Konstruktion fehlerkorrigierender Codes mit Hilfe torischer Flächen

Diplomarbeit

Vorgelegt im Fachbereich 3
(Mathematik & Informatik)
der Universität Bremen
im Wintersemester 2003 / 2004

von

Ina Bergen

Gutachter:

Prof. Dr. Jens Gamst (Universität Bremen)
Prof. Dr. Eberhard Oeljeklaus (Universität Bremen)

Inhaltsverzeichnis

Vorwort

Die Codierungstheorie entstand in der Mitte des 20. Jahrhunderts, sie ist also eine relativ neue Wissenschaft. Sie entstand im Zuge der Datenübermittlung über fehlerhafte Kanäle, wie zum Beispiel per Satellit. Bei dieser Art von Datenübertragung kommt es vor, dass Daten falsch übermittelt werden. Will man nun fehlerfreie Daten haben, muss man zusätzlich zur eigentlichen Information weitere Daten übermitteln, die dazu dienen, die Fehler im eigentlichen Datensatz zu erkennen und zu korrigieren. Eine einfache Möglichkeit ist zum Beispiel, die gleichen Daten mehrfach zu übermitteln. Da die Datenübertragung über große Entfernungen (per Satellit, vom Mond oder vom Mars…) aufwendig und teuer ist, versucht man, mit möglichst wenig zusätzlichen Daten möglichst viele Fehler zu korrigieren. Dies ist die Aufgabe der Codierungstheorie.

Um dieses Problem zu konkretisieren, muss man einige Begriffe erklären. Ein Code ist eine Menge von Worten gleicher Länge. Auf dieser Menge führt man einen Abstandsbegriff ein, indem man die Anzahl der Stellen zählt, an den sich zwei Worte unterscheiden. Der minimale Abstand zwischen zwei Worten des Codes wird als Minimaldistanz des Codes bezeichnet. Es ist anschaulich klar, dass man um so mehr Fehler mit einem Code korrigieren kann, je größer seine Minimaldistanz ist. Damit kann man die Aufgabenstellung der Codierungstheorie folgendermaßen formulieren: Gesucht wird ein Code, der bei fester Wortlänge möglichst viele Worte enthält (damit viel Information übermittelt werden kann) und eine möglichst große Minimaldistanz hat (damit viele Fehler korrigiert werden können). Die letzten beiden Bedingungen konkurrieren dabei miteinander, wie man sich leicht vorstellen kann: Je mehr Worte man zum Code hinzunimmt, desto kleiner wird der Abstand zwischen zwei Worten. Die drei charakteristischen Größen Länge, Wortanzahl und Minimaldistanz werden auch als Parameter des Codes bezeichnet, und man sagt, man suche eine Code mit "guten Parametern".

Einer der größten Durchbrüche auf diesem Gebiet gelang in der 80er Jahren des letzten Jahrhunderts, als man zum ersten Mal Codes mit Methoden der algebraischen Geometrie konstruierte. Dabei werden spezielle Funktionen auf algebraischen Kurven ausgewertet. Diese Codes haben gute Parameter, sie verbesserten die bisherigen Grenzen für Parameter zum ersten Mal seit 30 Jahren. Sie sind allerdings bislang noch ohne praktische Bedeutung.

Die Idee des Artikels "Toric Surfaces and Error-correcting Codes" von Johan P. Hansen aus dem Jahre 2002, welcher dieser Arbeit zugrunde liegt, ist es nun, algebraisch-geometrische Codes nicht durch Auswertung von Funktionen auf eindimensionalen Kurven, sondern auf zweidimensionalen Flächen zu erhalten. Dabei benutzt er eine besondere Art von Flächen, die sogenannten torischen Flächen. Diese sind der zweidimensionale Spezialfall einer torischen Varietät.

Der Grund für die Benutzung torischer Varietäten (im Gegensatz zu beliebigen Varietäten) liegt darin, dass sie eine besonders schöne explizite Beschreibung haben: Man kann zu einem Polytop im $\mathbb{R}^n$, also der konvexen Hülle von endlich vielen Punkten, in kanonischer Weise eine torische Varietät konstruieren. Die Eigenschaften des Polytops spiegeln sich in den Eigenschaften der Varietät wieder. Durch Beschränkung der Auswahl der Polytope kann man zum Beispiel erreichen, dass die Varietät stets glatt ist.

Die Codes, die mit Hilfe torischer Varietäten konstruiert werden, heißen torische Codes. Sie haben besonders gute Parameter. So berechnet zum Beispiel David Joyner in seinem Artikel [9], dass mit dieser Methode Codes erzeugt werden können, welche die bisherigen Schranken für Parameter verbessern.

Der Aufbau dieser Arbeit ist wie folgt:

Im ersten Kapitel werden Grundbegriffe der Codierungstheorie eingeführt. Es wird das Konzept des fehlerkorrigierenden Codes erklärt, und es werden Schranken für die maximale Anzahl von Worten eines Codes bei gegebener Wortlänge und Minimaldistanz angegeben.

Das zweite Kapitel widmet sich klassischen algebraisch-geometrischen Codes. Die theoretischen Grundlagen, algebraische Kurven, Divisoren auf Kurven und Differentiale auf Kurven, werden erklärt, und damit werden zwei algebraisch-geometrische Codes definiert: Die geometrischen Verallgemeinerungen des Reed-Solomon-Codes und des Goppa-Codes. Die klassische Theorie algebraischer Kurven wird hierbei nur zitiert, die zentralen Sätze werden ohne Beweis angegeben.

Im dritten Kapitel wird die Theorie der torischen Varietäten erklärt. Die Konstruktion affiner torischer Varitäten mit Hilfe von polyedrischen Kegeln (die durch das gegebene Polytop bestimmt sind) wird explizit durchgeführt, und es wird erklärt, wie man allgemeine torische Varietäten durch Zusammenkleben affiner torischer Varitäten erhält.

Gegenstand des vierten Kapitels sind die torischen Codes, die nach ihrem Erfinder auch als Hansen-Codes bezeichnet werden. Zunächst in Anlehnung an die Artikel [5] und [6] von Hansen werden die Codes allgemein eingeführt, und es werden für spezielle Codes Sätze über die Parameter bewiesen. Im letzten Abschnitt werden die Parameter der speziellen torischen Codes noch zur Gilbert-Varshamov-Schranke, einer unteren Schranke für die maximale Anzahl der Elemente eines Codes, in Beziehung gesetzt.

Die ersten beiden Kapitel sollen dem Leser die Grundlagen der Codierungstheorie sowie die Idee der klassischen algebraisch-geometrischen Codes nahebringen. Die Inhalte findet man in jüngeren Lehrbüchern der Codierungstheorie, zum Beispiel dem Standardwerk "Introduction to Coding Theory" von J.H. van Lint aus dem Jahre 1981 und dem erst 2003 erschienenen Lehrbuch "Codierungstheorie" von W. Lütkebohmert. Das Hauptaugenmerk der Arbeit liegt auf den Kapiteln drei und vier, in denen die Theorie torischer Varietäten eingeführt und auf das konkrete Problem der Hansen-Codes angewandt wird.

Ich möchte Jens Gamst herzlich für seine hervorragende Betreuung danken. Durch seine Hilfsbereitschaft und Kompetenz hat es viel Spaß gemacht, dieses Thema zu bearbeiten.

Weiterhin möchte ich mich bei meiner Arbeitsgruppe, der WE AℓZAGK (Algorithmische Zahlentheorie, Algebraische Geometrie und Kryptologie), bedanken. Im Rahmen des Arbeitsgruppenseminars haben wir dort die ersten Grundlagen der Theorie torischer Varietäten behandelt.

Für das fleissige Fehlerlesen möchte ich neben Jens Gamst auch Tobias Rieck danken. Eventuelle Fehler, die sich dennoch eingeschlichen haben, habe ich mit großer Wahrscheinlichkeit nachträglich eingebaut... Meinen Eltern danke ich für die unkomplizierte Unterstützung meines Studiums.

Kapitel 1

Fehlerkorrigierende Codes

1.1 Grundlagen

1.1.1 Einleitung

Der Ursprung der Codierungstheorie ist folgendes Problem: Wird eine Datenmenge über einen Kanal (zum Beispiel per Satellit) versendet, werden die Daten durch Rauschen verändert. Die Codierungstheorie hat nun die Aufgabe, die auftretenden Fehler zu erkennen und zu korrigieren. Dazu werden beim Codieren den vorhandenen Daten weitere, redundante Informationen hinzugefügt. Diese ermöglichen es, beim Decodieren Fehler zu erkennen und eventuell sogar zu korrigieren. Die zusätzliche Information sorgt nämlich dafür, dass die erlaubten Codewörter so verschieden sind, dass in der Nähe einer übertragenen Datenmenge jeweils nur genau ein Codewort liegt.

Beispiel: ISBN

Jedes in den USA und Westeuropa erscheinende Buch erhält zur Identifikation die Internationale Standard-Buchnummer (ISBN). Diese besteht aus zehn Ziffern, wobei an der letzten Stelle auch ein X (stellvertretend für die Zahl 10) stehen kann. Die eigentliche Buchnummer besteht aus den ersten neun Ziffern. Die zehnte Ziffer wird dann so gewählt, dass für die ISBN $a_1 a_2 \ldots a_{10}$ gilt:

$$1a_1 + 2a_2 + 3a_3 + \cdots + 10a_{10} \equiv 0 \mod 11$$

Zum Beispiel ist 3-528-03197-2 eine gültige ISBN, denn

$$1 \cdot 3 + 2 \cdot 5 + 3 \cdot 2 + 4 \cdot 8 + 5 \cdot 0 + 6 \cdot 3 + 7 \cdot 1 + 8 \cdot 9 + 9 \cdot 7 + 10 \cdot 2 = 231 = 21 \cdot 11.$$

Fehler an genau einer Stelle der Nummer werden mit dieser Methode stets erkannt, Fehler an zwei Stellen können sich dagegen aufheben. Kennt man die Stelle, an der der Fehler vorliegt, kann dieser sogar korrigiert werden. Wäre von der oben genannten ISBN etwa die zweite Stelle unleserlich, so müsste man eine Zahl $a \in \{0, \ldots, 9\}$ finden, so dass $2a + 221 \equiv 0 \mod 11$ ist. Diese Aufgabe hat in $\mathbb{F}_{11}$, dem Körper mit 11 Elementen, genau eine Lösung, nämlich $a = 5$.

1.1.2 Definitionen

Sei p eine Primzahl und $l \in \mathbb{N}_{>0}$. Für die Primzahlpotenz $q = p^l$ betrachten wir den Körper $\mathbb{F}_q$ mit q Elementen und darüber den n-dimensionalen Vektorraum $\mathbb{F}_q^n$. Zunächst brauchen wir ein Maß für die Größe der auftretenden Fehler.

1.1.1. Definition

Für $x \in \mathbb{F}_q^n$ definiert man die *Hamming-Norm* (bzw. das *Hamming-Gewicht*) als die Anzahl der von Null verschiedenen Komponenten:

$$w(x) = w(x_1, \ldots, x_n) = {}^{\#}\{1 \leq i \leq n : x_i \neq 0\}$$

Damit hat man auch eine Abstandsfunktion auf $\mathbb{F}_q^n$,

$$d_H(x, y) := w(x - y),$$

die sogenannte *Hamming-Distanz* von x und y.

1.1.2. Bemerkung

Die Hamming-Distanz ist eine Metrik, denn man rechnet leicht nach:

1. $d(x, y) = 0 \iff x = y$
2. $d(x, y) = d(y, x)$
3. $d(x, z) \leq d(x, y) + d(y, z)$

1.1.3. Bemerkung

Die Hamming-Distanz ist translationsinvariant:

$$d_H(x+z, y+z) = d_H(x, y)$$

1.1.4. Bemerkung

Trotz der Bezeichung Hamming-Norm ist das Hamming-Gewicht im allgemeinen keine Norm, denn für $\lambda \in \mathbb{F}_q^*$ gilt $w(\lambda x) = w(x) \neq \lambda w(x)$ für $\lambda \neq 1$ und $\omega(x) \neq 0$.

1.1.5. Definition

1. Ein *Code* ist eine Teilmenge $\mathcal{C}$ von $\mathbb{F}_q^n$. Die Elemente von $\mathcal{C}$ heissen *Codewörter*, n wird als *Wortlänge* oder *Blocklänge* von $\mathcal{C}$ bezeichnet.
2. Ist ein Code $\mathcal{C}$ ein Untervektorraum von $\mathbb{F}_q^n$, so heisst $\mathcal{C}$ *linearer Code* über $\mathbb{F}_q$. Hat $\mathcal{C}$ über $\mathbb{F}_q$ die Dimension k, so ist $\mathcal{C}$ ein $[n, k]$-Code über $\mathbb{F}_q$.
3. Die *Minimaldistanz* eines Codes $\mathcal{C}$ wird definiert als:
$$d(\mathcal{C}) := \min\{d_H(x, y); x, y \in \mathcal{C}, x \neq y\}.$$
4. Ein linearer Code $\mathcal{C}$ über $\mathbb{F}_q$ mit Blocklänge n, Dimension k und Minimaldistanz d heißt $[n, k, d]$-Code.
5. Die *Informationsrate* eines linearen Codes ist k/n.

1.1.6. Bemerkung

Wir betrachten hier nur lineare Codes. Aufgrund der Translationsinvarianz der Hamming-Distanz läßt sich die Minimaldistanz in diesem Fall auf den minimalen Abstand zum Nullpunkt zurückführen:

$$\begin{aligned} d(\mathcal{C}) &= \min\{d_H(x,y); x,y \in \mathcal{C}, x \neq y\} \\ &= \min\{d_H(x-y,0); x,y \in \mathcal{C}, x \neq y\} \\ &= \min\{d_H(z,0); z \in \mathcal{C}, z \neq 0\} \\ &= \min\{w(z); z \in \mathcal{C}, z \neq 0\} \end{aligned}$$

1.1.7. Lemma

Sei $\mathcal{C}$ ein Code mit Minimaldistanz $2e+1$, $e \in \mathbb{N}$. Sei nun $z \in \mathbb{F}_q^n$ ein übermitteltes Wort, bei dem Fehler an höchstens e Stellen vorliegen. Dann existiert genau ein Codewort $x \in \mathcal{C}$ mit $d(x,z) \leq e$.

Beweis:

Die Existenz ist per Konstruktion klar. Sei $y \neq x$ ein weiteres Codewort. Dann gilt (mit Dreiecksungleichung)

$$d(y,z) \geq \underbrace{d(x,y)}_{\geq 2e+1} - \underbrace{d(x,z)}_{\leq e} \geq e+1.$$

$\not\$$

Aufgrund dieser Tatsache definiert man:

1.1.8. Definition

Ein Code $\mathcal{C}$ heißt *e-fehlerkorrigierend* für $e \in \mathbb{N}$, wenn für alle $x, y \in \mathcal{C}$ mit $x \neq y$ gilt

$$d_H(x, y) \geq 2e + 1$$

Eine Möglichkeit, einen Code zu beschreiben, ist die Angabe einer Basis von $\mathcal{C}$. Die Basisvektoren fasst man dann als Zeilen einer Matrix auf.

1.1.9. Definition

Sei $\mathcal{C}$ ein $[n, k]$-Code. Eine $(k \times n)$-Matrix, deren Zeilen eine Basis von $\mathcal{C}$ bilden, heißt *Erzeugermatrix* oder *Generatormatrix* von $\mathcal{C}$.

Selbstverständlich ist die Wahl der Basis nicht eindeutig. Durch eventuelles Spaltenvertauschen (d.h. Umnumerieren der Koordinaten) und Gauss-Algorithmus erreicht man, dass die Generatormatrix eines Codes in sogenannter reduzierter Form gewählt werden kann:

$$G = [E_k | P] = \left[\begin{array}{ccc|c} 1 & & 0 & \\ & \ddots & & P \\ 0 & & 1 & \end{array}\right]$$

Dabei ist E_k die $(k \times k)$-Einheitsmatrix und P eine $(k \times (n-k))$-Matrix.

Ist ein Code in dieser reduzierten Form gegeben, so gibt es zu jedem vorgegebenen k-Tupel $x_1, \ldots, x_k \in \mathbb{F}_q$ genau ein Codewort, dessen erste k Stellen mit den gegebenen übereinstimmen. Die restlichen Stellen sind dann eindeutig bestimmt und können zur Fehlererkennung bzw. Fehlerkorrektur benutzt werden.

