft $(\mathrm{K}_{0,-1})$ und $X^{\frac{q^{2d+2}-1}{q^2-1}} = X^{\sum_{i=0}^{d} q^{2i}}$ die Eigenschft (K_1) hat, muß $P_d(X)$ die Eigenschaft $(\mathrm{K}_{0,1})$ besitzen. Hilfssatz 3.11 liefert nun schließlich, daß $P_d(S)$ und somit $U(S)$ die Eigenschaft $(\mathrm{K}_{0,-1})$ erfüllen. $\square$

Die Funktionen U und $\tilde{\Delta}$ genügen also der Eigenschaft $(\mathrm{K}_{0,-1})$. Die Funktionen U_d und h hingegen besitzen keine derartige Kongruenzeigenschaft (wohl aber die Inverse $h^{-1} = U^{1-q^2} = U \cdot (U^{-1})^{q^2}$). Anders als bei der Produktfunktion U, die selbst bei Berücksichtigung der Lückenaussage von Korollar 2.16 und obiger Kongruenzbedingung noch dünn besetzt ist, verschwinden von denjenigen Koeffizienten der Diskriminantenfunktion $\tilde{\Delta}$, die von der Kongruenzbedingung $(\mathrm{K}_{0,-1})$ nicht berührt werden, nur äußerst wenige. Ebenso sind nahezu alle Koeffizienten der Funktion h von Null verschieden. Im Falle $q = 2$, in dem bekanntlich h und $\tilde{\Delta}$ übereinstimmen, scheint von allen Koeffizienten dieser Potenzreihe nur ein einziger zu verschwinden – derjenige mit Index 7.

Die Kongruenzeigenschaft $(\mathrm{K}_{0,-1})$ der Potenzreihen U und $\tilde{\Delta}$ kann man bei der Implementierung der Algorithmen aus Abschnitt 2.3 (vor allem bei Algorithmus 2) ausnutzen, denn Koeffizienten, deren Index weder kongruent zu 0 noch zu -1 modulo q ist, sind zwangsläufig Null und brauchen nicht berechnet zu werden. Die Multiplikationsfunktion des hierzu entwickelten Computerprogramms läßt neben der Wahl zwischen zwei Multiplikationsmethoden, die unterschiedlich günstig sind, je nachdem, ob zu erwarten ist, daß das Produkt dünn oder dicht besetzt sein wird, auch die Berücksichtigung dieser Kongruenzbedingung zu.

Die Potenzreihe h erfüllt, wie bereits zum Ausdruck gebracht, keine Kongruenzbedingung der Form $(\mathrm{K}_{x_1,\dots,x_n})$, dafür genügen ihre Koeffizienten h_k der folgenden andersartigen Kongruenzeigenschaft:

$$h_{k\cdot q^d} \equiv h_k \mod [d], \quad d \in \mathbb{N}. \tag{3.1}$$

Hieraus folgt

$$h_{q^d} \;=\; \begin{cases} 1+[d] & \text{für } q = 2, \\ -[d] & \text{für } q > 2. \end{cases}$$

Einen Beweis von (3.1), der *Hecke-Operatoren* und *Goss-Polynome* benutzt, findet man in [5].

Im Folgenden werden wir eine Aussage über Kongruenzen *innerhalb* der Koeffizienten $c_i \in \mathbb{F}_q[T]$ der zu untersuchenden Potenzreihen beweisen.

Lemma 3.12. *Seien* $f = \sum_{j\geq 0} f_j T^j \in \mathbb{F}_q[T]$ *und* $i \in \mathbb{N}_0$. *Dann sind äquivalent:*

(i) *Für alle* $j \geq 0$ *mit* $f_j \neq 0$ *gilt*

$$j \equiv i \mod q-1.$$

(ii) *Für alle* $a \in \mathbb{F}_q^*$ *gilt*

$$f(aT) \;=\; a^i f(T).$$

Beweis.
(i) $\Rightarrow$ (ii): Sei $a \in \mathbb{F}_q^*$. Dann gilt

$$f(aT) \;=\; \sum_{j\geq 0} f_j\,(aT)^j \;=\; \sum_{j\geq 0} f_j\,a^j\,T^j.$$

Nach (i) können wir jedes $j \geq 0$ mit $f_j \neq 0$ in der Form

$$j = k_j\,(q-1) + i, \quad k_j \in \mathbb{N}_0$$

schreiben. Somit gilt

$$f(aT) \;=\; \sum_{j\geq 0} f_j\,a^{k_j\,(q-1)+i}\,T^j \;=\; a^i \sum_{j\geq 0} f_j\,T^j \;=\; a^i\,f(T),$$

denn es ist $a^{q-1} = 1$.

(ii) $\Rightarrow$ (i): Wir können $q > 2$ annehmen, denn für $q = 2$ ist die Aussage trivial. Wir fixieren ein $a \in \mathbb{F}_q^* \smallsetminus \{1\}$. Dann gilt nach (ii)

$$f(aT) \;=\; \sum_{j\geq 0} f_j\,a^j\,T^j \;=\; a^i \sum_{j\geq 0} f_j\,T^j.$$

Multiplizieren mit a^{-i} liefert

$$\sum_{j\geq 0} f_j\,a^{j-i}\,T^j \;=\; \sum_{j\geq 0} f_j\,T^j,$$

also $a^{j-i} = 1$ für alle $j \geq 0$. Wegen $a \neq 1$ muß $q-1 \mid j-i$ gelten, also

$$j \equiv i \mod q-1.$$

$\square$

Satz 3.13. *Die Koeffizienten $c_i \in \mathbb{F}_q[T]$ der Funktionen f_{T^d}, $H_{d,j}$, U, h, $\tilde{\Delta}$ und ihrer Inversen erfüllen die äquivalenten Bedingungen von Lemma 3.12 (wobei der Index i auch die Rolle des Wertes i in 3.12 spielt).*

Beweis.
(1) Es seien $f = \sum_{i\geq 0} f_i\,S^i$, $g = \sum_{i\geq 0} g_i\,S^i \in A[[S]]$ zwei Potenzreihen, die beide Bedingung (ii) (und somit auch (i)) aus Lemma 3.12 erfüllen, d.h. für alle $i \geq 0$ und alle $a \in \mathbb{F}_q^*$ gelte

$$f_i(aT) \;=\; a^i\,f_i(T) \quad\text{und}\quad g_i(aT) \;=\; a^i\,g_i(T).$$

Dann gilt für die Summe $f+g=\sum_{i\geq 0}(f_i+g_i)\,S^i$

$$(f_i+g_i)(aT) \;=\; f_i(aT)+g_i(aT) \;=\; a^i\,f_i(T)+a^i\,g_i(T) \;=\; a^i\,(f_i+g_i)(T)$$

und für das Produkt $f\cdot g=\sum_{k\geq 0}\left(\sum_{i+j=k} f_i\cdot g_j\right)S^k$

$$\begin{aligned}(f_i\,g_j)(aT) \;&=\; f_i(aT)\,g_j(aT) \;=\; a^i\,f_i(T)\cdot a^j\,g_j(aT)\\ &=\; a^{i+j}\,f_i(T)\,g_j(T) \;=\; a^k(f_i\,g_j)(T),\end{aligned}$$

d.h. die Koeffizienten der Summe und des Produkts erfüllen wieder die Bedingung (ii). Ist darüberhinaus f invertierbar mit Inverser $f^{-1}=\sum_{i\geq 0} w_i\,S^i$ $(w_0=f_0^{-1},\; w_i=-f_0^{-1}\sum_{j=1}^{i} f_j\,w_{i-j})$, so gilt auch für die Koeffizienten w_i der Inversen

$$\begin{aligned}w_i(aT) \;&=\; -f_0^{-1}\sum_{j=1}^{i}(f_j\,g_{i-j})(aT) \;=\; -f_0^{-1}\sum_{j=1}^{i}\left(a^j f_j(T)+a^{i-j}g_{i-j}(T)\right)\\ &=\; -f_0^{-1}\,a^i\sum_{j=1}^{i}(f_j\,g_{i-j})(T) \;=\; a^i\,w_i(T).\end{aligned}$$

Ebenso sieht man durch Betrachtung der äquivalenten Bedingung (i), daß diese bei Multiplikation mit S^k erhalten bleibt, wenn $k\equiv 0 \mod q-1$ ist. (Dieser Fall tritt in Formel (2.5) auf.)

(2) Wir zeigen nun Bedingung (i) für die Koeffizienten von f_{T^d} mittels vollständiger Induktion nach d. Dann gilt die Aussage des Satzes wegen (1) und mit den gleichen Argumenten wie im Beweis von 3.2 auch für die Funktionen $H_{d,j}$, U, h und $\tilde{\Delta}$, da sich diese durch arithmetische Operationen aus f_{T^d} aufbauen und hierbei die geforderten Bedingungen erhalten bleiben.