1.1.10. Definition

Die Koordinaten $x_{k+1}, \ldots, x_n$ eines Codewortes bezüglich einer reduzierten Basis heißen *Kontrollsymbole* oder *parity check symbols*.

Um nun aus dem ursprünglichen Wort $x = (x_1, \ldots, x_k)$ das Codewort $\tilde{x} = (x_1, \ldots, x_k, k_1, \ldots, k_{n-k})$ mit Kontrollsymbolen $k_1, \ldots, k_{n-k}$ zu erhalten, multipliziert man x mit der Erzeugermatrix, und zwar von rechts:[1]

$$^t(x') = {}^t x \cdot G$$

Aus dem Codewort erhält man dann wieder das Klartextwort, indem man die Kontrollsymbole weglässt.

Natürlich kann man den Untervektorraum $\mathcal{C}$ auch durch lineare Gleichungen angeben. $\mathcal{C}$ ist die Lösung eines homogenen linearen Gleichungssystems mit $(n-k)$ linear unabhängigen Gleichungen. Sei dieses durch die Matrix H gegeben. Dann gilt also für $x \in \mathbb{F}_q^n$:

$$x \in \mathcal{C} \iff Hx = 0$$

Insbesondere gilt für die Erzeugermatrix G von $\mathcal{C}$:

$$H \cdot {}^t G = 0.$$

1.1.11. Definition

Eine solche Matrix H heißt *Kontrollmatrix* oder *parity check matrix.*

Hat man die Erzeugermatrix in reduzierter Form gegeben, so läßt sich eine Kontrollmatrix sofort explizit angeben:
Zur Erzeugermatrix $G = [E_k|P]$ ist $H = [-{}^t P|E_{n-k}]$ eine Kontrollmatrix.

Nun soll die Fehlerkorrektur explizit ausgeführt werden. Für lineare Codes entspricht das dem folgenden Problem:

Zu $y \in \mathbb{F}_q^n$ sucht man ein $c \in \mathcal{C}$, so dass $\nu = y - c$ minimale Hamming-Norm hat.

[1] Dies ergibt sich aus der bedauerlichen Tatsache, dass die Basisvektoren in den Zeilen von G stehen.

ν ist offenbar ebenfalls ein Element der Nebenklasse $y + \mathcal{C}$, und da alle Elemente dieser Nebenklasse mit demselben Fehlervektor decodiert werden können, sucht man in jeder Nebenklasse einen festen Vektor minimaler Hamming-Norm.

1.1.12. Definition

Einen Vektor minimaler Hamming-Norm in einer Nebenklasse von $\mathcal{C}$ bezeichnet man als *Nebenklassenleitterm* oder *Nebenklassenführer*, auf englisch *coset leader*.

1.1.13. Bemerkung

Der Nebenklassenleitterm ist im allgemeinen nicht eindeutig bestimmt.

Ist H eine Kontrollmatrix, so befinden sich die Vektoren $x, y \in \mathbb{F}_q^n$ genau dann in derselben Nebenklasse, wenn $Hx = Hy$ gilt (denn dann ist $x - y \in \mathcal{C}$ und also $H(x - y) = 0$). Dieses Kriterium wird zur Einteilung der Vektoren in die Nebenklassen benutzt.

1.1.14. Definition

Sei $x \in \mathbb{F}_q^n$ und H eine Kontrollmatrix des Codes $\mathcal{C}$. Der Vektor $Hx \in \mathbb{F}_q^{n-k}$ wird als *Syndrom von x* bezeichnet.

Die Fehlerkorrektur eines Vektors $x \in \mathbb{F}_q^n$ erfolgt dann folgendermaßen:

- Zunächst wird $z = Hx$ berechnet. Ist $z = 0$, ist x bereits ein Codewort, und damit ist die Fehlerkorrektur beendet.
- Ist $z \neq 0$, wählt man zu z einen Nebenklassenleitterm ν_z mit $H\nu_z = z$.
- Der Vektor $x \in \mathbb{F}_q^n$ mit Syndrom $z \in \mathbb{F}_q^{n-k}$ wird dann korrigiert zu $x - \nu_z$.

1.1.3 Hamming-Codes

Ein wichtiges Beispiel für einen fehlerkorrigierenden Code sind die Hamming-Codes. Zunächst soll ein Beispiel für einen Hamming-Code vorgestellt werden, dann werden die Hamming-Codes allgemein definiert.

1.1.3.1 Beispiel für einen Hamming-Code

Betrachtet wird ein Code, bei dem pro Codewort 4 Bit Information verschickt werden. An diese 4 Bit werden weitere 3 Bit zur Fehlerkorrektur angehängt, es handelt sich also um einen binären $[7,4]$-Code: $\mathcal{C} \subset \mathbb{F}_2^7$.

Das Codierungsschema ist dabei wie folgt: Ist das zu codierende Wort $v_1v_2v_3v_4$, so wird es codiert zu $v_1v_2v_3v_4k_1k_2k_3$ mit $k_1 = v_1 + v_3 + v_4$, $k_2 = v_1 + v_2 + v_4$ und $k_3 = v_1 + v_2 + v_3$.

Eine vollständige Liste der Codewörter ist dann:

uncodiert	codiert	uncodiert	codiert
0000	0000000	1000	1000111
0001	0001110	1001	1001001
0010	0010101	1010	1010010
0011	0011011	1011	1011100
0100	0100011	1100	1100100
0101	0101101	1101	1101010
0110	0110110	1110	1110001
0111	0111000	1111	1111111

Da in jedem Codewort $\neq 0$ die 1 mindestens dreimal auftritt, hat der $[7,4]$-Hamming-Code die Minimaldistanz 3, er ist also 1-fehlerkorrigierend.

Eine Basis für $\mathcal{C}$ erhält man, indem man die Standardbasisvektoren des $\mathbb{F}_2^4$ entsprechend des Codierungsschemas zu Vektoren des $\mathbb{F}_2^7$ erweitert. Man erhält: $f_1 = (1,0,0,0,1,1,1)$, $f_2 = (0,1,0,0,0,1,1)$, $f_3 = (0,0,1,0,1,0,1)$ und $f_4 = (0,0,0,1,1,1,0)$.

Damit erhält man als Generatormatrix:

$$G = \left[\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$$

Nach dem allgemeinen, oben beschriebenen Verfahren ergibt sich damit folgende Kontrollmatrix:

$$H = \left[\begin{array}{cccc|ccc} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]$$

Der $[7,4]$-Hamming-Code läßt sich mit dem folgenden Bild veranschaulichen:

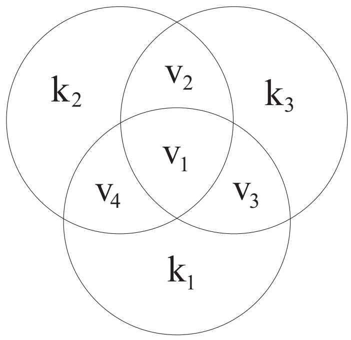

Bild 1.1.

k_1, k_2 und k_3 werden dabei so bestimmt, dass in jedem Kreis die Summe der Einträge gleich Null ist.

An dieser Darstellung kann die Fehlerkorrektur nun anschaulich durchgeführt werden: Weiss man, dass genau einer der Werte v_1, v_2, v_3 oder v_4 verändert wurde, so ist die Summe entweder in zwei Kreisen oder in allen drei Kreisen ungleich Null. Im folgenden Beispiel ist die Summe nur in den oberen Kreisen ungleich Null, daher ist v_2 verändert worden:

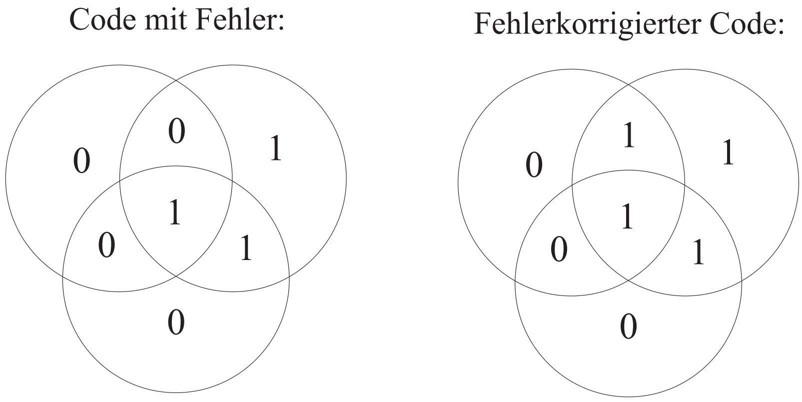

Bild 1.2. Fehlerkorrektur beim $[7,4]$-Hamming-Code.

Die Informationsrate des Codes beträgt $4/7$. Hätte man statt des $[7,4]$-Hamming-Codes jeden Bitstring einfach dreimal gesendet (was ebenfalls 1-fehlerkorrigierend wäre), hätte die Informationsrate nur $1/3$ betragen. Trotz seiner einfachen Struktur ist der Code also recht effektiv. In der Praxis ist er jedoch kaum zu gebrauchen, da oft mehr als ein Fehler vorkommt.

1.1.3.2 Definition und Eigenschaften der Hamming-Codes

1.1.15. Definition

Sei $q = p^l$ mit p prim, $l \in \mathbb{N}_{>0}$. Für ein $r \in \mathbb{N}_{>0}$ setze man $n = (q^r - 1)/(q-1)$. Ein linearer $[n, n-r]$-Code heißt *Hamming-Code*, wenn die Kontrollmatrix H paarweise linear unabhängige Spalten hat.

1.1.16. Bemerkung

Die Spalten der Kontrollmatrix sind Elemente des $\mathbb{F}_q^r$. Die Tatsache, dass diese paarweise linear unabhängig sind, bedeutet, dass jedes Paar von Spalten verschiedene Geraden im F_q^r definiert. Da es im $\mathbb{F}_q^r$ genau $(q^r-1)/(q-1)$ Geraden durch den Nullpunkt gibt, ist n also maximal mit dieser Eigenschaft.

1.1.17. Bemerkung

Die Existenz von Hamming-Codes läßt sich konstruktiv zeigen: Man schreibt Basisvektoren der Geraden im $\mathbb{F}_q^r$ auf, sortiert so, dass die r Standardbasisvektoren am Ende stehen, und erhält damit eine Kontrollmatrix der Form

$$[R|E_r].$$

Wie wir oben gesehen haben, ist die Matrix

$$[E_{n-r}| - {}^tR]$$

dann eine Erzeugermatrix des Codes.

1.1.18. Satz

Hamming-Codes haben Minimaldistanz 3 und sind also 1-fehlerkorrigierend.

Beweis:

Dies wird indirekt bewiesen.

Annahme: Es gibt Elemente der Hamming-Norm 1 oder 2.

1. Sei x ein Element mit Hamming-Norm 1, dann hat x nur einen Eintrag ungleich Null, sei dieser an der i-ten Stelle. Dann ist die i-te Spalte der Kontrollmatrix gleich Null. Die Spalten der Kontrollmatrix sind aber linear unabhängig. $\lightning$

2. Sei y ein Element mit Hamming-Norm 2, dann hat y genau zwei Einträge ungleich Null, etwa an der i-ten und j-ten Stelle. Dann sind die Spalten i und j der Kontrollmatrix linear abhängig. $\lightning$

Allerdings gibt es stets ein Element mit Hamming-Norm 3, da z.B. die Vektoren e_1, e_2 und $e_1 + e_2$ stets zulässige Spalten einer Kontollmatrix sind und diese einen Vektor mit Hamming-Norm 3 annuliert.

$

Die Fehlerkorrektur des Hamming-Codes ist nun denkbar einfach: Sei ein empfangenes y kein Codewort, also $Hy \neq 0$. Dann ist Hy per Konstruktion des Hamming-Codes ein Vielfaches von genau einer Spalte von H, etwa der Spalte i: $Hy = \lambda h_i$. Die i-te Spalte von H ist aber $H \cdot e_i$, also ist λe_i in der gleichen Nebenklasse wie y und daher offensichtlich ein zugehöriger Nebenklassenleitterm. y wird also zu $y - \lambda e_i$ korrigiert.

1.2 Schranken für Codes

Sei $\mathbb{F}_q$ unser Codierungsalphabet. Um die Übertragungsrate eines Codes zu maximieren, soll zu vorgegebenen natürlichen Zahlen n und d eine Zahl M maximal bestimmt werden, so dass ein (n, M, d)-Code existiert.

Dieses M ist in der Praxis oft nicht explizit zu bestimmen, aber man kann obere und untere Schranken angeben. Offensichtlich ist M nach oben durch die Anzahl der Elemente von $\mathbb{F}_q^n$ beschränkt: $M \leq q^n$. Daher existiert stets so ein maximales M.

1.2.1. Definition

$A(n, d) = \max\{M \in \mathbb{N} |\text{ ein } (n, M, d) - \text{Code existiert}\}$.
Ein (n, M, d)-Code mit $M = A(n, d)$ wird *optimal* genannt.

1.2.2. Bemerkung

Lineare $[n, k, d]$-Codes mit $M = q^k$ heißen optimal, wenn $d = n-k+1$ gilt. Wir werden im Abschnitt über obere Schranken sehen, dass solche Codes tatsächlich im eben definierten Sinne optimal sind.

In der Praxis sind vor allem Codes großer Länge von Bedeutung, da solche die Wahrscheinlichkeit eines Übertragungsfehlers reduzieren. Ist p die Wahrscheinlichkeit, an einer Stelle eines Wortes einen falschen Buchstaben zu übertragen, so passieren in einem Wort der Länge n im Durchschnitt np Fehler. Betrachtet man nun Codes wachsender Länge n, dann muss d mindestens so schnell wie $2np$ wachsen, damit man die Fehler korrigieren kann. Daher definiert man als asymptotische Variante von $A(n, d)$:

1.2.3. Definition

$\alpha(\delta) = \limsup_{n \to \infty} n^{-1} \log_q A(n, n\delta)$.

Die Funktionen A und α lassen sich im allgemeinen nicht explizit angeben. In diesem Abschnitt wollen wir untere und obere Schranken für sie vorstellen.

Ein praktisches technisches Hilfsmittel zum Zählen der Punkte eines Codes sind Kugeln bezüglich der Hamming-Distanz:

1.2.4. Definition

Die Kugel vom Radius r um x wird definiert als

$$B_r(x) = \{y \in \mathbb{F}_q^n \mid d(x,y) \leq r\}.$$

Die Anzahl der Punkte einer Kugel im $\mathbb{F}_q^n$ wird mit $V_q(n,r)$ bezeichnet:

$$V_q(n,r) = {}^{\#}B_r(x).$$

1.2.5. Lemma

$$V_q(n,r) = \sum_{i=0}^{r} \binom{n}{i} (q-1)^i$$

Beweis:

Zu zählen sind jeweils die Vektoren, die sich an i Stellen von x unterscheiden. Für die Auswahl der Stellen gibt es $\binom{n}{i}$ Möglichkeiten. An jeder dieser Stellen kann ein von x verschiedener Vektor $(q-1)$ Werte annehmen.

$\#$

1.2.6. Bemerkung

Man beachte, dass $V_q(n,r)$ nicht von x abhängig ist.

1.2.1 Untere Schranken

1.2.7. Satz (Gilbert-Varshamov-Schranke)

Für $d, n \in \mathbb{N}$ mit $d \leq n$ gilt

$$A(n,d) \geq \frac{q^n}{V_q(n, d-1)}$$

Beweis:

Sei $\mathcal{C}$ ein optimaler (n, M, d)-Code. Dann gibt es kein Element von $\mathbb{F}_q^n$, das zu allen Elementen von $\mathcal{C}$ einen Abstand $\geq d$ hat. Also wird $\mathbb{F}_q^n$ von den Kugeln um Elemente aus $\mathcal{C}$ vom Radius $d-1$ überdeckt. Summiert man deren Ordnungen, erhält man also wenigstens soviele Elemente wie die von $\mathbb{F}_q^n$:

$$M \cdot V_q(n, d-1) \geq q^n.$$

1.2.8. Bemerkung

Obwohl die Forderung nach der Linearität eines Codes auf den ersten Blick als starke Einschränkung erscheint, läßt sich mit Hilfe dieses Satzes beweisen, dass zu einer gegebenen unteren Schranke für $A(n, d)$ auch lineare Codes existieren.[2]

1.2.9. Korollar (Asymptotische Gilbert-Varshamov-Schranke)

Für $\delta = d/n$ gilt $\alpha(\delta) \geq 1 - \lim_{n\to\infty} n^{-1} \log_q V_q(n, \delta n)$.