Nach (1.6) ist f_{T^d} von der Form

$$f_{T^d} \;=\; \sum_{j=0}^{d} c_{d,j}\,S^{D(d,j)},$$

d.h. wir haben jeweils zu zeigen, daß für $j=0,\ldots,d$ alle in $c_{d,j}$ auftretenden Exponenten kongruent zu $D(d,j)$ modulo $q-1$ sind. Für $d=0$, also $f_1=1$, trifft dies offenbar zu. Im Induktionsschritt zeigen wir nun, daß die Koeffizienten $c_{d+1,j}$, $j=0,\ldots,d+1$, von $f_{T^{d+1}}$ die geforderte Eigenschaft besitzen. Für $j=0$ gilt wie im Fall $d=0$

$$c_{d+1,0}=1,\quad D(d+1,0)=0 \quad\text{und}\quad 0\equiv 0 \mod q-1.$$

Für $j=d+1$ ist

$$c_{d+1,d+1}=T^{d+1},\quad D(d+1,d+1)=\sum_{k=0}^{d} q^k,$$

also

$$D(d{+}1, d{+}1) \;-\; (d+1) \;=\; \sum_{k=0}^{d} q^k \;-\; (d+1).$$

Dieser Ausdruck ist sicher durch $q-1$ teilbar, da er als Polynom in q betrachtet Eins als Nullstelle hat. Daher gilt

$$d+1 \equiv D(d{+}1, d{+}1) \mod q{-}1.$$

Für $0 < j < d+1$ ist nach (1.8)

$$c_{d+1,j} \;=\; c_{d,j}^q \;+\; T \cdot c_{d,j-1},$$

wobei nach Induktionsannahme alle in $c_{d,j}^q$ auftretenden Exponenten kongruent zu $q \cdot D(d,j) = D(d{+}1, j)$ modulo $q-1$ und alle Exponenten in $T \cdot c_{d,j-1}$ kongruent zu $D(d, j{-}1) + 1$ modulo $q-1$ sind. Weiter gilt

$$\begin{aligned} D(d, j{-}1) + 1 \;&=\; \sum_{k=d-j+1}^{d-1} q^k \;+\; 1 \;=\; \sum_{k=d-j+1}^{d} q^k \;-\; q^d + 1 \\ &=\; D(d{+}1, j) \;-\; (q^d - 1) \\ &\equiv\; D(d{+}1, j) \mod q{-}1, \end{aligned}$$

d.h. sowohl alle Exponenten in $c_{d,j}^q$ als auch alle Exponenten in $T \cdot c_{d,j-1}$ sind kongruent zu $D(d{+}1, j)$ modulo $q-1$, also gilt das Gleiche auch für $c_{d+1,j}$. □

Beispiel 3.14. Für $q = 7$ lautet der Koeffizient δ_{105} der Diskriminantenfunktion $\tilde{\Delta}$

$$\delta_{105} \;=\; 6\,T^{15} + T^{21} + 2\,T^{57} + 5\,T^{63} + 6\,T^{99} + T^{105},$$

wobei alle Differenzen $105-15,\; 105-21, \ldots$ Vielfache von $q-1 = 6$ sind.

Bemerkung 3.15.

(i) Für beliebige Polynome f_a ist die Aussage von Satz 3.13 im Allgemeinen falsch. Man betrachte als Gegenbeispiel etwa

$$f_{1+T} = 1 + (1+T)\,S$$

für $q > 2$.

(ii) Nach Satz 3.13 gilt für die Länge der Koeffizienten $c_i \in \mathbb{F}_p[T]$ einer der Funktionen f_{T^d}, $H_{d,j}$, U, h, $\tilde{\Delta}$ oder ihrer Inversen die Abschätzung

$$L(c_i) \;\leq\; \left[\frac{i}{q-1}\right] + 1, \tag{3.2}$$

denn alle in c_i (bezüglich T) vorkommenden Exponenten müssen von der Form

$$\bar{i} + k\,(q-1), \quad 0 \le k \le \left[\frac{i}{q-1}\right],$$

sein. Dabei sei $0 \le \bar{i} \le q-2$ der Minimalrest von i modulo $q-1$.

Die Schranke (3.2) wird aber i. A. weit unterschritten. Wahrscheinlich gilt sogar $\lim_{i\to\infty} \frac{L(c_i)}{i} = 0$, möglicherweise mit Ausnahme des Falles $q = 2$. Dies konnte jedoch nur für den Fall der Produktfunktion U relativ zuverlässig verifiziert werden; die Grade, bis zu denen die Funktionen U^{-1}, h und $\tilde{\Delta}$ bekannt sind, sind hierfür noch zu gering. Zwar wachsen im Mittel die Längen der nichttrivialen Koeffizienten c_i mit dem Parameter i, jedoch offensichtlich von geringerer als linearer Ordnung.

Die Annahme, diejenigen Koeffizienten aus $\mathbb{F}_p$ von $c_i \in \mathbb{F}_p[T]$, die nicht nach Satz 3.13 verschwinden müssen, seien über $\mathbb{F}_p$ gleichverteilt, ist offenbar nicht gerechtfertigt, denn es scheint zumindest ein wesentlich größerer Anteil als $\frac{1}{p}$ Null zu sein.

(iii) Neben der Gültigkeit von $c_i(aT) = a^i\, c_i(T)$ für $a \in \mathbb{F}_q^*$ besitzen die Koeffizienten c_i der Funktionen U_d, U, h, $\tilde{\Delta}$ und ihrer Inversen, nicht jedoch f_{T^d} oder $H_{d,j}$ für $j < d-1$, die Eigenschaft, invariant unter Verschiebungen der Form $T \mapsto T + a$ zu sein:

$$c_i(T+a) \;=\; c_i(T) \quad \text{für alle } a \in \mathbb{F}_q.$$

Dies wird in [5] bewiesen. Äquivalent dazu ist die Aussage $c_i \in \mathbb{F}_q[T^q - T]$.

3.3 Explizite Formeln

Im folgenden Satz beweisen wir, daß diejenigen Koeffizienten der Produktfunktion U, deren Index eine Potenz von q mit ungeradem Exponenten m ist, eine sehr regelmäßige Gestalt besitzen. Sie sind – bis auf Vorzeichen – von der Form $T + T^q + \cdots + T^{q^m}$.

Satz 3.16. *Sei $l = q^m$, $m \in \mathbb{N}$ ungerade. Dann gilt für den Koeffizienten u_l der Produktfunktion U*

$$u_l \;=\; \sum_{i=0}^{m} \epsilon(i)\, T^{q^{m-i}} \tag{3.3}$$

$$\textit{mit}\quad \epsilon(i) \;:=\; \begin{cases} +1 & \textit{für } i \equiv 0,3 \mod 4, \\ -1 & \textit{für } i \equiv 1,2 \mod 4. \end{cases}$$

Dem eigentlichen Beweis dieses Satzes schicken wir noch zwei Lemmata voraus.

Lemma 3.17. *Es gelte*

$$\sum_{i=1}^{r} q^{\alpha_i} \;=\; \sum_{i=1}^{s} q^{\beta_i}$$

mit nichtnegativen ganzen Zahlen $\alpha_1 < \cdots < \alpha_r$, $\beta_1 \leq \cdots \leq \beta_s$ *und* $s \leq r$. *Dann gilt bereits* $s = r$ *und* $\alpha_i = \beta_i$ *für* $i = 1, \ldots, r$.

Beweis. Vollständige Induktion nach r.
Für $r = 1$ ist die Aussage trivial, für $r > 1$ folgt sie aus der Induktionsannahme, wenn $\alpha_1 = \beta_1$ gezeigt ist. Zunächst muß $\alpha_1 \geq \beta_1$ gelten, denn im Falle $\alpha_1 < \beta_1$ wäre $\sum_{i=1}^{r} q^{\alpha_i}$ im Gegensatz zu $\sum_{i=1}^{s} q^{\beta_i}$ nicht kongruent zu 0 modulo q^{β_1}.

Sei $m := \max\,\{1 \leq i \leq s \mid \beta_i < \alpha_2\}$.
(Der Wert $m \geq 1$ ist wohldefiniert wegen $\beta_1 \leq \alpha_1 < \alpha_2$.)

Durch Kongruenzbetrachtung modulo q^{α_2} folgt

$$q^{\alpha_1} \;=\; \sum_{i=1}^{m} q^{\beta_i}, \tag{*}$$

also

$$\sum_{i=2}^{r} q^{\alpha_i} \;=\; \sum_{i=m+1}^{s} q^{\beta_i},$$

so daß nach Induktionsannahme $r-1 = s-m$ gilt. Aus den Bedingungen $s \leq r$ und $m \geq 1$ ergibt sich, daß $s = r$ und insbesondere $m = 1$ gelten muß, also liefert (*), daß $\alpha_1 = \beta_1$ ist. □

Lemma 3.18. *Wir setzen für* $3 \leq d \in \mathbb{N}$

$$\begin{aligned} A(d) \;:=\; & \sum_{i=1}^{d-2} (-1)^{d+i} \left(-T^{q^{i-1}} + T^{q^{i+1}} + T^{q^{2i-1}} + T^{q^{2i}} - T^{q^{2i+1}} - T^{q^{2i+2}}\right) \\ & + (-1)^d \left(T - T^{q^2}\right) \;+\; T^{q^{d-2}} - T^{q^{d-1}} - T^{q^{2d-3}} + T^{q^{2d-1}}, \end{aligned}$$

$$B(d) \;:=\; -\,2 \sum_{i=0}^{2d-3} \epsilon(i)\, T^{q^{2d-3-i}} \;-\, T^{q^{2d-2}} + T^{q^{2d-1}}$$

mit $\epsilon(i)$ *wie in Satz 3.16 definiert. Dann gilt*

$$A(d) \;=\; B(d).$$

Beweis. Mit der Bezeichnung

$$C(d) \;:=\; T^{q^{2d-4}} - T^{q^{2d-3}} - T^{q^{2d-2}} + T^{q^{2d-1}}$$

rechnet man leicht nach, daß

$$A(d) \;+\; A(d-1) \;=\; C(d) \qquad (*)$$

und

$$B(d) \;+\; B(d-1) \;=\; C(d) \qquad (**)$$

gilt. Wir zeigen nun die Identität $A(d) = B(d)$ mit vollständiger Induktion nach d. Für $d = 3$ gilt

$$A(3) \;=\; B(3) \;=\; -2\,T + 2\,T^q + 2\,T^{q^2} - 2\,T^{q^3} - T^{q^4} + T^{q^5}.$$

Sei $A(d-1) = B(d-1)$ für einen Wert $d-1 \geq 3$ richtig. Dann gilt

$$\begin{aligned} A(d) &= C(d) - A(d-1) && \text{nach } (*) \\ &= C(d) - B(d-1) && \text{nach Induktionsannahme} \\ &= B(d) && \text{nach } (**). \end{aligned}$$

□

Wir können nun den Satz 3.16 beweisen. Das Vorgehen des Beweises ist von „algorithmischer“ Art – es wird das Zustandekommen der Koeffizienten u_l bei der Berechnung von U (bzw. P_d) gemäß Algorithmus 2 aus Abschnitt 2.3 untersucht.

Beweis von Satz 3.16.

(1) Seien $d \in \mathbb{N}$, $m = 2d-1$.
Wir betrachten das Polynom $P_d = \prod_{i=0}^{d} U_i$. Wegen

$$P_{d+1} \;=\; P_d \cdot U_{d+1}$$

muß P_d mit P_{d+1} bis zum Grad $E(U_{d+1})-1$ übereinstimmen. Weiter gilt nach Lemma 2.11 (v)

$$E(U_d) \;=\; q^{2d-1}\,(q-1),$$

d.h. $E(U_d)$ ist bezüglich d streng monoton wachsend, so daß P_d bereits mit der Potenzreihe U bis zum Grad $E(U_{d+1})-1 = q^{2d}\,(q-1)-1$ übereinstimmt. (Zusätzlich wissen wir nach Lemma 2.14 (i), daß für $q \geq 3$ dieser Wert bereits den Grad von P_d übersteigt.) Der Grad von P_d ist nach (2.1) durch

$$\deg(P_d) \;=\; \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)}$$

gegeben. Die in P_d vorkommenden Exponenten der Form q^k mit k ungerade sind daher genau $q^1, q^3, \ldots, q^{2d-1}$. Da diese allesamt kleiner als $E(U_{d+1})-1$ sind, stimmen die zugehörigen Koeffizienten mit den Koeffizienten $u_{q^1}, u_{q^3}, \ldots, u_{q^{2d-1}}$ der Produktfunktion U überein. Es genügt deshalb zu zeigen, daß für jedes $d \in \mathbb{N}$ der Koeffizient $u_{q^{2d-1}}$ in P_d von der im Satz behaupteten Gestalt ist.

Die Produkte $Q_d(X) = \prod_{i=0}^{d} V_i(X)$ und $P_d(S) = \prod_{i=0}^{d} U_i(S)$ besitzen die gleichen Koeffizienten mit verschiedener Indizierung; die Indizes entsprechen sich nach (2.3) wie folgt:

$$\begin{array}{rcl}
Q_d(X) & \longleftrightarrow & P_d(S) \\
k & \longrightarrow & \dfrac{1}{q-1}\left(\dfrac{q^{2d+2}-1}{q^2-1} - k\right) \\
\dfrac{q^{2d+2}-1}{q^2-1} - k\,(q-1) & \longleftarrow & k.
\end{array}$$

Der Koeffizient mit Index q^{2d-1} in $P_d(S)$ entspricht also dem Koeffizienten mit Index

$$\frac{q^{2d+2}-1}{q^2-1} - q^{2d-1}\,(q-1) \;=\; \frac{q^{2d}-1}{q^2-1} + q^{2d-1} \;=\; \sum_{i=0}^{d-1} q^{2i} + q^{2d-1}$$

in $Q_d(X)$. Für Q_d haben wir die Formel (2.6) :

$$Q_d \;=\; \sum_{\sigma \in S_{d+1}} \epsilon(\sigma) \prod_{i=0}^{d} (\rho_{T^i})^{q^{\sigma(i)}}.$$

Des Weiteren gilt nach (1.10) für $i \in \mathbb{N}_0$

$$\rho_{T^i} \;=\; \sum_{j=0}^{i} c_{i,i-j}\, X^{q^j}$$

und somit

$$(\rho_{T^i})^{q^{\sigma(i)}} \;=\; \sum_{j=0}^{i} (c_{i,i-j})^{q^{\sigma(i)}}\, X^{q^{j+\sigma(i)}}.$$

Daher haben alle in $\prod_{i=0}^{d}(\rho_{T^i})^{q^{\sigma(i)}}$ auftretenden Exponenten die Form

$$q^{j_0+\sigma(0)} + q^{j_1+\sigma(1)} + \ldots + q^{j_d+\sigma(d)},$$

wobei j_i als Laufindex von ρ_{T^i} die Nebenbedingung $0 \le j_i \le i$ erfüllen muß, $i = 0, \ldots, d$.

Es gilt nun zu untersuchen, welche Terme in der Formel (2.6) zu dem Koeffizienten, der $u_{q^{2d-1}}$ entspricht, beitragen können, d.h. wir benötigen sämtliche Lösungen der Gleichung

$$\sum_{i=0}^{d-1} q^{2i} + q^{2d-1} = \sum_{i=0}^{d} q^{j_i+\sigma(i)}.$$

Hierbei sei eine „Lösung“ ein Paar (V, σ) mit $V := (j_0, \ldots, j_d) \in \mathbb{N}_0^{d+1}$, $0 \le j_i \le i$ für $i = 0, \ldots, d$ und $\sigma \in S_{d+1}$, für das obige Gleichheit gilt. Der Beitrag einer solchen Lösung zum gesuchten Koeffizienten ist dann

$$\epsilon(\sigma) \prod_{i=0}^{d} (c_{i,i-j_i})^{q^{\sigma(i)}}.$$

In der betrachteten Gleichung steht auf beiden Seiten jeweils eine Summe von q-Potenzen, wobei zumindest die q-Potenzen auf der linken Seite paarweise verschieden sind. Wir können also hierfür Lemma 3.17 zur Anwendung bringen, welches uns sagt, daß die obige Gleichung nur dann erfüllt sein kann, wenn eine termweise Identität vorliegt, d.h. wenn

$$\{0, 2, 4, \ldots, 2d-2,\ 2d-1\} = \{j_i + \sigma(i) \mid i = 0, \ldots, d\} \qquad (*)$$

gilt. Die Bestimmung aller Lösungen von (*) ist nun ein rein kombinatorisches Problem, das wir im Folgenden lösen werden.

(2) Wir wollen zunächst die Menge aller möglichen Lösungen von (*) näher klassifizieren. Summieren wir in (*) jeweils die Elemente beider Mengen, und zwar die rechte Seite im Spezialfall $j_i = i$ für alle i, so erhalten wir für die linke Seite

$$\sum_{i=0}^{d-1} 2i + 2d-1 = 2 \cdot \frac{1}{2}\, d\,(d-1) + 2d-1 = d^2 + d - 1$$

und für die rechte Seite

$$\sum_{i=0}^{d} i + \sum_{i=0}^{d} i = 2 \cdot \frac{1}{2}\, d\,(d+1) = d^2 + d.$$

Die Summe der rechten Seite ist also in diesem Fall genau um 1 „zu groß“. Dies erzwingt, daß für eine Lösung (V, σ) von (*) gilt: Es gibt genau ein i_0 $(1 \leq i_0 \leq d)$ mit $j_{i_0} = i_0 - 1$, und $j_i = i$ für $i \neq i_0$. Dieses führt uns zur folgenden Bezeichnung:

Sei für $1 \leq i \leq d$

$$\begin{aligned} V_i^d &:= (v_0, \ldots, v_d) \in \mathbb{N}_0^{d+1} \quad \text{mit } v_i = i-1 \text{ und } v_k = k \text{ für } k \neq i \\ &= (0, 1, \ldots, i{-}1, i{-}1, i{+}1, \ldots, d). \end{aligned}$$

Dann ist also jede Lösung von (*) von der Form (V_i^d, σ) für ein i. In diesem Fall heiße $\sigma \in S_{d+1}$ eine *Lösung zu* V_i^d.