[2] siehe [11], §5.1.

Beweis:

Das ist eine direkte Konsequenz der Gilbert-Varshamov-Schranke für $A(n, d)$.

$\ddagger$

1.2.10. Bemerkung

Obwohl die Gilbert-Varshamov-Schranke so trivial ist, galt sie lange als gut, die asymptotische Variante wurde sogar für exakt gehalten. 1982 verbesserten Tsfasman, Vladut und Zink die asymptotische Gilbert-Varshamov-Schranke mit Methoden der algebraischen Geometrie. [3]

1.2.2 Obere Schranken

1.2.11. Satz (Singleton-Schranke)

Für $n, d, q \in \mathbb{N}$ mit $q \geq 2$ gilt

$$A(n, d) \leq q^{n-d+1}.$$

Beweis:

Punktiert man einen (n, M, d)-Code $(d-1)$-mal (d.h. man läßt $d-1$ Koordinaten weg), bleiben alle Codewörter voneinander verschieden, also erhält man einen $(n-d+1, M, \tilde{d})$-Code mit $\tilde{d} \geq 1$. Daher gilt

$$M \leq q^{n-d+1}.$$

$\ddagger$

[3] siehe [15].

1.2.12. Bemerkung

Für einen linearen $[n, k, d]$-Code mit $M = q^k$ folgt damit $k \leq n-d+1$. Also sind optimale lineare Codes tatsächlich optimal im Sinne der Definition auf Seite 12.

Die asymptotische Variante der Singleton-Schranke folgt wiederum direkt aus der endlichen, sie lautet:

1.2.13. Korollar

Für alle $\delta \in [0, 1]$ gilt $\alpha(\delta) \leq 1 - \delta$.

1.2.14. Satz (Hamming-Schranke)

Für $q, n, e \in \mathbb{N}$, $q \geq 2$, $d = 2e + 1$ gilt

$$A(n, d) \leq \frac{q^n}{V_q(n, e)}.$$

Beweis:

Sei $\mathcal{C}$ ein $(n, M, 2e + 1)$-Code. Dann sind die Kugeln $B_e(x)$ mit $x \in \mathcal{C}$ disjunkt. Also ist die Summe der Elemente dieser Kugeln höchstens q^n:

$$M \cdot V_q(n, e) \leq q^n.$$

$\$$

Kapitel 2

Algebraisch-geometrische Codes

In den 80er Jahren des vorigen Jahrhunderts wurden zum ersten Mal Methoden der algebraischen Geometrie zur Entwicklung fehlerkorrigierender Codes benutzt. Damit wurden Codes mit guten Parametern, also hohen Übertragungsraten erzeugt. Diese Codes sind bislang noch ohne praktische Bedeutung.

Die Codewörter werden hierbei definiert, indem man rationale Funktionen mit Polen beschränkter Ordnung in gewissen Punkten auswertet. Konkretisiert wird der Begriff der „Pole beschränkter Ordnung“ durch das Konzept der Divisoren.

Im letzten Abschnitt dieses Kapitels sollen zwei Beispiele für algebraisch-geometrische Codes vorgestellt werden.

Der Zweck dieses Kapitel ist es, das Prinzip der Codes auf algebraischen Kurven vorzustellen, damit man im vierten Kapitel die Analogie der torischen Codes zu den klassischen algebraisch-geometrischen Codes sieht. Die wichtigen Sätze werden ohne Beweis angegeben. Inhaltlich orientiert sich das Kapitel im Wesentlichen an [11], [12] und [14], wo auch die meisten Beweise zu finden sind.

2.1 Algebraische Kurven

Im Folgenden sei k stets ein algebraischer Abschluss von $\mathbb{F}_q$.

$\mathbb{A}^n = \mathbb{A}^n(k)$ ist der n-dimensionale affine Raum mit Koordinaten $x_1, \ldots, x_n$ mit $x_i \in k$. $\mathbb{P}^n = \mathbb{P}^n(k)$ ist der n-dimensionale projektive Raum mit homogenen Koordinaten $x_0, x_1, \ldots, x_n$ mit $x_i \in k$.

2.1.1. Definition

Eine *affine Varietät* ist die Nullstellenmenge endlich vieler Polynome:

$$C(f_1, \ldots, f_s) = \{x \in \mathbb{A}^n | f_j(x) = 0 \text{ für } j = 1, \ldots, s\}$$

mit $f_j \in k[X_1, \ldots, X_n]$.
Eine *projektive Varietät* ist die Nullstellenmenge endlich vieler homogener Polynome:

$$C(F_1, \ldots, F_s) = \{[x] \in \mathbb{P}^n | F_j(x) = 0 \text{ für } j = 1, \ldots, s\}$$

mit $F_j \in k[X_0, \ldots, X_n]$ homogen.

In diesem Kapitel sollen nur ebene Kurven betrachtet werden, also eindimensionale Untervarietäten des $\mathbb{A}^2$ oder $\mathbb{P}^2$. Im affinen Fall ist eine Kurve die Nullstellenmenge einer Gleichung in zwei Variablen, im projektiven Fall die Nullstellenmenge einer homogenen Gleichung in drei Variablen.

Eine Varietät heißt *irreduzibel*, wenn man sie nicht in nichttrivialer Weise als Vereinigung zweier Varietäten schreiben kann. In diesem Kapitel sollen nur irreduzible Varietäten betrachtet werden.

2.1.2. Definition

Sei $\wp$ ein Primideal in $k[x_1, \ldots, x_n]$ und C die Nullstellenmenge von $\wp$. Der Ring $k[x_1, \ldots, x_n]/\wp$ wird als *Koordinatenring* $k[C]$ der Varietät C bezeichnet.

2.1.3. Bemerkung

C ist eine Varietät im oben definierten Sinne, da die Nullstellenmenge von $\wp$ durch endlich viele Polynome erzeugt wird.

2.1.4. Bemerkung

Im affinen Fall werden die Elemente des Koordinatenrings *Polynomfunktionen* genannt.
Im projektiven Raum $\mathbb{P}^n$ ist es nicht sinnvoll, von Polynomfunktionen zu sprechen, da diese in einem Punkt mit homogenen Koordinaten nicht wohldefiniert sind.

2.1.5. Definition

Der Quotientenkörper des Koordinatenringes einer affinen Varietät C ist der *Körper der rationalen Funktionen*. Er wird mit $k(C)$ bezeichnet.

Rationale Funktionen im projektiven Raum sind Quotienten von homogenen Polynomen gleichen Grades.

2.1.6. Definition

Sei C eine affine oder projektive Varietät, und seinen f und g Polynome auf C (im projektiven Fall: homogen vom selben Grad). Sei $P \in C$ und $g(P) \neq 0$. Dann ist die Funktion f/g *regulär* im Punkt P.

2.1.7. Definition

Der *lokale Ring* O_p der Varietät C im Punkte P ist die Menge der rationalen Funktionen auf C, die in P regulär sind.

2.1.8. Bemerkung

Der lokale Ring einer Varietät ist tatsächlich ein lokaler Ring im algebraischen Sinne, denn er hat genau ein maximales Ideal:

$$m_P = \{f \in O_P | f(P) = 0\}.$$

Sei C eine affine Kurve mit der Gleichung $F(x, y) = 0$, sei $P = (a, b)$ ein Punkt der Kurve. Ist eine der beiden partiellen Ableitungen F_x oder F_y ungleich Null in P, so ist P ein *nichtsingulärer Punkt*. Dann hat die Kurve einen Tangententialraum T_P im Punkt P, definiert durch die Gleichung

$$d_P F := F_x(a, b)(x - a) + F_y(a, b)(y - b) = 0$$

Besteht eine Kurve nur aus nichtsingulären Punkten, bezeichnet man sie als *glatt*. In diesem Abschnitt sollen nur glatte Kurven betrachtet werden, da man in diesem Fall in jedem Punkt der Kurve einen lokalen Parameter hat.[1] Eine Funktion t ist ein lokaler Parameter im Punkt P, wenn $d_P t$ auf T_P ungleich Null ist. Jedes Element z von O_P läßt sich dann schreiben als $z = u \cdot t^m$, wobei u eine Einheit (also ein invertierbares Element aus O_P) ist und $m \in \mathbb{N}$ eindeutig bestimmt ist und nicht von der Wahl des lokalen Parameters abhängt.

2.1.9. Definition

1. Sei K ein Körper. Eine *diskrete Bewertung* auf K ist eine Funktion $v : K^\times \to \mathbb{Z}$, die folgende Eigenschaften erfüllt.
   (a) v ist surjektiv.
   (b) $v(xy) = v(x) + v(y)$ für alle $x, y \in K^\times$.
   (c) $v(x + y) \geq \min\{v(x), v(y)\}$ für alle $x, y \in K^\times$ mit $x + y \neq 0$.

   Der Unterring $\{x \in K | v(x) \geq 0\} \cup \{0\}$ ist der *Bewertungsring* von v.
2. Ein Integritätsbereich R ist ein *diskreter Bewertungsring*, wenn R der Bewertungsring einer diskreten Bewertung auf dem Quotientenkörper von R ist.

[1] siehe etwa [11], §10.2.

Sei f ein Element des lokalen Ringes im Punkte P, und gelte $f = u \cdot t^m$ für einen lokalen Parameter in P. Dann kann man im Punkt P definieren: $v_P(f) = m$. Ist $m > 0$, so hat f eine Nullstelle der Ordnung m in P.

Der Körper $k(C)$ der rationalen Funktionen ist der Quotientenkörper des lokalen Ringes O_P. Die Bewertung v_P läßt sich auf $k(C)$ erweitern per

$$v_P(f/g) = v_P(f) - v_P(g).$$

Ist $v_P(f/g) = m < 0$, so hat f/g einen Pol der Ordnung m in P.

Damit sind die lokalen Ringe glatter Kurven stets diskrete Bewertungsringe.

2.1.10. Definition

Sei V eine Kurve über $\mathbb{F}_q$. Die Kurvenpunkte, deren Koordinaten in $\mathbb{F}_q$ liegen, heißen *rationale Punkte.*

Beispiel:

Sei C die Kleinsche Quartik, also die projektive ebene Kurve mit der Gleichung $X^3Y + Y^3Z + Z^3X = 0$. Wir betrachten diese über dem algebraischen Abschluss von $\mathbb{F}_2$ sowie einigen Zwischenkörpern.

Über $\mathbb{F}_2$ hat die Kurve nur die offensichtlichen rationalen Punkte $[1:0:0]$, $[0:1:0]$ und $[0:0:1]$. Hat ein Punkt von C über einem Erweiterungskörper von $\mathbb{F}_2$ eine Koordinate gleich Null, so folgt aus der Gleichung, dass eine weitere Koordinate Null ist, und also ergeben sich die schon angegebenen Punkte aus $\mathbb{F}_2$. Wir suchen also nun nur nach Punkten, deren Koordinaten alle ungleich Null sind.

Über $\mathbb{F}_4$ kommen noch zwei weitere rationale Punkte hinzu:
Ist $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2 + X + 1)$ mit den Elementen $\{0, 1, \xi, \xi + 1\}$, so rechnet man leicht nach, dass $[1 : \xi : \xi + 1]$ und $[1 : \xi + 1 : \xi]$ Punkte der Kurve sind, und dass es keine weiteren Punkte geben kann. In ähnlicher Weise rechnet man nach, dass C über $\mathbb{F}_8$ 24 Punkte hat.

Um nun ein Beispiel für einen Code vorzustellen und dessen Parameter berechnen zu können, müssen wir das Schnittverhalten von Kurven behandeln. Bekanntlich hat ein Polynom vom Grad n höchstens n Nullstellen. Über einem algebraisch abgeschlossenen Körper erhält man genau n Nullstellen, wenn man diese mit Vielfachheiten zählt. Dies soll nun auf den Schnitt von zwei ebenen Kurven verallgemeinert werden.

2.1.11. Satz (Bézout)

Zwei ebene Kurven vom Grad l und m über einem algebraisch abgeschlossenen Körper, die keine gemeinsame Komponente haben, schneiden sich in genau lm Punkten, wenn man diese mit Vielfachheit zählt und die Punkte im Unendlichen berücksichtigt.

Der Beweis dieses Satzes ist relativ aufwendig und soll hier nicht ausgeführt werden.[2]

2.1.12. Bemerkung

Ist der Grundkörper nicht algebraisch abgeschlossen, so schneiden sich die Kurven in höchstens lm Punkten.

Beispiel:

Die affinen ebenen Kurven E und F mit den Gleichungen $X^3 + Y^3 = 1$ und $X = Y$ haben keinen Schnittpunkt über dem algebraischen Abschluss von $\mathbb{F}_2$.

Betrachtet man jedoch die homogenisierten Gleichungen $X^3 + Y^3 + Z^3 = 0$ und $X + Y = 0$, sieht man, dass diese den gemeinsamen Punkt $[1 : 1 : 0]$ haben. Dieser ist Wendepunkt der Kurve E mit Wendetangente F, hat also die Schnittvielfachheit drei.

[2] Der Beweis findet sich etwa in [12], §8.1.

Beispiel: Reed-Solomon-Code

Sei V_l der Vektorraum der Polynome in zwei Variablen mit Grad $\leq l$ mit Koeffizienten in $\mathbb{F}_q$:

$$V_l = \{F \in \mathbb{F}_q[x,y] |\, \deg F \leq l\}$$

Sei G ein irreduzibles Element von $\mathbb{F}_q[x,y]$ mit $\deg G = m$; seien $P_1, \ldots, P_n$ paarweise verschiedene Punkte der ebenen Kurve $G(x,y) = 0$, also gilt $G(P_i) = 0$ für alle $i = 1, \ldots, n$. Wir definieren den Code $\mathcal{C}$ per

$$\begin{aligned} \mathcal{C} &= \{(F(P_1), \ldots, F(P_n)) | F \in V_l\} \\ &= \{(F(P_1), \ldots, F(P_n)) | F \in \mathbb{F}_q[x,y], \deg F \leq l\} \end{aligned}$$

Wie im Kapitel 1 bezeichnen wir die Dimension des Codes mit k und die Minimaldistanz mit d. Dann gilt:

2.1.13. Satz

Sei $lm < n$. Dann gilt für die Dimension und die Minimaldistanz des Reed-Solomon-Codes $\mathcal{C}$:

$$k = \begin{cases} \binom{l+2}{2} & \text{für } l < m, \\ lm + 1 - \binom{m-1}{2} & \text{für } l \geq m. \end{cases}$$

$$d \geq n - lm$$

Beweis:

Die Monome $x^\alpha y^\beta$ mit $\alpha + \beta \leq l$ bilden eine Basis von V_l. Daher ergibt sich (z.B. durch Induktion)

$$\dim V_l = {}^{\#}\{(\alpha, \beta) \in \mathbb{N} \times \mathbb{N} |\, \alpha + \beta \leq l\} = \binom{l+2}{2}.$$

Nun betrachten wir die Abbildung

$$\varphi : V_l \to \mathcal{C},$$

$$F \mapsto (F(P_1), \ldots, F(P_n)),$$

diese ist offensichtlich linear und surjektiv. $\varphi(F) \neq 0$ gilt genau dann, wenn G kein Faktor von F ist:

Falls G ein Faktor von F ist, gilt offensichtlich $\varphi(F) = 0$.

Sei nun $\varphi(F) = 0$. Betrachte die ebenen Kurven $F = 0$ mit $\deg F = \tilde{l} \leq l$ und $G = 0$ mit $\deg G = m$. Die Punkte $P_1, \ldots, P_n$ liegen im Schnitt beider Kurven, aber nach Voraussetzung ist $\tilde{l}m \leq lm < n$, also haben F und G nach dem Satz von Bézout einen gemeinsamen Faktor. G ist irreduzibel, also gilt $G|F$.