Zusammen mit den Ergebnissen aus (1) gilt nun also

$$u_{q^{2d-1}} = \sum_{i=1}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \epsilon(\sigma) \prod_{j=0}^{d} (c_{j,j-v_j})^{q^{\sigma(j)}},$$

mit $v_i = i - 1$ und $v_j = j$ für $j \neq i$, d.h.

$$u_{q^{2d-1}} = \sum_{i=1}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \epsilon(\sigma) \prod_{\substack{j=0 \\ j \neq i}}^{d} (c_{j,0})^{q^{\sigma(j)}} \cdot (c_{i,1})^{q^{\sigma(i)}}.$$

Es gilt nach Satz 1.3 sowie Bemerkung 1.4 (i)

$$c_{j,0} = 1 \quad \text{und} \quad c_{i,1} = \sum_{k=0}^{i-1} T^{q^k},$$

so daß wir erhalten

$$u_{q^{2d-1}} = \sum_{i=1}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i)}}. \qquad (**)$$

Um diesen Ausdruck auswerten zu können, müssen wir $\epsilon(\sigma)$ und $\sigma(i)$ für alle Lösungen $\sigma \in S_{d+1}$ zu V_i^d für $i = 1, \ldots, d$ kennen.

(3) Wir zeigen nun mittels vollständiger Induktion nach d (konstruktiv!), daß es zu jedem V_i^d genau zwei Lösungen $\sigma_1, \sigma_2 \in S_{d+1}$ gibt. Die Induktionsannahme lautet in voller Länge:

> Für $d \in \mathbb{N}$ und $1 \leq i \leq d$ existieren genau zwei verschiedene Lösungen $\sigma_1, \sigma_2 \in S_{d+1}$ zu V_i^d. Für gerades d sind beide Lösungen zu V_1^d von der Form
> $$\sigma = (s_0, \ldots, s_{d-1},\ d{-}1),$$

für ungerades $d > 1$ von der Form

$$\sigma = (s_0, \ldots, s_{d-2},\, d,\, d-2).$$

Beweis:
In den Fällen $d = 1$ und $d = 2$ prüft man leicht nach, daß genau die folgenden Lösungen existieren:

- Zu V_1^1 : $\sigma = (0,1),\ (1,0)$.
- Zu V_1^2 : $\sigma = (0,2,1),\ (2,0,1)$.
- Zu V_2^2 : $\sigma = (0,1,2),\ (0,2,1)$.

Sei die Behauptung für $d-1$ erfüllt ($d \geq 3$). Wir konstruieren im Induktionsschritt $d-1 \to d$ die geforderten Lösungen zu V_i^d, $i = 1, \ldots, d$, aus denjenigen, die nach Induktionsannahme zu V_j^{d-1}, $j = 1, \ldots, d-1$, existieren.

1.Fall: $i > 1$.
Seien $\sigma_1 = (s_0, \ldots, s_{d-1})$, $\sigma_2 = (t_0, \ldots, t_{d-1}) \in S_d$ die beiden einzigen nach Induktionsannahme existierenden Lösungen von (*) zu V_{i-1}^{d-1}, d.h. die Bedingung

$$\begin{aligned}\{x_k + k \mid k = 0, \ldots, d-1,\ k \neq i-1\} \ &\cup\ \{x_{i-1} + i-2\} \\ &= \ \{0, 2, 4, \ldots, 2d-4,\ 2d-3\}\end{aligned}$$

mit $(x_0, \ldots, x_{d-1}) \in S_d$ ist genau dann erfüllt, wenn entweder $x_k = s_k$ für alle $k = 0, \ldots, d-1$ oder $x_k = t_k$ für alle $k = 0, \ldots, d-1$ gilt. Folglich ist

$$\begin{aligned}\{x_k + k + 2 \mid k = 0, \ldots, d-1,\ k \neq i-1\} \ &\cup\ \{x_{i-1} + i\} \\ &= \ \{2, 4, 6, \ldots, 2d-2,\ 2d-1\}\end{aligned}$$

und somit auch

$$\begin{aligned}\{x_k + k + 2 \mid k = 0, \ldots, d-1,\ k \neq i-1\} \ &\cup\ \{0,\ x_{i-1} + i\} \\ &= \ \{0, 2, 4, \ldots, 2d-2,\ 2d-1\}\end{aligned}$$

ebenfalls genau in den Fällen $x_k = s_k$ für alle k und $x_k = t_k$ für alle k richtig. Daher sind

$$\tilde{\sigma}_1 := (0,\ s_0 + 1, \ldots, s_{d-1} + 1), \quad \tilde{\sigma}_2 := (0,\ t_0 + 1, \ldots, t_{d-1} + 1) \ \in S_{d+1}$$

die einzigen Lösungen von (*) zu V_i^d. Insbesondere gilt $\tilde{\sigma}_1 \neq \tilde{\sigma}_2$, denn es ist $\sigma_1 \neq \sigma_2$.

2. Fall: $i = 1$, $d > 2$ gerade.
Seien $\sigma_1 = (s_0, \ldots, s_{d-3},\ d-1,\ d-3)$, $\sigma_2 = (t_0, \ldots, t_{d-3},\ d-1,\ d-3) \in S_d$ die beiden

Lösungen von (*) zu V_1^{d-1}, d.h. die Mengengleichung

$$\begin{aligned}\{x_k + k \mid k = 0, \ldots, d-3,\ k \neq 1\} \ \cup\ \{x_1,\ 2d-4,\ 2d-3\} \\ = \ \{0, 2, 4, \ldots, 2d-4,\ 2d-3\}\end{aligned}$$

ist mit $(x_0, \ldots, x_{d-1}) \in S_d$ nur in den Fällen $x_k = s_k$ für alle $k = 0, \ldots, d-1$ oder $x_k = t_k$ für alle $k = 0, \ldots, d-1$ erfüllt. Dann muß auch die daraus resultierende Gleichung

$$\begin{aligned}\{x_k + k \mid k = 0, \ldots, d-3,\ k \neq 1\} \ \cup\ \{x_1,\ 2d-4,\ 2d-2,\ 2d-1\} \\ = \ \{0, 2, 4, \ldots, 2d-2,\ 2d-1\}\end{aligned}$$

genau in diesen Fällen erfüllt sein, so daß

$$\tilde{\sigma}_1 := (s_0, \ldots, s_{d-3},\ d,\ d-3,\ d-1), \quad \tilde{\sigma}_2 := (t_0, \ldots, t_{d-3},\ d,\ d-3,\ d-1) \ \in S_{d+1}$$

die beiden einzigen Lösungen von (*) zu V_1^d darstellen. Insbesondere sind beide von der geforderten Form und verschieden.

3. Fall: $i = 1,\ d > 1$ ungerade.
Seien wieder $\sigma_1 = (s_0, \ldots, s_{d-2},\ d-2)$, $\sigma_2 = (t_0, \ldots, t_{d-2},\ d-2) \in S_d$ die beiden Lösungen von (*) zu V_1^{d-1}, was bedeutet, daß die Gleichheit

$$\begin{aligned}\{x_k + k \mid k = 0, \ldots, d-2,\ k \neq 1\} \ \cup\ \{x_1,\ 2d-3\} \\ = \ \{0, 2, 4, \ldots, 2d-4,\ 2d-3\}\end{aligned}$$

mit der Forderung $(x_0, \ldots, d_{d-1}) \in S_d$ genau dann gilt, wenn entweder $x_k = s_k$ für alle k oder $x_k = t_k$ für alle k ist. Dann muß das Gleiche auch für

$$\begin{aligned}\{x_k + k \mid k = 0, \ldots, d-2,\ k \neq 1\} \ \cup\ \{x_1,\ 2d-2,\ 2d-1\} \\ = \ \{0, 2, 4, \ldots, 2d-2,\ 2d-1\}\end{aligned}$$

gelten, d.h.

$$\tilde{\sigma}_1 := (s_0, \ldots, s_{d-2},\ d,\ d-2), \quad \tilde{\sigma}_2 := (t_0, \ldots, t_{d-2},\ d,\ d-2) \ \in S_{d+1}$$

sind die beiden einzigen Lösungen von (*) zu V_1^d. Beide sind von der geforderten Gestalt und verschieden.

Damit ist die Existenz genau zweier verschiedener Lösungen $\sigma_1, \sigma_2 \in S_{d+1}$ zu jedem V_i^d, $i = 1, \ldots, d$, bewiesen.

(4) Aufgrund von (**)

$$u_{q^{2d-1}} \ = \ \sum_{i=1}^{d} \ \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \ \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i)}}$$

sind bei den Lösungen $\sigma \in S_{d+1}$ zu V_i^d insbesondere die Werte $\epsilon(\sigma)$ und $\sigma(i)$ von Interesse. Diese können wir nun bestimmen, denn aus der Konstruktion der Lösungen im Beweis aus (3) läßt sich folgendes ablesen:

Seien $d, i \geq 2$, $\sigma \in S_d$ eine Lösung zu V_{i-1}^{d-1} und $\tilde{\sigma} \in S_{d+1}$ die entsprechend dem Beweis aus (3) fortgesetzte Lösung zu V_i^d. Dann gelten die Beziehungen

$$\tilde{\sigma}(i) = \sigma(i-1) + 1 \quad \text{und} \quad \epsilon(\tilde{\sigma}) = \epsilon(\sigma). \tag{***}$$

Ist hingegen $\sigma \in S_d$ eine Lösung speziell zu V_1^{d-1} und $\tilde{\sigma} \in S_{d+1}$ die fortgesetzte Lösung zu V_1^d, so gilt

$$\tilde{\sigma}(1) = \sigma(1) \quad \text{und} \quad \epsilon(\tilde{\sigma}) = -\epsilon(\sigma).$$

Zusammen mit den Lösungen in den Fällen $d = 1, 2$ folgt, daß (bei passender Numerierung) für die Lösungen zu V_i^d, $d \in \mathbb{N}$, $i = 1, \ldots, d$, folgendes gilt:

$$\sigma_1(i) = \begin{cases} i+1, & \text{falls } 1 \leq i \leq d-1 \\ d, & \text{falls } i = d \end{cases}, \qquad \sigma_2(i) = i-1,$$

$$\epsilon(\sigma_1) = (-1)^{d+i}, \qquad \epsilon(\sigma_2) = (-1)^{d+i+1}.$$

(5) Wir können jetzt den Beweis vollenden und die Behauptung über den Koeffizienten $u_{q^{2d-1}}$ mittels vollständiger Induktion nach d zeigen:

$$u_{q^{2d-1}} = \sum_{i=0}^{2d-1} \epsilon(i)\, T^{q^{2d-1-i}}.$$

In den Fällen $d = 1$ und $d = 2$ folgt dies sofort durch Einsetzen der explizit gegebenen Lösungen aus dem Induktionsanfang von (3) in (**). Um den Schluß $d-1 \to d$ zu zeigen, betrachten wir wieder die Gleichung (**)

$$u_{q^{2d-1}} = \sum_{i=1}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i)}}.$$

Die Ergebnisse aus (4) liefern uns die folgende Information über die Lösungen $\sigma_1, \sigma_2 \in S_{d+1}$ zu V_1^d:

$$\sigma_1(1) = 2, \quad \sigma_2(1) = 0, \quad \epsilon(\sigma_1) = (-1)^{d+1}, \quad \epsilon(\sigma_2) = (-1)^d.$$

Setzen wir dies in (**) ein, so erhalten wir

$$u_{q^{2d-1}} \;=\; (-1)^d\,(T - T^{q^2}) \;+\; \sum_{i=2}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^d}} \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i)}} .$$

Aufgrund der Beziehung (***) können wir dies wie folgt umformen:

$$\begin{aligned}
u_{q^{2d-1}} \;&=\; (-1)^d\,(T - T^{q^2}) \;+\; \sum_{i=2}^{d} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_{i-1}^{d-1}}} \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i-1)+1}} \\
&=\; (-1)^d\,(T - T^{q^2}) \;+\; \sum_{i=1}^{d-1} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^{d-1}}} \epsilon(\sigma) \left(\sum_{k=0}^{i} T^{q^k} \right)^{q^{\sigma(i)+1}} \\
&=\; (-1)^d\,(T - T^{q^2}) \;+\; \sum_{i=1}^{d-1} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^{d-1}}} \epsilon(\sigma) \left(\sum_{k=1}^{i+1} T^{q^k} \right)^{q^{\sigma(i)}} .
\end{aligned}$$

Da nach (**)

$$u_{q^{2d-3}} \;=\; \sum_{i=1}^{d-1} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^{d-1}}} \epsilon(\sigma) \left(\sum_{k=0}^{i-1} T^{q^k} \right)^{q^{\sigma(i)}}$$

gilt, folgt zwischen $u_{q^{2d-1}}$ und $u_{q^{2d-3}}$ der Zusammenhang

$$u_{q^{2d-1}} \;=\; u_{q^{2d-3}} \;+\; (-1)^d\,(T - T^{q^2}) \;+\; \sum_{i=1}^{d-1} \sum_{\substack{\sigma \text{ Lösung} \\ \text{zu } V_i^{d-1}}} \epsilon(\sigma) \; \left(-T + T^{q^i} + T^{q^{i+1}} \right)^{q^{\sigma(i)}} .$$

Nutzen wir die Ergebnisse aus (4) über die Werte $\epsilon(\sigma)$ und $\sigma(i)$, so erhalten wir

$$\begin{aligned}
u_{q^{2d-1}} \;&=\; u_{q^{2d-3}} \;+\; (-1)^d\,(T - T^{q^2}) \\
&\quad +\; \sum_{i=1}^{d-2} (-1)^{d+i} \left[\left(-T + T^{q^i} + T^{q^{i+1}} \right)^{q^{i-1}} \;-\; \left(-T + T^{q^i} + T^{q^{i+1}} \right)^{q^{i+1}} \right] \\
&\quad +\; \left(-T + T^{q^{d-1}} + T^{q^d} \right)^{q^{d-1}} \;-\; \left(-T + T^{q^{d-1}} + T^{q^d} \right)^{q^{d-2}} \\
&=\; u_{q^{2d-3}} \;+\; (-1)^d\,(T - T^{q^2}) \\
&\quad +\; \sum_{i=1}^{d-2} (-1)^{d+i}\, \left(-T^{q^{i-1}} + T^{q^{i+1}} + T^{q^{2i-1}} + T^{q^{2i}} - T^{q^{2i+1}} - T^{q^{2i+2}} \right) \\
&\quad +\; T^{q^{d-2}} - T^{q^{d-1}} - T^{q^{2d-3}} + T^{q^{2d-1}} .
\end{aligned}$$

Mit den Bezeichnungen von Lemma 3.18 bedeutet dies, daß für beliebiges $d \geq 3$

$$u_{q^{2d-1}} \;=\; u_{q^{2d-3}} \;+\; A(d)$$

gilt. Da Lemma 3.18 besagt, daß $A(d) = B(d)$ ist, folgt

$$u_{q^{2d-1}} \;=\; u_{q^{2d-3}} \;+\; B(d).$$

Nach Induktionsannahme und der Definition von $B(d)$ lautet der Koeffizient $u_{q^{2d-1}}$ also

$$\begin{aligned}
u_{q^{2d-1}} &= \sum_{i=0}^{2d-3} \epsilon(i)\, T^{q^{2d-3-i}} - 2 \sum_{i=0}^{2d-3} \epsilon(i)\, T^{q^{2d-3-i}} - T^{q^{2d-2}} + T^{q^{2d-1}} \\
&= - \sum_{i=0}^{2d-3} \epsilon(i)\, T^{q^{2d-3-i}} - T^{q^{2d-2}} + T^{q^{2d-1}} \\
&= - \sum_{j=2}^{2d-1} \epsilon(j-2)\, T^{q^{2d-1-j}} - T^{q^{2d-2}} + T^{q^{2d-1}} \\
&= \sum_{i=2}^{2d-1} \epsilon(i)\, T^{q^{2d-1-i}} \;+\; \epsilon(1)\, T^{q^{2d-2}} \;+\; \epsilon(0)\, T^{q^{2d-1}} \\
&= \sum_{i=0}^{2d-1} \epsilon(i)\, T^{q^{2d-1-i}}.
\end{aligned}$$

Dieses war zu zeigen. □

Bemerkung 3.19.

(i) Auch für $l = q^m$ mit m gerade und $q > 2$ kann man den Koeffizienten u_l explizit angeben – diese Aussage ist jedoch trivial, denn nach Korollar 2.16 muß für diesen Koeffizienten $u_l = 0$ gelten, da er in eine Lücke der Potenzreihe U hineinfällt. Im Fall $q = 2$ ist diesbezüglich keine Regelmäßigkeit erkennbar.

(ii) Seltsamerweise scheint der auf $u_{q^{2d-1}}$ ($d \geq 3$ für $q = 2$, $d \geq 2$ sonst) folgende nichttriviale Koeffizient $u_{q^{2d-1}+q-1}$ von U bis auf die Vorzeichen exakt von der gleichen Gestalt wie $u_{q^{2d-1}}$ zu sein, obwohl er sich offensichtlich auf ganz andere Weise als $u_{q^{2d-1}}$ im Beweis von Satz 3.16 ergibt.