Ist $m > l$, teilt G nur das Nullpolynom aus V_l. Dann ist φ injektiv, also

$$k = \dim V_l = \binom{l+2}{2}.$$

Im Fall $m \leq l$ ist $G \cdot V_{l-m}$ der Kern von φ, also gilt

$$\begin{aligned} k &= \dim V_l - \dim V_{l-m} = \binom{l+2}{2} - \binom{l-m+2}{2} \\ &= \frac{m}{2}(2l - m + 3) = lm + 1 - \binom{m-1}{2}. \end{aligned}$$

Ein Codewort ungleich Null hat nach dem Satz von Bézout höchstens lm Koordinaten gleich Null, also gilt für die Minimaldistanz

$$d \geq n - lm.$$

$\$$

2.2 Divisoren

Sei im folgenden V eine glatte projektive Kurve über k.

2.2.1. Definition

- *Divisoren* sind formale Linearkombinationen von Punkten:

$$D = \sum_{P \in V} n_P P, \quad n_P \in \mathbb{Z},\ n_P \neq 0 \text{ nur für endlich viele } P$$

- $\mathrm{Div}(V)$ ist die additive Gruppe aller Divisoren auf V mit formaler Addition.

- Ein Divisor heißt *effektiv*, wenn alle Koeffizienten $n_P \geq 0$ sind. Man schreibt

$$D \succeq 0.$$

- Der *Grad* des Divisors D ist gegeben durch

$$\deg D = \sum n_P.$$

- Der *Träger* eines Divisors ist definiert als

$$\mathrm{supp}\ D = \{P \in V | n_P \neq 0\}.$$

Sei v_P die im vorigen Abschnitt definierte diskrete Bewertung rationaler Funktionen auf V im Punkte P.

2.2.2. Definition

Der *Divisor einer rationalen Funktion* f auf V mit $f \not\equiv 0$ ist gegeben durch

$$\mathrm{div}\ f = \sum_{P \in V} v_P(f) P.$$

Der Divisor einer rationalen Funktion wird als *Hauptdivisor* bezeichnet.

Da die projektiven rationalen Funktionen Quotienten von Polynomen gleichen Grades sind, haben diese über dem algebraisch abgeschlossenen Körper k gleichviele Nullstellen wie Pole (mit Vielfachheiten gezählt). Daher gilt:

2.2.3. Satz

Der Grad eines Hauptdivisors ist Null.

Beispiel:

Sei $\operatorname{char} k \neq 2$ und seien $e_1, e_2, e_3 \in k$ paarweise verschieden. Dann ist die Kurve C mit der Gleichung

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

eine glatte elliptische Kurve. Der Punkt im Unendlichen wird mit P_∞ bezeichnet. Sei $P_i = (e_i, 0)$ für $i = 1, 2, 3$.

Die Funktion y ist Null in den Punkten P_1, P_2 und P_3, und in diesen Punkten ist y lokaler Parameter. Also gilt

$$\operatorname{div}(y) = (P_1) + (P_2) + (P_3) - 3(P_\infty).$$

Die Funktion $x - e_i$ ist Null im Punkt P_i, y ist dort lokaler Parameter und es gilt $x - e_i \sim y^2$. Daher gilt

$$\operatorname{div}(x - e_i) = 2(P_i) - 2(P_\infty).$$

2.2.4. Definition

Sei D ein Divisor auf einer Kurve V. Dazu definiert man:

$$\mathcal{L}(D) = \{f \in k(V)^* | \operatorname{div} f + D \succeq 0\} \cup \{0\}.$$

2.2.5. Bemerkung

Offenbar ist $\mathcal{L}(D)$ ein Vektorraum. Seine Dimension wird mit $l(D)$ bezeichnet.

2.2.6. Bemerkung

Schreibt man den Divisor D als $D = \sum n_i P_i - \sum m_j Q_j$ mit $n_i, m_j > 0$ für alle i, j, dann besteht $\mathcal{L}(D)$ aus der Nullfunktion und den Funktionen, die Pole der Ordnung $\leq n_i$ in den P_i und Nullstellen der Ordnung $\geq m_j$ in den Q_j haben und sonst regulär sind.

2.2.7. Satz

$\deg D < 0 \Longrightarrow \mathcal{L}(D) = \{0\}$

Beweis:

Ist $\deg D < 0$, so auch $\deg(D + \operatorname{div} f) < 0$ für jede rationale Funktion f. Also ist $f \notin \mathcal{L}(D)$.

$

2.2.8. Satz

$l(D) \leq 1 + \deg D$

Insbesondere ist $\mathcal{L}(D)$ also stets endlichdimensional. Dieser Satz soll hier nicht bewiesen werden.[3]

Beispiel:

Sei V die projektive Gerade $\mathbb{P}^1$, sei P der Nullpunkt und $D = n \cdot P$.

Der Vektorraum $\mathcal{L}(D)$ besteht dann aus den Funktionen, die maximal Pole der Ordnung n in P haben und sonst (also auch in ∞) regulär sind. Eine Basis von $\mathcal{L}(D)$ ist gegeben durch $1, \frac{1}{z}, \frac{1}{z^2}, \ldots \frac{1}{z^n}$.

Der Vektorraum $\mathcal{L}(-D)$, der alle Funktionen enthält, die im Nullpunkt Nullstellen der Ordnung höchsten n haben und sonst regulär sind, besteht dagegen nur aus der Null, da eine rationale Funktion auf $\mathbb{P}^n$ stets (mit Vielfachheit gezählt) gleichviele Pole wie Nullstellen hat. So hätte zum Beispiel z^n in Null die richtige Nullstellenordnung, aber auch einen Pol der Ordnung n in ∞.

2.3 Differentiale auf Kurven

Sei C eine glatte ebene affine Kurve, gegeben durch die Gleichung $F(X,Y) = 0$, sei $P = (a,b)$ ein Punkt der Kurve. Wie wir schon im Abschnitt 2.1 gesehen haben, ist T_P, der Tangentialraum im Punkt P, definiert durch $d_P F = 0$.

Wir betrachten nun die Menge $\Phi[C]$ aller Abbildungen, die jedem Punkt $P \in C$ eine Linearform auf T_P zuordnen.

2.3.1. Definition

Ein Element von $\phi \in \Phi[C]$ heißt *reguläre Differentialform* auf der Kurve C, wenn für jeden Punkt P von C eine Umgebung U existiert, in der ϕ darstellbar ist als $\phi = \sum f_i dg_i$ mit in U regulären Funktionen f_i und g_i.

Die Menge aller regulären Diffentialformen ist ein $k[C]$-Modul, dieser wird mit $\Omega[C]$ bezeichnet. Erzeugt wird $\Omega[C]$ durch die Elemente df mit $f \in k[C]$. Dabei gelten die wohlbekannten Rechenregeln: $d(f+g) = df + dg$, $d(fg) = fdg + gdf$, $da = 0$ für $a \in k$. Will man auch rationale Differentialformen definieren, kommt dazu noch die Quotientenregel $d(f/g) = (gdf - fdg)/g^2$.

Um rationale Differentialformen auf einer glatten projektiven Kurve C zu erklären, betrachtet man Paare (U, ω) mit einer nichtleeren offenen affinen Teilmenge $U \subset C$ und einer Differentialform ω, die auf U die Form fdg hat. Zwei

[3] Ein Beweis findet sich etwa in [12], Abschnitt 8.3

solche Paare (U, ω) und (V, η) sind äquivalent, wenn die Differentialformen auf der Schnittmenge $U \cap V$ übereinstimmen. Die Äquivalenzklassen bezüglich dieser Relation bezeichnen wir dann als Differentiale auf der Kurve. Die Menge der Differentiale auf der Kurve C wird mit $\Omega(C)$ bezeichnet.

2.3.2. Satz

$\Omega(C)$ hat Dimension 1 über $k(C)$. Ist t ein lokaler Parameter in der Umgebung eines Punktes P, so kann ein Differential ω dort als $\omega = f\,dt$ mit einer rationalen Funktion f dargestellt werden.

Dieser Satz soll hier nicht bewiesen werden.[4]

2.3.3. Bemerkung

Die Bedeutung des Satzes ergibt sich daraus, dass es auf projektiven Kurven Differentiale ungleich Null gibt, die auf der ganzen Kurve regulär sind. Alle rationalen auf der ganzen Kurve regulären Funktionen sind aber konstant.

Die Ausnahme bildet dabei nur die projektive Gerade $\mathbb{P}^1$: Auf dieser gibt es keine regulären Differentiale ungleich Null.

[4] Ein Beweis findet sich etwa in [12], Abschnitt 6.1

2.3.4. Definition

Der Divisor eines Differentials ω ist gegeben durch

$$\operatorname{div} \omega = \sum_{P \in C} v_P(f_P) P,$$

wenn ω im Punkt P die lokale Darstellung $\omega = f_P \, dt_P$ hat und v_P die (auf $k(C)$ fortgesetzte) Bewertung von O_P ist.

2.3.5. Bemerkung

Die Bewertung hängt nicht von der Wahl des lokalen Parameters ab, der Divisor ist also wohldefiniert. Nur endlich viele Koeffizienten sind ungleich Null.

Der Beweis findet sich in der Standardliteratur.

2.3.6. Definition

Ein Differential ω heißt *regulär auf* C, wenn

$$v_p(\omega) \geq 0 \quad \text{für alle } P \in C.$$

2.3.7. Bemerkung

Ist ω ein Differential und f eine rationale Funktion, so ist der Divisor von $f\omega$ gegeben durch

$$\operatorname{div}(f\omega) = \sum_{P \in C} v_P(f \cdot f_P) P = \sum_{P \in C} (v_P(f) + v_P(f_P)) P = \operatorname{div} f + \operatorname{div} \omega.$$

Sind ω und $\tilde{\omega}$ Differentiale ungleich Null, so gibt es eine rationale Funktion f mit $\tilde{\omega} = f\omega$. Dann gilt div $\tilde{\omega}$ − div ω = div f, also unterscheiden sich die Divisoren von ω und von $\tilde{\omega}$ nur um einen Hauptdivisor. Modulo Hauptdivisoren gibt es also nur eine Äquivalenzklasse, diese wird mit W bezeichnet.

2.3.8. Definition

Die Elemente von W werden als *kanonische Divisoren* bezeichnet.

Wie im vorigen Abschnitt betrachtet man nun den Vektorraum

$$\mathcal{L}(W) = \{f \in k(V)^* | \operatorname{div} f + W \succeq 0\} \cup \{0\},$$

seine Dimension wird wieder mit $l(W)$ bezeichnet.

Damit definiert man:

2.3.9. Definition

Sei C eine glatte projektive Kurve über k. Das *Geschlecht* g der Kurve wird dann definiert als $g := l(W)$.

Das Geschlecht einer Kurve wird im Folgenden mehrfach benötigt. Zu seiner Bestimmung soll hier nur folgender Satz ohne Beweis zitiert werden:

2.3.10. Satz

Ist C eine nichtsinguläre Kurve vom Grad d, so gilt für ihr Geschlecht

$$g = \frac{1}{2}(d-1)(d-2).$$

Beispiel 1:

Auf der projektiven Geraden $\mathbb{P}_1$ gibt es keine regulären Differentiale ungleich Null:

Sei t eine Koordinatenfunktion auf $\mathbb{P}^1$. Für die affinen Punkte $a \in \mathbb{P}^1$ ist dann $t - a$ lokaler Parameter, und daher gilt

$$v_a(dt) = v_a(d(t-a)) = 0.$$

In P_∞, dem Punkt im Unendlichen, ist jedoch $1/t$ lokaler Parameter, also gilt

$$v_\infty(dt) = v_\infty(-t^2 d(1/t)) = -2.$$

Damit hat man insgesamt

$$\operatorname{div}(dt) = -2P_\infty.$$

dt ist also kein reguläres Differential. Jedes weitere Differential ω auf $\mathbb{P}_1$ unterscheidet sich von dt nur um eine rationale Funktion: $\omega = f\,dt$ Daher gilt:

$$\deg \operatorname{div} \omega = -2,$$

und damit ist auch ω nicht regulär.

Beispiel 2:

Auf elliptischen Kurven gibt es ein reguläres Differential ungleich Null:

Sei die elliptische Kurve C gegeben durch die Gleichung

$$Y^2 = (X - e_1)(X - e_2)(X - e_3),$$

mit paarweise verschiedenen e_i, und sei $P_i = (e_i, 0)$ für $i = 1, 2, 3$. Sei P_∞ der Punkt im Unendlichen.

Das Differential dx verschwindet in den Punkten P_i, und dort ist y lokaler Parameter. Dort gilt $dx = d(y^2) = 2ydy$, daher ist der Divisor des Differentials dx gegeben durch:

$$\operatorname{div}(dx) = 1 \cdot (P_1) + 1 \cdot (P_2) + 1 \cdot (P_3) - 3 \cdot (P_\infty)$$

Nach dem Beispiel auf Seite 26 gilt

$$\operatorname{div}(y) = 1 \cdot (P_1) + 1 \cdot (P_2) + 1 \cdot (P_3) - 3 \cdot (P_\infty).$$

Damit folgt

$$\operatorname{div}(dx/y) = 0,$$

dx/y ist also ein reguläres nichtverschwindendes Differential.

Um später die geometrischen Goppa-Codes definieren zu können, benötigen wir noch den Begriff des Residuums eines Differentials im Punkte P.

2.3.11. Definition

Sei C eine glatte projektive algebraische Kurve und ω ein Differential auf C. Sei t ein lokaler Parameter in $P \in C$ und $\omega = f dt$ die lokale Darstellung von ω. Dann definiert man

$$\operatorname{Res}_P(\omega) = a_{-1},$$

wenn f die formale Laurententwicklung $f = \sum_{i \in \mathbb{Z}} a_i t^i$ hat.

Der Nachweis, dass das Residuum nicht von der Wahl des lokalen Parameters abhängt, wird hier nicht durchgeführt.[5]

Für die Summe der Residuen eines Differentials auf einer glatten Kurve C gilt ein Satz, der analog zum Residuensatz für holomorphe Funktionen ist. Dieser wird hier ohne Beweis angegeben:[6]

2.3.12. Satz

Ist C eine glatte projektive Kurve und ω ein Differential auf C, so gilt

$$\sum_{P \in C} \operatorname{Res}_P(\omega) = 0.$$

[5] siehe [11], Abschnitt 8.4

[6] siehe [11], Abschnitt 8.4

2.4 Satz von Riemann-Roch

Bei der Bestimmung der Dimension der Vektorräume $\mathcal{L}(D)$ im nächsten Abschnitt braucht man ein zentrales Resultat der algebraischen Geometrie, den Satz von Riemann-Roch. Der Beweis ist sehr aufwendig und wird hier nicht durchgeführt.[7]

2.4.1. Satz (Riemann-Roch)

Sei D ein Divisor auf einer glatten projektiven Kurve vom Geschlecht g, und sei W ein kanonischer Divisor. Dann gilt

$$l(D) - l(W - D) = \deg D - g + 1.$$

2.4.2. Korollar

Sei W ein kanonischer Divisor auf einer glatten projektiven Kurve vom Geschlecht g. Dann gilt

$$\deg W = 2g - 2.$$

Beweis:

Rationale Funktionen auf einer projektiven Kurve, die in jedem Punkt regulär sind, sind konstant. Daher gilt $\mathcal{L}(0) = k$ und also $l(0) = 1$. Setzt man im Satz von Riemann-Roch $D = W$ und berücksichtigt $g = l(W)$, so folgt die Behauptung.

$

2.4.3. Korollar

Sei D ein Divisor auf einer glatten projektiven Kurve vom Geschlecht g, und sei $\deg D > 2g - 2$. Dann gilt

$$l(D) = \deg D - g + 1.$$

[7]Eine Diskussion des Beweises findet man in [14].

Beweis:

Nach dem eben bewiesenen Satz gilt $\deg(W - D) = \deg W - \deg D < 0$, also ist $\mathcal{L}(W - D) = \{0\}$ und $l(W - D) = 0$. Mit dem Satz von Riemann-Roch folgt die Behauptung.

Anwendung: Weierstrass-Gleichung für elliptische Kurven

Sei E eine elliptische Kurve über K mit Nullpunkt O. Diese hat Geschlecht 1. Nun betrachtet man die Vektorräume $\mathcal{L}(n \cdot O)$ für $n = 1, 2, \ldots$. Nach dem eben bewiesenen Korollar gilt für die Dimension von $\mathcal{L}(n \cdot O)$:

$$l(n \cdot O) = \deg(n \cdot O) - g + 1 = \deg(n \cdot O) = n.$$

Wir wählen nun Funktionen x und y aus $K(E)$ so, dass $\{1, x\}$ eine Basis von $\mathcal{L}(2 \cdot O)$ und $\{1, x, y\}$ eine Basis von $\mathcal{L}(3 \cdot O)$ ist.[8] x hat im Nullpunkt einen Pol zweiter Ordnung, y einen Pol dritter Ordnung.