Weitere Beobachtungen:

Ähnliche Formeln wie (3.3) im Fall des Koeffizienten $u_{q^{2d-1}}$ der Produktfunktion U scheinen auch für gewisse Koeffizienten der Diskriminantenfunktion $\tilde{\Delta}$ zu gelten. Hier hat man sogar allgemeiner eine (empirische) Regel für die Koeffizienten der Form $\delta_{a\cdot q^k}$. Diese lautet:

Für $k \geq 2$, $a \in \mathbb{N}$ und $q > a+1$ gilt

$$\delta_{a\cdot q^k} \;=\; \sum_{i=0}^{a-1} \Big(r_{2i+1}\, T^{iq^k+(a-i-1)q+1} \;+\; r_{2i+2}\, T^{iq^k+(a-i)q} \Big) \;+\; (-1)^a\, T^{aq^k} \tag{3.4}$$

mit $r_j \in \mathbb{F}_p^*,\ j = 1,\ldots,2a$. Hierbei gilt $r_1 = a,\ \ r_2 = a+1,\ \ r_3 = a^2 - a,\ \ r_4 = -a^2$ sowie $r_{2a-1} = (-1)^a \cdot a,\ \ r_{2a} = (-1)^{a+1} \cdot 2a$. Weitere Regelmäßigkeiten sind unter den r_j anscheinend nicht erkennbar. Die restlichen Koeffizienten r_j in den Fällen $a = 4,5,6$ lauten (wahrscheinlich) wie folgt:

a	j	r_j
4	5	-12
	6	18
5	5	-30
	6	40
	7	20
	8	-30
6	5	-60
	6	75
	7	60
	8	-80
	9	-30
	10	45

Man beachte, daß man die Koeffizienten r_j aus den numerischen Ergebnissen einer Rechnung mit konkretem Wert $q = p^n$ nur modulo p ablesen kann, so daß für kleines p bzw. q Information verlorengehen kann. Erst bei Vorliegen von Ergebnissen für mehrere (möglichst große) Werte von p kann man mit Hilfe des Chinesischen Restsatzes die wahrscheinlichen allgemeinen Werte der Koeffizienten r_j rekonstruieren. Die Bedingung $q > a+1$ erfordert des Weiteren für große a immer höhere Werte von q, was die Untersuchung erschwert. Die oben angegebenen Koeffizienten r_j sind aus Berechnungen mit Primzahlpotenzen q bis einschließlich 13 entstanden.

Falls die Bedingung $q > a+1$ nicht erfüllt ist, so hat der Koeffizient $\delta_{a\cdot q^k}$ immer noch eine zu (3.4) ähnliche Gestalt. Es entfallen dann meist einige Terme (nicht nur aus Kongruenzgründen), und es kommt manchmal der konstante Term 1 hinzu.

Für die Funktion h scheinen ebenfalls ähnliche Formeln zu gelten.

Anhang A

Statistische Daten

In Folgenden sind einige statistischen Daten zu den Funktionen U_d, U, U^{-1}, h und $\tilde{\Delta}$ tabelliert. Die genauen Bedeutungen der einzelnen Spalten entnehme man den jeweiligen Anmerkungen. Allgemein findet man in den Tabellen die Grade und Längen (in Bezug auf die Variable S) gewisser Anfangssegmente der jeweiligen Funktion sowie die mittleren Grade und Längen der Koeffizienten aus $A = \mathbb{F}_q[T]$ des entsprechenden Segments, wobei für die Berechnung dieser Mittelwerte jeweils nur diejenigen Koeffizienten aus A berücksichtigt wurden, von denen nicht bereits aus irgendwelchen Gründen bekannt ist, daß sie Null sein müssen. Diese mögliche Länge ist in jenen Fällen angegeben. Des Weiteren gelte bei den Angaben zu den mittleren Graden der Koeffizienten die Konvention, daß das Nullpolynom den Grad Null habe.

Die Angabe von „0“ bei der Berechnungsdauer bedeutet, daß das entsprechende Objekt praktisch in Nullzeit berechnet ist. Einige auftretende sehr kurze Berechnungszeiten suggerieren, daß es möglich sein sollte, die jeweilige Funktion noch bis zu höheren Ordnungen zu berechnen – dies wurde im Fall der Funktionen U_d, U und $\tilde{\Delta}$ meist auch in der Tat versucht, scheiterte jedoch entweder am Speicherbedarf oder der explodierenden Berechnungsdauer. Bei den übrigen Funktionen U^{-1} und h ergab sich die Größenordnung der Berechnung aus derjenigen der Potenzreihe $\tilde{\Delta}$ – wird $\tilde{\Delta}$ bis zum Grad q^k berechnet, so erhält man, wie zu Ende von Abschnitt 2.3 geschildert, im gleichen Rahmen die Funktionen U^{-1} und h bis zur Ordnung q^{k-1}.

A.1 Daten zu den Teilprodukten U_d

Tabelle A.1: Statistische Daten zu den Teilprodukten U_d

q	d	Grad	mögl. Länge	Länge	mittl. Grad	mittl. Länge	Dauer
2	2	12	10	9	2,8	2,2	0
	3	56	42	31	9,2	3,8	0
	4	240	178	120	33,1	10,3	0
	5	992	738	447	129,1	4,1	17 s
	6	4 030	3 010	1 894	508,5	124,2	2 h 14 min
3	2	36	20	16	5,7	2,1	0
	3	351	191	134	40,1	7,5	0
	4	3 240	1 784	1 244	363,4	52,5	1 min 30 s
4	2	80	34	24	8,9	1,8	0
	3	1 344	578	327	96,9	7,1	1 s
	4	21 760	9 474	5 019	1 437,4	58,7	1 h 45 min
5	2	150	52	36	13,9	2,4	0
	3	3 875	1 377	930	304,1	22,4	4 s
7	2	392	100	64	25,5	2,8	0
	3	19 551	5 147	3 416	1 185,6	50,9	2 min
8	2	576	130	69	26,8	1,7	0
	3	37 376	8 706	3 750	1 146,1	15,2	30 s
9	2	810	164	88	34,6	2,1	0
	3	66 339	13 853	7 375	2 345,9	33,7	4 min

Die nicht selbsterklärenden Spalten der linksstehenden Tabelle haben den folgenden Inhalt:

Spalte 4 – *mögliche Länge*:

Die Polynome U_d besitzen eine relativ „große“ Lücke zwischen dem Absolutglied 1 und dem nächsten nichttrivialen Koeffizienten mit Index $E(U_d) = q^{2d-2}\,(q-1)$, siehe Lemma 2.11 (v). Alle übrigen Koeffizienten können a priori von Null verschieden sein. Somit beträgt die theoretisch mögliche Länge von U_d

$$\deg(U_d) - E(U_d) + 2.$$

Spalte 6 – *mittlerer Grad*, Spalte 7 – *mittlere Länge*:

Es sind nur diejenigen Koeffizienten berücksichtigt, deren Index nicht im Intervall von 1 bis $E(U_d) - 1$ liegen. Die Spalteninhalte errechnen sich also als die Summe der Grade bzw. Längen durch die mögliche Länge aus Spalte 4.

Spalte 8 – *Dauer*:

Angegeben ist die Gesamtberechnungsdauer von $U_1, \ldots, U_d$ mit Algorithmus 1 aus Abschnitt 2.3, wobei aber nahezu die gesamte Rechenzeit für U_d verbraucht wird, die verstrichene Zeit für $U_1, \ldots, U_{d-1}$ also vernachlässigbar ist. Für größere Werte d als die hier angegebenen war es nicht möglich, U_d zu berechnen, obwohl die kurzen Berechnungszeiten der vorhandenen U_d dies vermuten lassen.