Weiterhin hat $\mathcal{L}(6 \cdot O)$ die Dimension 6, enthält aber die Funktionen 1, x, y, x^2, xy, y^2 und x^3. Daher gibt es zwischen diesen eine lineare Relation:

$$a_1 + a_2 x + a_3 y + a_4 x^2 + a_5 xy + a_6 y^2 + a_7 x^3 = 0.$$

Damit sich die Pole aufheben, müssen a_6 und a_7 ungleich Null sein. Durch die Variablentransformation $u = -1/(a_6 a_7)x$ und $v = 1/(a_6 a_7^2)y$ und anschliessende Division durch $a_6^3 a_7^4$ ergibt sich eine kubische Weierstrassgleichung.

2.4.4. Bemerkung

Man kann für x die Weierstrasssche $\wp$-Funktion und für y deren Ableitung wählen.

[8] Im Fall einer glatten Kurve C über K kann eine Basis von $\mathcal{L}(D)$ stets aus Funktionen von $K(C)$ gewählt werden. Ein Beweis findet sich etwa in [14], Abschnitt II.5.

Auch für Differentiale definiert man nun:

2.4.5. Definition

Sei D ein Divisor auf einer Kurve C. Man definiert

$$\Omega(D) = \{\omega \in \Omega(C) : (\omega) - D \succeq 0\}$$

Die Dimension von $\Omega(D)$ wird mit $\delta(D)$ bezeichnet und heißt *Spezialitätsindex* von D.

Der Zusammenhang mit Funktionen ergibt sich durch

2.4.6. Satz

$\Omega(D) \cong \mathcal{L}(W - D)$

Beweis:

Sei $W = (\omega)$. Dazu definiert man die lineare Abbildung $\phi : \mathcal{L}(W - D) \to \Omega(D)$ per $\phi(f) = f\omega$. Diese ist offenbar ein Isomorphismus.

$\$$

2.4.7. Korollar

$\delta(D) = l(W - D)$.

2.5 Codes zu algebraischen Kurven

Der Grundkörper, also unser Codierungsalphabet, sei von nun an wieder $\mathbb{F}_q$. Alle Theoreme (insbesondere Riemann-Roch) behalten dabei ihre Gültigkeit. Die Verifikation wird hier nicht durchgeführt.

Sei von nun an V eine glatte projektive Kurve, $P_1, \ldots, P_n$ Punkte auf V und D der Divisor $P_1 + \cdots + P_n$. Außerdem sei G ein weiterer Divisor auf V mit $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$.

Zur Vereinfachung wird G weiterhin so gewählt, dass der Träger von G nur aus rationalen Punkten besteht und $2g - 2 < \deg(G) < n$ gilt.

2.5.1. Definition

Der lineare Code $\mathcal{C}(D, G)$ der Länge n über $\mathbb{F}_q$ ist das Bild der linearen Abbildung

$$\alpha : \mathcal{L}(G) \to \mathbb{F}_q^n$$

mit

$$\alpha(f) = (f(P_1), \ldots, f(P_n)).$$

Dies ist der *geometrisch verallgemeinerte Reed-Solomon-Code.*

2.5.2. Satz

Der geometrisch verallgemeinerte Reed-Solomon-Code hat die Dimension

$$k = \deg G - g + 1$$

und die Minimaldistanz

$$d \geq n - \deg G.$$

Beweis:

ad k: Sei $f \in \operatorname{Ker} \alpha$, also $f(P_i) = 0$ für $i = 1, \ldots, n$. Per Definition ist $f \in \mathcal{L}(G)$, also auch $f \in \mathcal{L}(G - D)$, da $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$. Da G kleineren Grad als D hat, ist $f = 0$. Also ist α injektiv und $k = l(G)$.

Aufgrund der vereinfachenden Voraussetzung $2g-2 < \deg(G)$ läßt sich das zweite Korollar des Satzes von Riemann-Roch anwenden. Damit folgt die Behauptung.

ad d: Hat $\alpha(f)$ Hamming-Norm d, dann gibt es $n-d$ Punkte $P_{j_1}, \ldots, P_{j_{n-d}}$ mit $f(P_{j_i}) = 0$. Ist E der Divisor $P_{j_1} + \cdots + P_{j_{n-d}}$, dann ist f enthalten in $\mathcal{L}(G-E)$ (siehe oben). Also hat $G-E$ nichtnegativen Grad:

$$\deg G - \deg E = \deg G - n + d \geq 0.$$

2.5.3. Definition

Der lineare Code $\mathcal{C}^*(D,G)$ der Länge n über $\mathbb{F}_q$ ist das Bild der linearen Abbildung

$$\alpha^* : \Omega(G-D) \to \mathbb{F}_q^n$$

mit

$$\alpha^*(\eta) = (\mathrm{Res}_{P_1}(\eta), \ldots, \mathrm{Res}_{P_n}(\eta)).$$

Dies ist der *geometrisch verallgemeinerte Goppa-Code.*

2.5.4. Satz

Der geometrische Goppa-Code hat die Dimension

$$k^* = n - \deg G + g - 1$$

und die Minimaldistanz

$$d^* \geq \deg G - 2g + 2.$$

Beweis:

ad k^*:

$$\begin{aligned}\eta \in \text{Ker } \alpha^* &\iff \eta \in \Omega(G-D) \quad \text{und} \quad \text{Res}_{P_i}(\eta) = 0 \quad \text{für } i = 1, \ldots, n\\ &\iff \eta \in \Omega(G-D) \quad \text{und } \eta \text{ regulär in } P_1, \ldots, P_n\\ &\iff \eta \in \Omega(G)\end{aligned}$$

Daher gilt:

$$\begin{aligned}k^* &= \dim \mathcal{C}^*(D,G) = \dim \text{ Im } \alpha^* = \dim \Omega(G-D) - \dim \Omega(G)\\ &= \dim \mathcal{L}(W-G+D) - \dim \mathcal{L}(W-G)\\ &= l(W-G+D) - l(W-G)\\ &= l(G-D) - \deg(G-D) + g - 1\\ &\quad -(l(G) - \deg G + g - 1) \qquad \text{nach Riemann-Roch}\\ &= \underbrace{l(G-D)}_{=0,\text{ da } \deg G < \deg D} - \deg G + \underbrace{\deg D}_{=n} - l(G) + \deg G\\ &= n - \deg G + g - 1 \qquad \text{nach dem 2. Korollar zu Riemann-Roch}\end{aligned}$$

ad d^*:
Dies geht analog zur Bestimmung der Minimaldistanz des Reed-Solomon-Codes:

Sei $\eta \neq 0$ und $\alpha^*(\eta) \in \mathcal{C}^*(D,G)$ mit Hamming-Norm d^*, dann gibt es $(n-d^*)$ Punkte $P_{j_1}, \ldots, P_{j_{n-d^*}}$ mit

$$\text{Res}_{P_{j_\kappa}}(\eta) = 0 \qquad \text{für } \kappa = 1, \ldots, n - d^*.$$

Setze $E = P_{j_1} + \cdots + P_{j_{n-d^*}}$, dann gilt $\eta \in \Omega(E + G - D)$

$$\begin{aligned}&\Longrightarrow \mathcal{L}(W - (E+G-D)) \neq \{0\}\\ &\Longrightarrow \deg(W - (E+G-D)) \geq 0\\ &\Longrightarrow 2g - 2 - (n-d^*) - \deg G + n \geq 0\\ &\qquad\qquad \text{nach dem 1. Korollar zu Riemann-Roch}\\ &\Longrightarrow d^* \geq \deg G + 2 - 2g\end{aligned}$$

$

Die Bezeichnung $\mathcal{C}^*$ für den geometrischen Goppa-Code ist kein Zufall:

2.5.5. Definition

Sei $\mathcal{C}$ ein $[n,k]$-Code über $\mathbb{F}_q$. Der *duale Code* ist dann gegeben durch

$$\mathcal{C}^* = \{y \in \mathbb{F}_q^n | (x|y) = 0 \text{ für alle } x \in \mathcal{C}\}$$

2.5.6. Bemerkung

Ist $\mathcal{C}$ ein $[n,k]$-Code, so ist $\mathcal{C}^*$ ein $[n, n-k]$-Code.

2.5.7. Satz

$\mathcal{C}^*(D,G)$ ist der duale Code von $\mathcal{C}(D,G)$.

Beweis:

Nach den Sätzen über die Dimension der Reed-Solomon- und Goppa-Codes ist bereits klar, dass $n = k + k^*$ gilt. Es bleibt zu zeigen, dass das Skalarprodukt von einem Element von $\mathcal{C}^*(D,G)$ und einem Element von $\mathcal{C}(D,G)$ stets Null ist.

Sei $f \in \mathcal{L}(G)$ und $\eta \in \Omega(G-D)$. Dann liegen alle Pole des Differentials $f\eta$ in $\operatorname{supp} D = \{P_1, \ldots, P_n\}$. Da f auf $\operatorname{supp} D$ regulär ist, ist Residuum von $f\eta$ im Punkt P_i gleich $f(P_i)\operatorname{Res}_{P_i}(\eta)$. Nach dem Residuensatz ist die Summe der Residuen des Differential $f\eta$ über alle Pole gleich Null:

$$0 = \sum_{i=1}^{n} f(P_i)\operatorname{Res}_{P_i}(\eta) = (\alpha(f)|\alpha^*(\eta)).$$

$

Kapitel 3

Torische Varietäten

In diesem Kapitel sollen einige Grundlagen aus der Theorie der torischen Varietäten dargestellt werden. Im Abschnitt über Konvexität wird der Begriff des streng konvexen polyedrischen Kegels eingeführt, der das Hauptwerkzeug bei der Konstruktion affiner torischer Varietäten sein wird. Diese Konstruktion wird explizit durchgeführt, und es wird erklärt, wie man allgemeine torische Varietäten aus bestimmten Kollektionen von Kegeln, den sogenannten Fächern konstruiert.

Die torischen Varietäten, die für die torischen Codes im nächsten Kapitel relevant sind, lassen sich aus einem Polytop konstruieren. Sie sind dann automatisch glatt und kompakt.

Das Kapitel orientiert sich inhaltlich an den Büchern über torische Varietäten von William Fulton [3] und Tadao Oda [13] und dem Tutorial von David Cox [1].

Wie in der Standardliteratur vorgegeben, wollen auch wir in diesem Kapitel stets mit $\mathbb{C}$ als Grundkörper arbeiten.

3.1 Definitionen und Beispiele

Zur Erinnerung wiederholen wir noch einmal die Definition der Varietät aus Abschnitt 2.1.

3.1.1. Definition

Eine *affine Varietät* ist die Nullstellenmenge endlich vieler Polynome:

$$V(f_1, \ldots, f_s) = \{x \in \mathbb{C}^n | f_j(x) = 0 \text{ für } j = 1, \ldots, s\}$$

mit $f_j \in \mathbb{C}[X_1, \ldots, X_n]$.
Eine *projektive Varietät* ist die Nullstellenmenge endlich vieler homogener Polynome:

$$V(F_1, \ldots, F_s) = \{[x] \in \mathbb{P}^n | F_j(x) = 0 \text{ für } j = 1, \ldots, s\}$$

mit $F_j \in \mathbb{C}[X_0, \ldots, X_n]$ homogen.

Beispiel:

Der komplexe Torus $(\mathbb{C}^\times)^n \subset \mathbb{C}^n$ ist eine affine Varietät, denn mit der Abbildung $(t_1, \ldots, t_n) \mapsto (t_1, \ldots, t_n, 1/t_1 \cdot \ldots \cdot t_n)$ erhält man

$$(\mathbb{C}^\times)^n \cong V(X_1 X_2 \cdot \ldots \cdot X_{n+1} - 1) \subset \mathbb{C}^{n+1}$$

Das Konzept der affinen und projektiven Varietäten liefert ein nützliches Hilfsmittel, die sogenannte *Zariski-Topologie*:

3.1.2. Definition

Eine Teilmenge des $\mathbb{C}^n$ oder $\mathbb{P}^n$ heißt *Zariski-abgeschlossen*, wenn sie eine Varietät ist.

Die offenen Mengen in der Zariski-Topologie sind also die Komplemente von Varietäten. Speziell definiert man:

3.1.3. Definition

Eine Menge heißt *prinzipal offen*, wenn ihr Komplement die Nullstellenmenge eines Polynoms ist.

Der Vorteil dieser Topologie ist, dass man sie über einem beliebigen Körper einführen kann, also zum Beispiel auch über endlichen Körpern. Da Varietäten bezüglich der Standardtopologie des $\mathbb{C}^n$ und $\mathbb{P}^n$ abgeschlossene Mengen sind, ist die Zariski-Topologie gröber als die Standardtopologie.

3.1.4. Definition

Eine Varietät heißt *irreduzibel*, wenn man sie nicht in nichttrivialer Weise als Vereinigung zweier Varietäten schreiben kann.

3.1.5. Definition

Eine *torische Varietät* ist eine irreduzible Varietät V mit folgenden Eigenschaften:

1. V enthält für geeignetes $n \in \mathbb{N}$ den Torus $T^n = (\mathbb{C}^\times)^n$ als dichte Zariski-offene Teilmenge.
2. Die natürliche Aktion von T^n auf sich selbst läßt sich zu einer algebraischen Aktion $T^n \times V \to V$ auf V fortsetzen.

Einfache Beispiele:

Offensichtlich sind $(\mathbb{C}^\times)^n$ und $\mathbb{C}^n$ torische Varietäten.

Auch $\mathbb{P}^n$ ist eine torische Varietät: Die Abbildung

$$(\mathbb{C}^\times)^n \to \mathbb{P}^n, \qquad (t_1, \ldots, t_n) \mapsto [1, t_1, \ldots, t_n]$$

identifiziert $(\mathbb{C}^\times)^n$ mit dem Komplement von $V(X_0 \cdot X_1 \cdot \cdots \cdot X_n)$ im $\mathbb{P}^n$.

Die Fortsetzung der natürlichen Aktion erhält man, indem man setzt:

$$(t_1, \ldots, t_n) \cdot [a_0, a_1, \ldots, a_n] = [a_0, t_1 \cdot a_1, \ldots, t_n \cdot a_n].$$

3.2 Konvexität

Da die Standardbeschreibung torischer Varietäten mit Hilfe von rationalen konvexen polyedrischen Kegeln erfolgt, folgt nun eine kurze Zusammenstellung der benötigten Fakten. Die zentrale Rolle für die Konstruktion spielt dabei das Gordansche Lemma, das hier daher mit Beweis aufgeführt wird.

Die Beweise der anderen Sätze sind einfach und können zum Beispiel in [3] nachgelesen werden.

3.2.1. Definition

- Ein *konvexer polyedrischer Kegel* ist eine Menge der Form

  $$\sigma = \{r_1 v_1 + \cdots + r_s v_s | v_i \in \mathbb{R}^n, r_i \in \mathbb{R}_{\geq 0}\},$$

  erzeugt von einer endlichen Anzahl von Vektoren $v_1, \ldots, v_s \in \mathbb{R}^n$. Diese Vektoren werden als *Erzeugende des Kegels* σ bezeichnet.

- Kann man die v_i aus $\mathbb{Z}^n$ wählen, so ist σ ein *rationaler konvexer polyedrischer Kegel*.

- Ist $\sigma \cap \{-\sigma\} = \{0\}$, so heißt σ *streng konvex*. Gleichbedeutend mit dieser Definition ist offenbar, dass σ keinen Vektorraum $\neq \{0\}$ enthält. Im Fall eines streng konvexen polyedrischen Kegels bezeichten man den Nullpunkt als *Spitze* des Kegels.

- Die *Dimension* des Kegels σ ist die Dimension des Vektorraums $\mathbb{R}\sigma$.

- Der *duale Kegel* $\check{\sigma}$ ist gegeben durch

  $$\check{\sigma} = \{u \in \mathbb{R}^n | (u|v) \geq 0 \text{ für alle } v \in \sigma\}$$

- Eine *Seite* τ von σ ist der Schnitt von σ mit einer Hyperebene H, wobei H von einer Linearform erzeugt wird, die auf $\sigma \geq 0$ ist. Seiten der Dimension 1 heißen *Kanten*, Seiten der Codimension 1 heißen *Facetten*.

Einige Basisresultate aus der Theorie der konvexen Mengen sind:

3.2.2. Satz (Satz von Farkas)

Ist σ ein konvexer polyedrischer Kegel, so auch sein dualer Kegel $\check{\sigma}$.

3.2.3. Satz

Ist σ ein streng konvexer polyedrischer Kegel im $\mathbb{R}^n$, so gilt $\dim \check{\sigma} = n$.

Bezeichungen: $N \cong \mathbb{Z}^n$ ist ein n-dimensionales Gitter im $\mathbb{R}^n$, $M = \operatorname{Hom}(N, \mathbb{Z})$ das duale Gitter im $(\mathbb{R}^n)^*$.

3.2.4. Satz (Gordansches Lemma)

Sei σ ein rationaler konvexer polyedrischer Kegel. Dann ist die Halbgruppe

$$S_\sigma = \check{\sigma} \cap M$$

endlich erzeugt.

Beweis:

Da σ rational ist, ist auch $\check{\sigma}$ rational. Daher kann man ein Erzeugendensystem $v_1, \ldots, v_s$ des Kegels $\check{\sigma}$ aus $\check{\sigma} \cap M$ wählen. Sei $K = \{\sum t_i v_i | 0 \leq t_i \leq 1\}$. Da K eine kompakte und M eine diskrete Menge ist, haben die beiden Mengen einen endlichen Schnitt. Die Elemente von $K \cap M$ erzeugen die Halbgruppe S_σ:

Sei nämlich $v \in \check{\sigma} \cap M$, also $v = \sum r_i v_i$ mit $r_i \in \mathbb{R}_{\geq 0}$. r_i lässt sich dann schreiben als $r_i = m_i + t_i$ mit $m_i \in \mathbb{N}$ und $0 \leq t_i \leq 1$. Dann gilt

$$v = \sum m_i \cdot \underbrace{v_i}_{\in K \cap M} + \underbrace{\sum t_i \cdot v_i}_{\in K \cap M}$$

$\$$

3.2.5. Satz

Sei σ ein rationaler konvexer polyedrischer Kegel, und sei $u \in S_\sigma = \check{\sigma} \cap M$. Dann ist $\tau = \sigma \cap u^\perp$ ein rationaler konvexer polyedrischer Kegel. Alle Seiten von σ haben diese Form, und

$$S_\tau = S_\sigma + \mathbb{N} \cdot (-u).$$

3.3 Affine torische Varietäten

In diesem Abschnitt soll erklärt werden, wie man aus streng konvexen rationalen polyedrischen Kegeln in natürlicher Weise Varietäten konstruiert, und es soll nachgewiesen werden, dass es sich bei diese Varietäten um torische Varietäten handelt.

Zunächst werden die benötigten allgemeinen Tatsachen zusammengestellt.

3.3.1 Allgemeine Vorbemerkungen

3.3.1. Definition

Sei A ein kommutativer Ring. Das *Spektrum* von A ist die Menge der Primideale von A. Es wird mit $\operatorname{Spec} A$ bezeichnet. Das *maximale Spektrum* von A ist die Menge der maximalen Ideale von A.

3.3.2. Bemerkung

Wir wollen stets das maximale Spektrum eines kommutativen Ringes A betrachten. Zur Vereinfachung bezeichnen wir auch dieses mit $\operatorname{Spec} A$. Im folgenden sollen A und B stets kommutative Ringe bezeichnen.

3.3.3. Bemerkung

Sei A eine endlich erzeugte $\mathbb{C}$ -Algebra. Dann ist A Quotient einer Polynomalgebra, d.h. es gibt einen surjektiven Algebrenhomomorphismus

$$\phi : \mathbb{C}[X_1, \ldots, X_m] \to A$$

3.3.4. Satz

Sei A eine endlich erzeugte $\mathbb{C}$ -Algebra. Dann entspricht das Spektrum von A, also die Menge der maximalen Ideale, gerade der Menge der Algebrenhomomorphismen $\psi : A \to \mathbb{C}$ mit $\psi(1) = 1$.

Beweis:

Zum maximalen Ideal $\mathfrak{m}$ gehört dabei der Homomorphismus ψ, dessen Kern $\mathfrak{m}$ ist. Aus dem Fundamentalsatz der Algebra folgt $A/\mathfrak{m} \cong \mathbb{C}$.

3.3.5. Bemerkung

Seien A und B endlich erzeugte $\mathbb{C}$ -Algebren. Ein Homomorphismus $h : A \to B$ induziert eine Abbildung $h^* : \operatorname{Spec} B \to \operatorname{Spec} A$ in folgender Weise:
Ist $\mathfrak{m}$ ein maximales Ideal in B, so ist sein Urbild $h^{-1}(\mathfrak{m})$ ein maximales Ideal in A, denn aus $B/\mathfrak{m} \cong \mathbb{C}$ folgt $A/h^{-1}(\mathfrak{m}) \cong \mathbb{C}$.

Insbesondere hat man für ein Primelement $f \in A$ die Lokalisierung $A \to A_f$, also $\operatorname{Spec} A_f \subset \operatorname{Spec} A$. Dabei gilt:

$$\begin{aligned} \operatorname{Spec} A_f &\cong \text{ alle maximalen Ideale von } A \text{, die } f \text{ nicht enthalten} \\ &\cong \text{ alle Algebrenhomomorphismen } \psi : A \to \mathbb{C} \text{ mit } \psi(f) \neq 0 \end{aligned}$$

A_f ist als Komplement von $f = 0$ eine prinzipal offene Menge.

Spezialfall:

Sei $A = \mathbb{C}[X_1, \ldots, X_n]$ der Polynomring in n Variablen. Dann wird jedes maximale Ideal von einem Punkt aus $\mathbb{C}^n$ erzeugt:

$$\mathfrak{m} = (X_1 - x_1, \ldots, X_n - x_n) \;\simeq\; (x_1, \ldots, x_n) \in \mathbb{C}^n$$

Für ein $f \in A = \mathbb{C}[X_1, \ldots, X_n]$ entspricht A_f allen Punkten außerhalb der Varietät $V(f)$.

3.3.2 Konstruktion affiner torischer Varietäten

Zu einem streng konvexen rationalen polyedrischen Kegel σ betrachten wir die Halbgruppe $S_\sigma = \check{\sigma} \cap M$.

Zu einer additiven Halbgruppe S_σ hat man stets den Gruppenring $\mathbb{C}[S_\sigma]$ von S_σ über $\mathbb{C}$, die Menge der formalen endlichen Summen der Form

$$\sum \alpha_u \chi^u \text{ für } \alpha_u \in \mathbb{C}, u \in S_\sigma$$

mit formalen Basiselementen χ^u.

Die χ^u, $u \in S_\sigma$ bilden eine Basis von $\mathbb{C}[S_\sigma]$ als $\mathbb{C}$-Vektorraum.

Mit der von der Addition in S_σ bestimmten Multiplikation $\chi^{u_1} \cdot \chi^{u_2} = \chi^{u_1+u_2}$ bildet der Gruppenring $\mathbb{C}[S_\sigma]$ eine kommutative $\mathbb{C}$-Algebra mit Einselement χ^0.

Wir bezeichnen $\mathbb{C}[S_\sigma]$ mit A_σ.

3.3.6. Lemma

A_σ ist endlich erzeugt.

Beweis:

Ist σ ein streng konvexer rationaler polyedrischer Kegel, so ist die Halbgruppe $S_\sigma = \check{\sigma} \cap M$ endlich erzeugt (Gordansches Lemma). Seien $u_1, \ldots, u_n$ die Erzeugenden von S_σ, also gilt $u = \sum m_i u_i$ für $u \in S_\sigma$.

$\mathbb{C}[S_\sigma]$ wird erzeugt von χ^u mit $u \in S_\sigma$. Es gilt $\chi^u = \chi^{\sum m_i u_i} = \prod (\chi^{u_i})^{m_i}$, also ist auch $\mathbb{C}[S_\sigma]$ endlich erzeugt.

$\$$

3.3.7. Bemerkung

Die Einbettung $j : S_\sigma \to \mathbb{C}[S_\sigma]$ hat die folgende universelle Eigenschaft:
Zu jedem Halbgruppenhomomorphismus $h : S_\sigma \to A$ in eine $\mathbb{C}$ -Algebra A mit $h(0) = 1$ existiert genau ein Algebrenhomomorphismus $g : \mathbb{C}[S_\sigma] \to A$ mit $h = g \circ j$.
g ist dabei gegeben durch $g(\sum \alpha_u \chi^u) = \sum \alpha_u j(u)$.

Zur Veranschaulichung als Diagramm:

$$\begin{tikzcd}
\mathbb{C}[S_\sigma] \arrow[r, dashed, "\exists ! g"] & A \\
S_\sigma \arrow[u, "j"] \arrow[ur, "h"'] &
\end{tikzcd}$$

Da Algebrenhomomorphismen $f : A \to B$ stets das Einselement von A auf das Einselement von B abbilden, betrachten wir nur Halbgruppenhomomorphismen, die 0 auf 1 abbilden.

Damit gilt:

$$(\mathrm{Hom}_{\mathrm{hg}}(S_\sigma, A) \text{ mit } 0 \mapsto 1\ ) \simeq \mathrm{Hom}_{\mathrm{alg}}(\mathbb{C}[S_\sigma], A).$$

Die Varietät U_σ zum streng konvexen rationalen polyedrischen Kegel σ wird nun folgendermaßen definiert:

$$U_\sigma = \mathrm{Spec}\,(\mathbb{C}[S_\sigma]) = \mathrm{Spec}\,(A_\sigma)$$

Nach den allgemeinen Vorbemerkungen gilt also:

$$\begin{array}{rcl}
\mathrm{Spec}\, A_\sigma & = & \text{Menge der maximalen Ideale von } A_\sigma \\
 & \cong & \text{Menge der Algebrenhomomorphismen } A_\sigma \to \mathbb{C} \\
 & & \qquad \text{(nach Nullstellensatz)} \\
 & \cong & \text{Menge der Halbgruppenhomomorphismen } S_\sigma \to \mathbb{C} \text{ mit } 0 \mapsto 1 \\
 & & \qquad \text{(universelle Eigenschaft)}
\end{array}$$

Beispiel:

Konstruiert man dies im einfachsten Fall $\sigma = \{0\}$, so hat man $\check{\sigma} = (\mathbb{R}^n)^*$, also $S_\sigma = M$.

Als Halbgruppe hat M die Erzeugenden $\pm e_1^*, \ldots, \pm e_n^*$, und man erhält

$$\mathbb{C}[M] = \mathbb{C}[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}].$$

Dies ist der Ring der *Laurentpolynome* in n Variablen.

Die zugehörige Varietät $U_{\{0\}} = \operatorname{Spec}(\mathbb{C}[M])$ ist die Menge der Algebrenhomomorphismen $f : \mathbb{C}[X_1, X_1^{-1}, \ldots, X_n, X_n^{-1}] \to \mathbb{C}$. Diese sind bestimmt durch die Bilder der X_i. Wegen $f(X_i^{-1}) = f(X_i)^{-1}$ gilt $f(X_i) \in \mathbb{C}^\times$.

Daher gilt

$$U_{\{0\}} \cong (\mathbb{C}^\times)^n.$$

$U_{\{0\}}$ ist also der affine algebraische Torus.

3.3.8. Satz

Sei σ ein streng konvexer rationaler polyedrischer Kegel und τ eine Seite von σ. Dann gibt es eine Einbettung von U_τ nach U_σ als prinzipal offene Menge.

Beweis:

Sei τ eine Seite des Kegels σ. Nach dem Satz auf Seite 46 existiert ein $u \in S_\sigma$ mit $\tau = \sigma \cap u^\perp$ und

$$S_\tau = S_\sigma + \mathbb{N} \cdot (-u).$$

Die Basiselemente von $\mathbb{C}[S_\tau]$ lassen sich dann in der Form

$$\chi^t = \chi^{w-pu} = \frac{\chi^w}{(\chi^u)^p}$$

mit $w \in S_\sigma$ und $p \in \mathbb{N}$ schreiben.

Daher gilt

$$A_\tau = (A_\sigma)_{\chi^u}$$

Nach den Vorbemerkungen im Abschnitt 3.3.1 folgt damit die Behauptung.

3.3.9. Korollar

U_σ enthält den Torus $(\mathbb{C}^\times)^n$ als prinzipal offene Menge.

Beweis:

Man setze im gerade bewiesenen Satz $\tau = \{0\}$. Nach dem Beispiel ist $U_{\{0\}} = (\mathbb{C}^\times)^n$.

3.3.10. Satz

Die Varietät U_σ zum streng konvexen rationalen polyedrischen Kegel σ ist eine torische Varietät.

Beweis:

1. Nach dem eben bewiesenen Korollar enthält U_σ den Torus T^n als prinzipal offene Menge. Prinzipal offene Mengen sind stets dicht.
2. Für einen Kegel σ in N ist die Aktion des Torus T_N auf U_σ wie folgt: Der Torus $T^n = T_N$ läßt sich nach Abschnitt 3.3.1 schreiben als

   $$T_N = \mathrm{Spec}(\mathbb{C}[M]) = \mathrm{Hom}(M, \mathbb{C}^\times),$$

   ein Punkt $t \in T_N$ kann also mit einem Gruppenhomomorphismus $t : M \to \mathbb{C}^\times$ identifiziert werden.

Bei der Konstruktion von U_σ haben wir gesehen, dass die Punkte von $x \in U_\sigma$ Halbgruppenhomomorphismen von S_σ nach $\mathbb{C}$ entsprechen.

Das Produkt $t \cdot x$ ist dann der Halbgruppenhomomorphismus von S_σ nach $\mathbb{C}$, der durch

$$u \mapsto t(u) \cdot x(u)$$

gegeben ist.

Für die Bestimmung der Parameter der torischen Codes im nächsten Kapitel wird es essentiell sein, dass die betrachtete torische Varietät glatt ist, also keine Singularitäten hat. Dazu zitieren wir folgenden Satz ohne Beweis:[1]

3.3.11. Satz

Eine affine torische Varietät U_σ ist genau dann glatt, wenn die Erzeugenden des Kegels σ Teil einer Basis des Gitters N sind.
In diesem Fall gilt

$$U_\sigma \cong \mathbb{C}^k \times (\mathbb{C}^\times)^{n-k}, \quad k = \dim \sigma \tag{1}$$

[1] siehe [3], Abschnitt 2.1, Proposition auf Seite 29.

3.4 Fächer und torische Varietäten

In diesem Abschnitt sollen allgemeine torische Varietäten aus bestimmten Kollektionen von Kegeln, den sogenannten Fächern, konstruiert werden. Dies geschieht, indem die zu den Kegeln gehörenden affinen torischen Varietäten geeignet verklebt werden.

Die grobe Idee ist dabei folgende: Wir haben eben gesehen, dass die affine torische Varietät U_τ zu einer Seite τ von σ bereits eine dichte offene Teilmenge der affinen torischen Varietät U_σ ist. Die affinen Varietäten werden dann längs dieser Mengen zusammengeklebt.

Da man die affinen torischen Varietäten längs dieser Varietäten zu gemeinsamen Seiten verkleben will, ergibt sich folgender Begriff des Fächers:

3.4.1. Definition

Eine Menge Δ von streng konvexen rationalen polyedrischen Kegeln $\sigma \subset \mathbb{R}^n$ heißt *Fächer in N*, wenn gilt:

- Jede Seite eines Kegels in Δ ist wieder ein Element von Δ.
- Der Durchschnitt zweier Kegel in Δ ist eine gemeinsame Seite beider Kegel.

Bemerkung: Hier sollen nur Fächer aus endlich vielen Kegeln betrachtet werden.

Die Konstruktion der Varietät zum Fächer Δ erfolgt nun folgendermaßen: Für zwei Kegel σ_1 und σ_2 nimmt man die disjunkte Vereinigung der Varietäten U_{σ_1} und U_{σ_2}. Die Varietät $U_{\sigma_1 \cap \sigma_2}$ ist dann eine prinzipal offene Untervarietät von U_{σ_1} und U_{σ_2}, und mittels dieser Einbettung werden U_{σ_1} und U_{σ_2} verklebt.