A.2 Daten zur Produktfunktion U

Tabelle A.2: Statistische Daten zu den Anfangssegmenten P_d der Produktfunktion U

q	d	Grad	mögl. Länge	Länge	mittl. Grad	mittl. Länge	Dauer
2	1	2	3	3	0,7	1,3	0
	2	14	15	11	4,9	3,3	0
	3	70	71	46	22,7	9,4	0
	4	310	311	190	99,0	34,3	0
	5	1 302	1 303	763	411,8	133,4	2 min
	6	5 334	5 335	3 017	1660,5	524,0	2 h 48 m.
3	1	3	3	3	1,0	1,3	0
	2	39	18	13	11,3	2,9	0
	3	390	171	66	102,0	10,4	0
	4	3 630	1 620	363	886,9	53,9	0
	5	33 033	14 895	2 037	7 857,1	351,1	9 min
4	1	4	3	3	1,3	1,3	0
	2	84	22	12	24,3	3,0	0
	3	1 428	353	58	356,2	10,4	0
	4	23 188	5 804	311	5 272,1	54,7	0
	5	372 372	93 687	1 726	80 134,2	406,8	8 min
5	1	5	3	3	1,7	1,3	0
	2	155	26	13	41,9	2,9	0
	3	4 030	639	68	932,2	10,2	0
	4	101 530	16 252	385	21 668,2	57,3	0
	5	2 542 155	408 115	2 274	518 648,8	499,4	15 min
7	1	7	3	3	2,3	1,3	0
	2	399	34	13	103,9	2,9	0
	3	19 950	1 619	68	4 393,1	10,2	0
	4	980 350	80 036	385	199 043,8	57,4	0
	5	48 056 757	3 928 023	2 274	9 321 057,5	499,4	16 min
8	1	8	3	3	2,7	1,3	0
	2	584	38	12	158,0	3,0	0
	3	37 960	2 361	58	8 633,5	10,4	0
	4	2 434 120	152 140	312	499 831,5	54,8	0
	5	155 821 128	9 747 295	1 783	30 178 345,5	433,4	15 min
9	1	9	3	3	3,0	1,3	0
	2	819	42	13	208,4	2,9	0
	3	67 158	3 303	67	14 558,2	10,3	0
	4	5 447 178	269 004	378	1 078 623,8	56,9	0
	5	441 287 847	21 805 467	2 236	83 139 018,3	481,6	18 min

Man beachte, daß für $q = 2$ und $d \geq 3$ das Polynom P_d mit der Potenzreihe U nur bis zum Grad $4^d - 1$ übereinstimmt.

Anmerkungen zu den Spalteninhalten:

Spalte 4 – *mögliche Länge*:

Die Produktfunktion U genügt einerseits nach Satz 3.9 der Kongruenzbedingung $(\mathrm{K}_{0,-1})$, d.h. der Index i aller von Null verschiedenen Koeffizienten u_i von U muß $i \equiv 0, -1 \mod q$ erfüllen. Andererseits besitzt U, falls $q > 2$ ist, nach Korollar 2.16 jeweils Lücken in den Intervallen zwischen $\deg(P_d) = \frac{q\,(q^d-1)(q^{d+1}-1)}{(q-1)(q^2-1)}$ und $E(U_{d+1}) = q^{2d-2}\,(q-1)$, $d \in \mathbb{N}$ beliebig. Die Anzahl der möglichen nichttrivialen Koeffizienten in P_d beträgt daher für $q > 2$

$$M(d) \;:=\; 3 + \sum_{i=2}^{d} \left((\deg(P_i) - E(U_i)) \cdot \frac{2}{q} + 1 \right) \;=\; 2 + d + \frac{2}{q} \sum_{i=2}^{d} (\deg(P_i) - E(U_i)).$$

(Bzw.: $M(1) = 3$, $\;M(d) = M(d-1) + 1 + \frac{2}{q}\,(\deg(P_d) - E(U_d))$.) Im Fall $q = 2$ können prinzipiell alle Koeffizienten von Null verschieden sein, da dann sowohl die Lückenaussage von Korollar 2.16 fehlschlägt, als auch die Kongruenzbedingung von Satz 3.9 nichts besagt.

Spalte 6 – *mittlerer Grad*, Spalte 7 – *mittlere Länge*:

Es sind hier nur die tatsächlich von Null verschiedenen Koeffizienten von U berücksichtigt, nicht alle theoretisch möglichen nichttrivialen Koeffizienten aus Spalte 4, denn in diesem Fall würden vor allem die mittleren Längen schon für kleine d dicht bei Null liegen, da sich die dünne Besetzung der Potenzreihe U zu stark auswirkt.

Spalte 8 – *Dauer*:

Angegeben ist die Berechnungsdauer von P_d bei Verwendung von Algorithmus 2 aus Abschnitt 2.3. Zum Vergleich einige Berechnungszeiten des weniger effizienten Algorithmus 1:

q	d	Dauer
2	5	8 min 16 s
2	6	1 d 23 h 12 min
3	4	4 min 30 s
4	4	1 h 2 min

Für $q = 5$ war P_4 nach 2 Wochen noch nicht berechnet.

A.3 Daten zur Inversen U^{-1}

Tabelle A.3: Statistische Daten zur Inversen U^{-1}, Abschnitte bis q^k

q	k	q^k	Länge	mittlerer Grad	mittlere Länge	Dauer
2	1	2	3	0,7	1,7	0
	2	4	5	1,2	1,6	0
	3	8	9	1,8	2,1	0
	4	16	14	2,6	1,9	0
	5	32	30	9,7	4,8	0
	6	64	48	7,9	3,7	0
	7	128	110	38,6	12,9	0
	8	256	177	28,7	10,3	0
	9	512	413	148,2	41,2	1 min 19 s
	10	1 024	668	111,3	35,2	1 h 29 min
	11	2 048	1 565	570,3	145,7	10 h 48 min
3	1	3	3	0,8	1,0	0
	2	9	8	2,1	1,4	0
	3	27	25	8,7	3,0	0
	4	81	71	19,0	4,9	0
	5	243	233	97,6	19,6	0
	6	729	694	212,6	43,5	22 s
	7	2 187	2 152	943,9	185,0	14 min
4	1	4	3	0,8	0,8	0
	2	16	11	3,1	1,2	0
	3	64	52	18,6	3,0	0
	4	256	178	51,5	4,4	0
	5	1 024	899	372,9	23,1	0
	6	4 096	3 286	1 012,0	53,6	4 min
5	1	5	3	0,8	0,8	0
	2	25	17	4,8	1,5	0
	3	125	107	41,7	5,7	0
	4	625	574	204,3	18,9	0
	5	3 125	3 060	1 423,8	129,5	1 min
7	1	7	3	0,9	0,5	0
	2	49	30	8,8	1,8	0
	3	343	289	117,7	9,4	0
	4	2 401	2 243	883,8	47,5	19 s

wird fortgesetzt

Fortsetzung						
q	k	q^k	Länge	mittlerer Grad	mittlere Länge	Dauer
8	1	8	3	0,9	0,5	0
	2	64	29	8,7	1,0	0
	3	512	374	145,5	4,6	0
	4	4 096	2 690	927,7	12,3	12 s
9	1	9	3	0,9	0,4	0
	2	81	38	11,5	1,3	0
	3	729	555	223,1	6,9	0
	4	6 561	5 186	1 943,8	28,5	28 s

Anmerkungen zu den Spalteninhalten:

Spalte 5 – *mittlerer Grad*, Spalte 6 – *mittlere Länge*:

Es ist keine Aussage bekannt, die das Verschwinden irgendwelcher Koeffizienten der Inversen U^{-1} erzwingen würde. Daher wurden hier alle Koeffizienten bis zum jeweiligen Grad berücksichtigt.

Spalte 7 – *Dauer*:

Die angegebenen Zeiten beziehen sich rein auf die Invertierung von U, wenn die Potenzreihe U bereits vorliegt.

A.4 Daten zur Funktion h

Tabelle A.4: Statistische Daten zur Funktion h, Abschnitte bis q^k

q	k	q^k	Länge	mittlerer Grad	mittlere Länge	Dauer
2	1	2	3	0,7	1,7	0
	2	4	5	1,2	1,8	0
	3	8	8	2,7	2,1	0
	4	16	16	6,6	3,2	0
	5	32	32	14,2	5,7	0
	6	64	64	30,0	11,5	0
	7	128	128	62,0	23,6	0
	8	256	256	125,9	49,3	0
	9	512	512	253,9	103,2	21 s
	10	1 024	1 024	509,9	215,3	5 min
	11	2 048	2 048	1 021,9	444,1	2 h 19 min
	(12)	4 095	4 095	2 045,5	908,9	2 d 12 h 43 min
3	1	3	3	0,8	1,0	0
	2	9	8	2,1	1,4	0
	3	27	24	8,7	2,9	0
	4	81	78	33,1	7,3	0
	5	243	240	112,0	21,9	0
	6	729	726	354,4	71,6	0
	7	2 187	2 184	1 083,2	236,6	1 min 10 s
4	1	4	3	0,8	0,8	0
	2	16	11	3,1	1,2	0
	3	64	52	19,3	2,9	0
	4	256	230	102,4	7,8	0
	5	1 024	992	469,2	28,7	0
	6	4 096	4 062	1 995,4	126,7	24 s
5	1	5	3	0,8	0,7	0
	2	25	17	4,8	1,5	0
	3	125	106	42,7	5,6	0
	4	625	591	268,7	23,5	0
	5	3 125	3 084	1 496,1	142,5	25 s
7	1	7	3	0,9	0,5	0
	2	49	30	8,8	1,8	0
	3	343	288	117,7	9,4	0
	4	2 401	2 276	1 057,3	54,9	16 s

wird fortgesetzt

Fortsetzung						
q	k	q^k	Länge	mittlerer Grad	mittlere Länge	Dauer
8	1	8	3	0,9	0,5	0
	2	64	29	8,7	1,0	0
	3	512	374	146,2	4,5	0
	4	4 096	3 662	1 655,1	20,2	10 s
9	1	9	3	0,9	0,4	0
	2	81	38	11,5	1,3	0
	3	729	554	223,1	6,9	0
	4	6 561	6 052	2 772,5	39,7	18 s

Anmerkungen zu den Spalteninhalten:

Spalte 5 – *mittlerer Grad*, Spalte 6 – *mittlere Länge*:

Es können a priori alle Koeffizienten von h ungleich Null sein. Wie aus der Tabelle ersichtlich, trifft dies auf die meisten Koeffizienten auch wirklich zu. Aus diesem Grund wurden bei der Berechnung der Werte dieser Spalte alle Koeffizienten einbezogen.