Das Hauptresultat ist dann:

3.4.2. Satz

Sei Δ ein Fächer, bestehend aus den Kegeln σ_i. Dann ist die Varietät $V(\Delta)$, die durch das Verkleben aller affinen torischen Varietäten jeweils entlang der Varietäten zu den gemeinsamen Seiten der Kegel entsteht, eine torische Varietät.

Dieser Satz soll hier nicht bewiesen werden.[2] Insbesondere ist zu zeigen, dass durch den Verklebungsprozess wieder eine Varietät entsteht.

Beispiele:

1. Betrachten wir zunächst Dimension 1 mit $N = \mathbb{Z}$. Dann gibt es folgende Fächer:

$$\Delta_1 = \{\{0\}\}, \quad \Delta_2 = \{\{0\}, \mathbb{R}_{\geq 0}\}, \quad \Delta_3 = \{\{0\}, \mathbb{R}_{\leq 0}\} \quad \text{und}$$
$$\Delta_4 = \{\{0\}, \mathbb{R}_{\geq 0}, \mathbb{R}_{\leq 0}\}.$$

Die zu den Fächern eins bis drei gehörenden torischen Varietäten sind die bereits bekannten affinen Varietäten: $\mathbb{C}^\times$ im ersten Fall und $\mathbb{C}$ im zweiten und dritten Fall. Die Varietät zu Δ_4 ergibt sich, indem wir längs der Varietät zur gemeinsamen Seite $\{0\}$, also entlang $U_{\{0\}} = \mathbb{C}^\times$ verkleben. Dies muss mit der Funktion $1/x$ geschehen, und man erhält

$$V_{\Delta_4} = \mathbb{C} \cup \{\infty\} = \mathbb{P}^1(\mathbb{C}).$$

2. Sei $N = \mathbb{Z}^2$ mit Standardbasis e_1, e_2, und seien $\sigma = \mathbb{R}_{\geq 0} \cdot e_1$ und $\tau = \mathbb{R}_{\geq 0} \cdot e_2$. Dazu betrachten wir den Fächer

$$\Delta = \{\{0\}, \sigma, \tau\}.$$

Die torischen Varietäten zu den Kegeln sind: $U_{\{0\}} = \mathbb{C}^\times \times \mathbb{C}^\times$, $U_\sigma = \mathbb{C} \times \mathbb{C}^\times$ und $U_\tau = \mathbb{C}^\times \times \mathbb{C}$. Verklebt man längs $U_{\{0\}}$, so ergibt sich

$$V_\Delta = \mathbb{C}^2 - \{(0,0)\}.$$

Ein weiteres zweidimensionales Beispiel findet sich am Ende des nächsten Abschnitts.

[2] siehe [3], Abschnitt 1.4

3.5 Die torische Varietät eines Polytops

Im vorigen Abschnitt haben wir gesehen, wie man eine torische Varietät aus einem Fächer konstruiert. Nun wollen wir Fächer aus Polytopen konstruieren, denen wir dann wieder torische Varietäten zuordnen. Mit dieser Konstruktion erhält man nur eine gewisse Klasse von Fächern, nämlich die zu projektiven torischen Varietäten gehörenden.

3.5.1. Definition

Ein *konvexes Polytop* $\Pi \subset \mathbb{R}^n$ ist die konvexe Hülle einer endlichen Menge von Punkten.

Bei uns werden nur zweidimensionale Polytope im $\mathbb{R}^2$ betrachtet. Sei $M \cong \mathbb{Z}^2$ ein zweidimensionales Gitter und $N = \mathrm{Hom}_{\mathbb{Z}}(M, \mathbb{Z})$ das duale Gitter.

3.5.2. Bemerkung

Polytope sollen stets Eckpunkte in M haben. Da bei den explizit betrachteten torischen Codes stets $M = \mathbb{Z}$ gilt, haben die Polytope dann sogar ganzzahlige Eckpunkte. In diesem Fall besteht der aus dem Polytop konstruierte Fächer aus rationalen Kegeln.

Nun soll aus dem Polytop ein Fächer konstruiert werden. Dazu wird das Polytop zunächst als Durchschnitt von Halbräumen dagestellt.

Wie bei den Kegeln bezeichnen wir die Seiten der Codimension 1 als Facetten. Für jede Facette F von Π gibt es einen inneren Normalenvektor $n_F \in M$ und eine ganze Zahl a_F, so dass Π geschrieben werden kann als:

$$\Pi = \bigcap_{F \text{ Facette von } \Pi} \{v \in \mathbb{R}^n | (v|n_F) \geq -a_F\}$$

Die Wahl des Normalenvektors wird eindeutig, wenn man zusätzlich verlangt, dass n_F minimale Länge hat.

Zu einer Seite S von Π sei σ_S der Kegel, der von den n_F zu allen Facetten erzeugt wird, die S enthalten. Dann ist

$$\Delta_\Pi = \{\sigma_S | S \text{ Seite von } \Pi\}$$

der *normale Fächer* zum Polytop Π.

Dadurch ergibt sich eine inklusionsumkehrende Bijektion zwischen den Seiten des Polytops und den Kegeln des Fächers.

$$\sigma_S \in \Delta_\Pi \qquad \longleftrightarrow \qquad S \subset \Pi$$

Zum Fächer Δ wird dann die torische Varietät V_Δ wie gewohnt konstruiert.

3.5.3. Bemerkung

Konstruiert man einen Fächer Δ mittels eines Polytops, so hat Δ automatisch folgende Eigenschaften:

- Δ besteht nur aus endlich vielen Kegeln.
- Δ ist vollständig, d.h. $\operatorname{supp} \Delta := \cup_{\sigma \in \Delta} = \mathbb{R}^2$.

Das hat zur Folge, dass die torische Varietät V_Δ kompakt ist (siehe [13], Abschnitt 1.4, Theorem 1.11).

Beispiel:

Sei Π das Einheitsquadrat mit den Eckpunkten $(1/2, 1/2)$, $(1/2, -1/2)$, $(-1/2, 1/2)$, $(-1/2, -1/2)$.

Dann gilt:

$$\begin{aligned} \Pi &= \{(x,y) \in \mathbb{R}^2 | x \geq -1/2\} \cap \{(x,y) \in \mathbb{R}^2 | x \leq 1/2\} \\ &\quad \cap \{(x,y) \in \mathbb{R}^2 | y \geq -1/2\} \cap \{(x,y) \in \mathbb{R}^2 | y \leq 1/2\} \end{aligned}$$

$$
\begin{aligned}
= \ & \left\{(x,y) \in \mathbb{R}^2 \,\middle|\, \left(\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} 2 \\ 0 \end{pmatrix} \right) \geq -1 \right\} \\
& \cap \left\{(x,y) \in \mathbb{R}^2 \,\middle|\, \left(\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} -2 \\ 0 \end{pmatrix} \right) \geq -1 \right\} \\
& \cap \left\{(x,y) \in \mathbb{R}^2 \,\middle|\, \left(\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} 0 \\ 2 \end{pmatrix} \right) \geq -1 \right\} \\
& \cap \left\{(x,y) \in \mathbb{R}^2 \,\middle|\, \left(\begin{pmatrix} x \\ y \end{pmatrix} \middle| \begin{pmatrix} 0 \\ -2 \end{pmatrix} \right) \geq -1 \right\}
\end{aligned}
$$

Die inneren Normalen sind also $\pm 2e_1$, $\pm 2e_2$.

Das ergibt folgenden Fächer:

- Die Facetten von Π ergeben die eindimensionalen Kegel, welche von den inneren Normalen erzeugt werden.
- Die Ecken von Π liegen jeweils in zwei Facetten. Zu $(-1/2, 1/2)$ etwa gehören die inneren Normalen $2e_1$ und $-2e_2$ und damit der von $2e_1$ und $-2e_2$ erzeugte zweidimensionale Kegel.

Im Bild ist der Kegel $\{0\}$ durch ein Kreuz dargestellt, die eindimensionalen Kegel durch schwarze Geraden und die zweidimensionalen Kegel sind grau schraffiert.

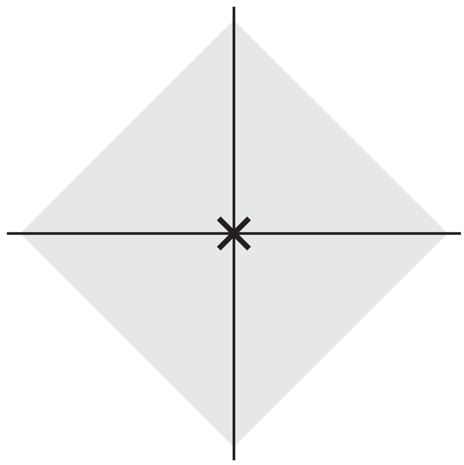

Bild 3.1.

Die affinen torischen Varietäten zu den zweidimensionalen Kegeln σ_i sind $U_{\sigma_i} = \mathbb{C}^2$, diese werden verklebt zu $X_\Pi = \mathbb{P}^1 \times \mathbb{P}^1$.

3.6 Die Trägerfunktion eines Polytops

3.6.1. Definition

Sei Π ein zweidimensionales rationales konvexes Polytop im $\mathbb{R}^2$. Die Trägerfunktion $h_\Pi : (\mathbb{R}^2)^* \to \mathbb{R}$ des Polytops Π ist gegeben durch

$$h_\Pi(n) = \inf\{\,(m|n)|\, m \in \Pi\}.$$

Mit Hilfe der Trägerfunktion ergibt sich eine alternative Möglichkeit, den im vorigen Abschnitt erklärten normalen Fächer eines Polytops zu konstruieren.

Sei Π ein Polytop und h_Π seine Trägerfunktion. Dann ist h_Π stückweise linear im folgenden Sinne: $(\mathbb{R}^2)^*$ läßt sich als Vereinigung nichtleerer streng konvexer Kegel σ schreiben, so dass h_Π auf jedem dieser Kegel linear ist. Man betrachtet nun den von den Kegeln σ erzeugten Fächer. Der gröbste Fächer, für den h_Π auf jedem Kegel des Fächers linear ist, ist der *normale Fächer* von Π.

Ist Δ ein Fächer, und ist h linear auf jedem $\sigma \in \Delta$, so nennt man h *Δ-linear.*

Sei Δ der normale Fächer von Π. Da h_Π auf jedem Kegel $\sigma \in \Delta$ linear ist, existiert für alle $\sigma \in \Delta$ ein $\lambda_\sigma \in M$ mit

$$h_\Pi(n) = (\lambda_\sigma|n) \quad \text{für alle } n \in \sigma.$$

Die eindimensionalen Kegel $\tau \in \Delta$ werden, wie wir in Abschnitt 3.5 gesehen haben, von den inneren Facettennormalen $n(\tau) \in \tau \cap N$ minimaler Länge erzeugt.

Durch eventuelles Verfeinern des Fächers kann man erreichen, dass jeweils zwei aufeinanderfolgende Facettennormalen eine $\mathbb{Z}$-Basis des Gitters N bilden. Das Ergebnis ist der *verfeinerte normale Fächer.* Die torische Varietät des verfeinerten normalen Fächers ist dann eine glatte Varietät.[3]

[3]siehe Seite 53.

3.7 Orbits der Torusaktion

Die torische Varietät V_Δ zerfällt in Orbits unter der Aktion des Torus T. Die Aktion des Torus ist dabei folgendermaßen definiert:[4] Sei $t \in T = \mathrm{Hom}(M, \mathbb{C}^\times)$ und $x \in U_\sigma = \mathrm{Hom}_{\mathrm{hg}}(S_\sigma, \mathbb{C})$. Das Produkt $t \cdot x$ ist dann der Halbgruppenhomomorphismus von S_σ nach $\mathbb{C}$, der durch $u \mapsto t(u) \cdot x(u)$ gegeben ist. Es gilt $t \cdot x \in U_\sigma$, also ist U_σ für alle Kegel $\sigma \in \Delta$ T-invariant.

Die Orbits von V_Δ unter T entsprechen eins zu eins den Kegeln $\sigma \in \Delta$. Zu einem Kegel σ ist der Orbit gegeben durch

$$O_\sigma = \mathrm{orb}\, \sigma = \mathrm{Hom}(M \cap \sigma^\perp, \mathbb{C}^\times),$$

und jeder T-Orbit ist von dieser Form.

Um die Orbits für spezielle Kegel explizit beschreiben zu können, definiert man:

3.7.1. Definition

Sei σ ein Kegel in N und U_σ die zugehörige affine Varietät. Der *ausgezeichnete Punkt* x_σ von U_σ ist der Halbgruppenhomomorphismus

$$x_\sigma : S_\sigma \to \mathbb{C}, \quad u \mapsto \begin{cases} 1 & \text{für } u \in \sigma^\perp \\ 0 & \text{sonst.} \end{cases}$$

Der zum Kegel σ gehörende Orbit O_σ enthält den ausgezeichneten Punkt von U_σ.

Allgemein gilt

$$O_\sigma \cong (\mathbb{C}^\times)^{n-k} \quad \text{falls } \dim \sigma = k,$$

und insbesondere $O_{\{0\}} = T$ und $O_\sigma = \{x_\sigma\}$ für $\dim \sigma = n$.

Der Abschluss von O_σ wird mit $V(\sigma)$ bezeichnet.

[4]siehe Abschnitt 3.3.2, Seite 53.

3.8 Divisoren auf torischen Varietäten

In Abschnitt 2.2 haben wir bereits Divisoren auf eindimensionalen Varietäten kennengelernt. Diese Divisoren, die als Linearkombinationen von Punkten der Kurve definiert wurden, sind ein Spezialfall der Weil-Divisoren:

3.8.1. Definition

Sei V eine Varietät. Ein *Weil-Divisor* auf V ist eine endliche formale Summe irreduzibler abgeschlossener Untervarietäten V_i der Codimension 1.

Wir brauchen nun noch eine weitere Sorte on Divisoren, die Cartier-Divisoren. Ein *Cartier-Divisor* D ist gegeben durch eine offene Überdeckung $V = \cup U_i$ und rationale Funktionen $f_i \not\equiv 0$ (genannt lokale Gleichungen), so dass f_i/f_j und f_j/f_i reguläre Funktionen ohne Nullstellen auf $U_i \cap U_j$ sind. Dann setzt man $D = \operatorname{div}(f_i^{-1})$ auf U_i.

Ein Cartier-Divisor D bestimmt stets einen Weil-Divisor $[D]$ per

$$[D] = \sum_{\operatorname{codim} V_i = 1} \operatorname{ord}_{V_i}(D) \cdot V_i.$$

ord_{V_i} ist dabei die Ordnung, mit der die Gleichung für D im lokalen Ring entlang der Untervarietät V_i verschwindet.

Da in unserem Fall die Varietät V stets glatt ist, sind die lokalen Ringe der irreduziblen Untervarietäten der Codimension eins diskrete Bewertungsringe, so dass die Ordnung dem bekannten Begriff entspricht.

Zu einer rationalen Funktion $f \not\equiv 0$ hat man ihren *Hauptdivisor* $\operatorname{div} f$, dessen lokale Gleichung in jeder offenen Menge gleich f ist.

In unserem Fall sind die Divisoren von Interesse, die invariant unter der Torus-Aktion sind. Wir haben bereits gesehen, dass die Orbits von V_Δ unter der Torusaktion den Kegeln des Fächers Δ entsprechen. Die irreduziblen Untervarietäten der Codimension eins entprechen dabei den eindimensionalen Kegeln $\tau \in \Delta$.

Seien $\tau_1, \ldots, \tau_d$ die eindimensionalen Kegel des Fächers. Die entsprechenden Divisoren sind die im vorigen Abschnitt definierten Orbitabschlüsse

$$D_i = V(\tau_i).$$

Die torusinvarianten Weil-Divisoren werden als *T-Weil-Divisoren* bezeichnet. Sie sind gegeben durch endliche Summen

$$\sum a_i D_i$$

mit ganzen Zahlen a_i. Die D_i bilden also eine $\mathbb{Z}$-Basis der T-Weil-Divisoren.

Die Cartier-Divisoren, die invariant unter der Torusaktion sind, werden *T-Cartier-Divisoren* genannt. Sie sind von der Form

$$D = \mathrm{div}(\chi^u)$$

(siehe [3], Abschnitt 3.3).