Spalte 7 – *Dauer*:

Die angegebenen Zeiten beziehen sich rein auf die Berechnung von h gemäß der Multiplikation $h = U^{q^2} \cdot U^{-1}$, wenn die Funktionen U und U^{-1} bereits zur Verfügung stehen.

A.5 Daten zur Diskriminantenfunktion $\tilde{\Delta}$

Tabelle A.5: Statistische Daten zur Diskriminantenfunktion $\tilde{\Delta}$, Abschnitte bis q^k

q	k	q^k	mögl. Länge	Länge	mittl. Grad	mittl. Länge	Dauer
2	1	2	3	3	0,7	1,7	0
	2	4	5	5	1,2	1,8	0
	3	8	9	8	2,7	2,1	0
	4	16	17	16	6,6	3,2	0
	5	32	33	32	14,2	5,7	0
	6	64	65	64	30,0	11,5	0
	7	128	129	128	62,0	23,6	0
	8	256	257	256	125,9	49,3	0
	9	512	513	512	253,9	103,2	21 s
	10	1 024	1 025	1 024	509,9	215,3	5 min
	11	2 048	2 049	2 048	1 021,9	444,1	2 h 19 min
	(12)	4 095	4 096	4 095	2 045,5	908,9	2 d 13 h
3	1	3	3	3	1,0	1,3	0
	2	9	7	6	1,7	1,3	0
	3	27	19	16	7,1	2,2	0
	4	81	55	50	30,4	5,0	0
	5	243	163	158	107,1	14,0	0
	6	729	487	482	347,1	47,0	0
	7	2 187	1 459	1 454	1 075,1	165,1	2 min
	8	6 561	4 375	4 370	3 261,8	593,4	1 d 3 h
4	1	4	3	3	1,0	1,3	0
	2	16	9	6	1,7	1,3	0
	3	64	33	24	7,1	2,2	0
	4	256	129	112	89,5	4,7	0
	5	1 024	513	481	441,3	14,1	0
	6	4 096	2 049	2 010	1 939,9	58,4	1 min
	7	16 384	8 193	8 152	8 060,1	281,0	2 h 37 min
5	1	5	3	3	1,3	1,3	0
	2	25	11	6	2,7	0,8	0
	3	125	51	36	27,5	2,4	0
	4	625	251	221	229,1	9,1	0
	5	3 125	1 251	1 204	1 395,2	44,2	17 s
	6	15 625	6 251	6 197	7 576,9	316,1	51 min

wird fortgesetzt

Fortsetzung							
q	k	q^k	mögl. Länge	Länge	mittl. Grad	mittl. Länge	Dauer
7	1	7	3	3	2,3	1,3	0
	2	49	15	6	3,7	0,6	0
	3	343	99	64	69,8	2,8	0
	4	2 401	687	596	880,7	14,8	0
	5	16 807	4 803	4 610	7 590,7	104,8	1 min 30 s
8	1	8	3	3	2,7	1,3	0
	2	64	17	6	4,2	0,5	0
	3	512	129	69	84,7	1,7	0
	4	4 096	1 025	817	1 324,2	7,2	0
	5	32 768	8 193	7 585	14 002,2	35,4	30 s
9	1	9	3	3	3,0	1,3	0
	2	81	19	6	4,7	0,5	0
	3	729	163	88	123,1	2,1	0
	4	6 561	1 459	1 186	2 211,0	10,9	0
	5	59 049	13 123	12 363	25 947,5	72,0	3 min

Anmerkungen zu den Spalteninhalten:

Spalte 4 – *mögliche Länge*:

Nach Korollar 3.10 besitzt die Diskriminantenfunktion $\tilde{\Delta}$ ebenso wie die Produktfunktion U die Eigenschaft $(\mathrm{K}_{0,-1})$, d.h. es können nur solche Koeffizienten von Null verschieden sein, deren Index $\equiv 0, -1 \mod q$ ist. Daher beträgt die maximal mögliche Anzahl nichttrivialer Koeffizienten des Anfangssegments der Potenzreihe $\tilde{\Delta}$ bis zum Grad q^k

$$2 \cdot q^{k-1} + 1.$$

Spalte 6 – *mittlerer Grad*, Spalte 7 – *mittlere Länge*:

Es sind nur diejenigen Koeffizienten mit Index $\equiv 0, -1 \mod q$ berücksichtigt.

A.6 Dateigrößen

Tabelle A.6: Dateigrößen

q	Funktion	bis zum Grad	Größe in Megabyte
2	U_5	vollständig	0,1
2	U_6	vollständig	1,9
3	U_4	vollständig	0,5
4	U_4	vollständig	2,8
5	U_3	vollständig	0,2
7	U_3	vollständig	1,3
8	U_3	vollständig	2,3
9	U_3	vollständig	2,4
2	P_5	vollständig	0,5
2	P_6	vollständig	7,9
3	P_5	vollständig	3,6
4	P_5	vollständig	3,6
5	P_5	vollständig	5,7
7	P_5	vollständig	5,7
8	P_5	vollständig	3,9
9	P_5	vollständig	5,7
2	U^{-1}	$2^{11} = 2\,048$	1,5
3	U^{-1}	$3^7 = 2\,187$	2,0
4	U^{-1}	$4^6 = 4\,096$	1,1
5	U^{-1}	$5^5 = 3\,125$	2,0
7	U^{-1}	$7^4 = 2\,401$	0,6
8	U^{-1}	$8^4 = 4\,096$	0,3
9	U^{-1}	$9^4 = 6\,561$	1,0
2	h	4 095	18,6
3	h	$3^7 = 2\,187$	2,6
4	h	$4^6 = 4\,096$	2,6
5	h	$5^5 = 3\,125$	2,3
7	h	$7^4 = 2\,401$	0,7
8	h	$8^4 = 4\,096$	0,4
9	h	$9^4 = 6\,561$	1,4

wird fortgesetzt

Fortsetzung			
q	Funktion	bis zum Grad	Größe in Megabyte
2	$\tilde{\Delta}$	4 095	18,6
3	$\tilde{\Delta}$	$3^8 = 6\,561$	13,0
4	$\tilde{\Delta}$	$4^7 = 16\,384$	11,6
5	$\tilde{\Delta}$	$5^6 = 15\,625$	9,9
7	$\tilde{\Delta}$	$7^5 = 2\,401$	2,6
8	$\tilde{\Delta}$	$8^5 = 32\,768$	1,5
9	$\tilde{\Delta}$	$9^5 = 59\,049$	4,8

Die Angaben beziehen sich auf die Größe der berechneten Dateien in binärer (programminterner) Form. In Form von Textdateien haben die Daten etwa die zwei- bis dreifache Größe. Alle Polynome U_d aus Tabelle A.1, die oben nicht aufgeführt sind, belegen jeweils weniger als 100 KB.

Symbolverzeichnis

Literaturverzeichnis

[1] E. Freitag, R. Busam: *Funktionentheorie*. Springer, 2. Auflage 1995.

[2] K. Geddes, S. Czapor, G. Labahn: *Algorithms for Computer Algebra*. Kluwer 1996.

[3] E.-U. Gekeler, M. van der Put, M. Reversat, J. Van Geel: *Drinfeld Modules, Modular Schemes and Applications*. World Scientific 1997.

[4] E.-U. Gekeler: *On the Coefficients of Drinfeld Modular Forms*. Invent. Math. 93, 667-700 (1988).

[5] E.-U. Gekeler: *The Drinfeld Discriminant Function Revisited: Growth Order and Congruences of Coefficients*. J. Number Theory, eingereicht.

[6] D. Goss: *Basic Structures of Function Field Arithmetic*. Springer 1996.

[7] B. Lopez, B. Wack: *On the Expansion of a Product Formula Related with the Drinfeld Discriminant Function*. J. Number Theory, erscheint.

[8] M. Mignotte: *Mathematics for Computer Algebra*. Springer 1992.

[9] J.-P. Serre: *Cours d´Arithmétique*. Presses Universitaires de France 1970.

[10] C. Small: *Arithmetic of Finite Fields*. Marcel Dekker 1991.

[11] B. Stroustrup: *Die C++ Programmiersprache*. Addison-Wesley, 3. Auflage 1998.