Kapitel 4

Torische Codes

In diesem Kapitel werden fehlerkorrigierende Codes dadurch konstruiert, dass rationale Funktionen auf einer torischen Fläche, also einer zweidimensionalen torischen Varietät, ausgewertet werden. Dabei sind die torischen Flächen jeweils durch ein rationales konvexes Polytop gegeben (siehe Abschnitt 3.5).

Das Kapitel orientiert sich inhaltlich zunächst an den Artikeln “Toric Surfaces and Error-Correcting Codes” und “Toric Varieties Hirzebruch Surfaces and Error-Correcting Codes” von Johan P. Hansen ([5] und [6]). Der zweite Artikel ist eine überarbeitete Version des ersten. Anschließend werden die Parameter der torischen Codes noch in Beziehung zur Gilbert-Varshamov-Schranke (Abschnitt 1.2.1) gesetzt.

Zum Beweis der Sätze über die Parameter torischer Codes verweist Hansen auf die Standardliteratur wie [3] und [13]. In diesen Büchern wird die Theorie torischer Varietäten über $\mathbb{C}$ entwickelt, die Konstruktion ist jedoch für einen beliebigen algebraisch abgeschlossenen Körper möglich.

Um die Theorie für den endlichen Körper $\mathbb{F}_q$ benutzen zu können, arbeitet man zunächst über einem algebraischen Abschluss $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$. Um zum Grundkörper $\mathbb{F}_q$ überzugehen, betrachtet man die Objekte, die invariant unter dem Frobenius-Homomorphismus sind. Diese Strategie würde allerdings den Rahmen dieser Arbeit sprengen, daher gehen wir wie Hansen davon aus, dass die Sätze weiterhin ihre Gültigkeit behalten, obwohl $\mathbb{F}_q$ nicht algebraisch abgeschlossen ist.

In diesem Kapitel sei stets $M \cong \mathbb{Z}^2$ ein Gitter und $N = \operatorname{Hom}(M, \mathbb{Z})$ das duale Gitter.

4.1 Definition und Beispiele

Sei F_q der Körper mit q Elementen für eine Primzahlpotenz q. Sei M ein zweidimensionales Gitter in $\mathbb{Z}^2$ und sei (m_1, m_2) eine $\mathbb{Z}$-Basis von M. Sei Π ein zweidimensionales konvexes Polytop mit Ecken in M.

Sei $\xi \in \mathbb{F}_q$ ein primitives Element. Für i, j mit $0 \leq i, j < q - 1$ setzen wir $P_{ij} = (\xi^i, \xi^j) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times$. Für jedes Element $u \in M \cap \Pi$ gibt es ein eindeutiges Paar $(\lambda_1, \lambda_2) \in \mathbb{Z}^2$, so dass

$$u = \lambda_1 m_1 + \lambda_2 m_2.$$

Damit setzen wir:

$$\chi^u(P_{ij}) = \left(\xi^i\right)^{\lambda_1} \cdot \left(\xi^j\right)^{\lambda_2}$$

4.1.1. Definition

Der Vektorraum $\mathcal{C}_\Pi$, der von den Vektoren

$$\{\chi^u(P_{ij})_{0 \leq i,j < q-1} | u \in M \cap \Pi\} \tag{1}$$

erzeugt wird, ist der *torische Code* des rationalen konvexen Polyeders Π.

4.1.2. Bemerkung

Torische Codes werden nach ihrem Erfinder Johan P. Hansen auch als *Hansen-Codes* bezeichnet.

4.1.3. Bemerkung

Per Konstruktion hat der oben definierte torische Code die Länge $(q-1)^2$.

4.1.1 Beispiele

In den nächsten Abschnitten werden wir sehen, dass man zu speziellen Polytopen die Dimension und Minimaldistanz der Hansen-Codes explizit angeben kann. Zu jedem dieser Polytope soll nun ein einfaches Beispiel berechnet werden.

Es wird dabei stets mit dem kleinsten nichttrivialen Polytop des gegebenen Typs gearbeitet und dazu das kleinstmögliche q bestimmt, für welches das Polytop echt im Quadrat mit der Seitenlänge $q-1$ enthalten ist.

In allen Beispielen ist $M = \mathbb{Z}^2$ mit Basis $v_1 = (1,0)$, $v_2 = (0,1)$.

Beispiel 1:

Sei Π_1 das Polytop mit den Ecken $(0,0)$, $(1,1)$ und $(0,2)$. Dann besteht $M \cap \Pi_1$ aus den Punkten $u_1 = (0,0)$, $u_2 = (0,1)$, $u_3 = (1,1)$ und $u_4 = (0,2)$.

$$\begin{aligned}
u_1 &= (0,0) = 0v_1 + 0v_2 \;\Rightarrow\; \lambda_1(u_1) = 0,\; \lambda_2(u_1) = 0,\\
u_2 &= (0,1) = 0v_1 + 1v_2 \;\Rightarrow\; \lambda_1(u_2) = 0,\; \lambda_2(u_2) = 1,\\
u_3 &= (1,1) = 1v_1 + 1v_2 \;\Rightarrow\; \lambda_1(u_3) = 1,\; \lambda_2(u_3) = 1,\\
u_4 &= (0,2) = 0v_1 + 2v_2 \;\Rightarrow\; \lambda_1(u_4) = 0,\; \lambda_2(u_4) = 2.
\end{aligned}$$

Sei $q = 4$ und $\mathbb{F}_4 = \mathbb{F}_2/(X^2+X+1) = \{0,1,X,X+1\}$. Ein erzeugendes Element von $\mathbb{F}_4^\times$ ist X, denn $X^2 = X+1$ und $X^3 = 1$. Damit ergibt sich:

$$\begin{array}{lll}
P_{11} = (X,X), & P_{12} = (X,X+1), & P_{13} = (X,1)\\
P_{21} = (X+1,X), & P_{22} = (X+1,X+1), & P_{23} = (X+1,1)\\
P_{31} = (1,X), & P_{32} = (1,X+1), & P_{33} = (1,1)
\end{array}$$

Man erhält zum Beispiel

$$\chi^{u_2}(P_{21}) = (X+1)^0 \cdot (X)^1 = X,$$

und insgesamt:

	P_{11}	P_{12}	P_{13}	P_{21}	P_{22}	P_{23}	P_{31}	P_{32}	P_{33}
$\chi^{u_1}(P_{ij})$	1	1	1	1	1	1	1	1	1
$\chi^{u_2}(P_{ij})$	X	$X+1$	1	X	$X+1$	1	X	$X+1$	1
$\chi^{u_3}(P_{ij})$	$X+1$	1	X	1	X	$X+1$	X	$X+1$	1
$\chi^{u_4}(P_{ij})$	$X+1$	X	1	$X+1$	X	1	$X+1$	X	1

Die Zeilen der Tabelle sind linear unabhängig, daher hat der Code $\mathcal{C}_{\Pi_1}$ die Dimension $k = 4$.

Mit Hilfe von Computeralgebra stellt man fest, dass der Code die Minimaldistanz $d = 3$ hat.

Beispiel 2:

Sei Π_2 das Polytop mit den Ecken $(0,0)$, $(1,0)$ und $(0,1)$. Dann besteht $M \cap \Pi_2$ nur aus den Eckpunkten von Π_2: $u_1 = (0,0)$, $u_2 = (1,0)$ und $u_3 = (0,1)$.

$$\begin{aligned}
u_1 = (0,0) = 0v_1 + 0v_2 &\;\Rightarrow\; \lambda_1(u_1) = 0,\; \lambda_2(u_1) = 0,\\
u_2 = (1,0) = 1v_1 + 0v_2 &\;\Rightarrow\; \lambda_1(u_2) = 1,\; \lambda_2(u_2) = 0,\\
u_3 = (0,1) = 0v_1 + 1v_2 &\;\Rightarrow\; \lambda_1(u_3) = 0,\; \lambda_2(u_3) = 1.
\end{aligned}$$

Sei $q = 3$. Ein erzeugendes Element von $\mathbb{F}_3^\times$ ist 2, damit ergibt sich:

$$P_{11} = (2,2), \quad P_{12} = (2,1), \quad P_{21} = (1,2), \quad P_{22} = (1,1).$$

Damit ergibt sich etwa

$$\chi^{u_1}(P_{11}) = (2)^0 \cdot (2)^0 = 1,$$

also insgesamt:

P_{ij}	P_{11}	P_{12}	P_{21}	P_{22}
$\chi^{u_1}(P_{ij})$	1	1	1	1
$\chi^{u_2}(P_{ij})$	2	2	1	1
$\chi^{u_3}(P_{ij})$	2	1	2	1

Die Vektoren $(1,1,1,1)$, $(2,2,1,1)$ und $(2,1,2,1)$ sind im $\mathbb{F}_3^4$ linear unabhängig, also hat der Code $\mathcal{C}_\Pi$ die Dimension $k = 3$.

Explizit ergibt sich:

$$\begin{aligned}
\mathcal{C}_\Pi &= L((1,1,1,1),(2,2,1,1),(2,1,2,1))\\
&= \{(0,0,0,0),(1,1,1,1),(2,2,2,2),(2,2,1,1),(1,1,2,2),(1,2,1,2),\\
&\quad (2,1,2,1),(2,2,0,0),(0,0,1,1),(0,0,2,2),(2,0,2,0),(0,1,0,1),\\
&\quad (0,2,0,2),(2,0,0,1),(0,1,2,0),(0,2,1,0),(1,1,0,0),(1,0,1,0),\\
&\quad (1,0,0,2),(0,1,1,2),(1,2,2,0),(1,2,0,1),(1,0,2,1),(2,0,1,2),\\
&\quad (2,1,0,2),(2,1,1,0),(0,2,2,1)\}.
\end{aligned}$$

Der Code hat also Minimaldistanz $d = 2$.

Beispiel 3:

Sei Π_3 das Polytop mit den Ecken $(0,0)$, $(1,0)$, $(1,1)$ und $(0,1)$. Dann besteht $M \cap \Pi_3$ nur aus den Eckpunkten von Π_3: $u_1 = (0,0)$, $u_2 = (1,0)$, $u_3 = (1,1)$ und $u_4 = (0,1)$.

$$\begin{aligned}
u_1 &= (0,0) = 0v_1 + 0v_2 &\Rightarrow\ & \lambda_1(u_1) = 0,\ \lambda_2(u_1) = 0,\\
u_2 &= (1,0) = 1v_1 + 0v_2 &\Rightarrow\ & \lambda_1(u_2) = 1,\ \lambda_2(u_2) = 0,\\
u_3 &= (1,1) = 1v_1 + 1v_2 &\Rightarrow\ & \lambda_1(u_3) = 1,\ \lambda_2(u_3) = 1,\\
u_4 &= (0,1) = 0v_1 + 1v_2 &\Rightarrow\ & \lambda_1(u_4) = 0,\ \lambda_4(u_3) = 1.
\end{aligned}$$

Sei $q = 3$. Ein erzeugendes Element von $\mathbb{F}_3^\times$ ist 2, damit ergibt sich:

$$P_{11} = (2,2), \quad P_{12} = (2,1), \quad P_{21} = (1,2), \quad P_{22} = (1,1).$$

Damit ergibt sich:

P_{ij}	P_{11}	P_{12}	P_{21}	P_{22}
$\chi^{u_1}(P_{ij})$	1	1	1	1
$\chi^{u_2}(P_{ij})$	2	2	1	1
$\chi^{u_3}(P_{ij})$	1	2	2	1
$\chi^{u_4}(P_{ij})$	2	1	2	1

Die Vektoren $(1,1,1,1)$, $(2,2,1,1)$, $(1,2,2,1)$ und $(2,1,2,1)$ sind im $\mathbb{F}_3^4$ linear unabhängig, also gilt $\mathcal{C}_{\Pi_3} = \mathbb{F}_3^4$. Die Minimaldistanz des Codes ist daher 1.

4.2 Torische Codes für spezielle Polytope

Im nächsten Abschnitt wird mit Hilfe der Theorie torischer Varietäten gezeigt, wie man die Dimension und eine untere Schranke für die Minimaldistanz torischer Codes bestimmen kann.

Damit werden dann insbesondere die folgenden Sätze über die Parameter der drei Beispielcodes bewiesen.

M sei weiterhin ein zweidimensionales Gitter mit $M \cong \mathbb{Z}^2$.

4.2.1. Satz

Sei $a \in \mathbb{N}_{>0}$ mit $2a < q-1$. Sei Π_1 das Polytop im $\mathbb{R}^2$ mit den Ecken $(0,0)$, (a,a) und $(0,2a)$ (siehe Bild 4.1).
Dann hat der Code $\mathcal{C}_{\Pi_1}$ die Dimension

$$k = {}^{\#}(M \cap \Pi_1) = (a+1)^2,$$

und für die Minimaldistanz gilt

$$d = (q-1)^2 - 2a(q-1).$$

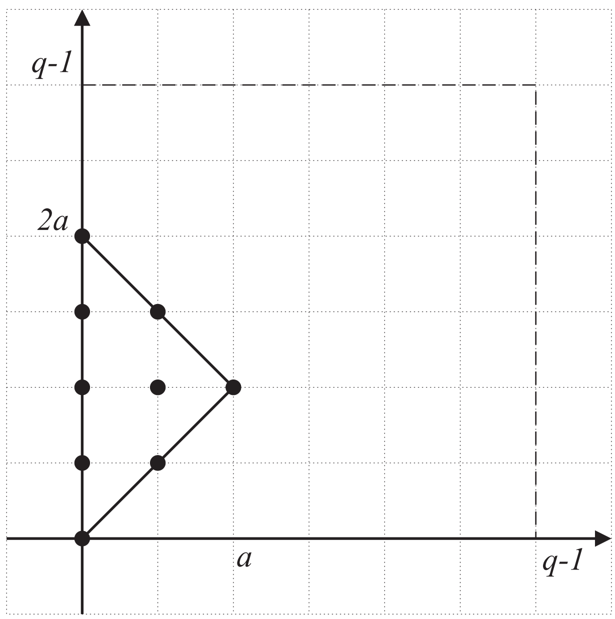

Bild 4.1. Das Polytop Π_1 mit den Ecken $(0,0)$, (a,a) und $(0,2a)$.

4.2.2. Satz

Sei $a \in \mathbb{N}_{>0}$ mit $a < q-1$. Sei Π_2 das Polytop im $\mathbb{R}^2$ mit den Ecken $(0,0)$, $(a,0)$ und $(0,a)$ (siehe Bild 4.2).
Dann hat der Code $\mathcal{C}_{\Pi_2}$ die Dimension

$$k = {}^{\#}(M \cap \Pi_2) = \frac{(a+1)(a+2)}{2},$$

und für die Minimaldistanz gilt

$$d = (q-1)^2 - a(q-1).$$

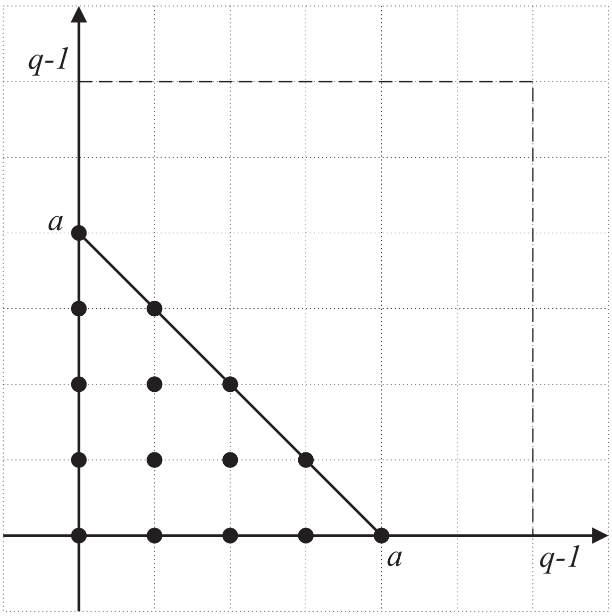

Bild 4.2. Das Polytop Π_2 mit den Ecken $(0,0)$, $(a,0)$ und $(0,a)$.

4.2.3. Satz

Sei $a, b \in \mathbb{N}_{>0}$ mit $a < q-1$ und $b < q-1$. Sei Π_3 das Polytop im $\mathbb{R}^2$ mit den Ecken $(0,0)$, $(a,0)$, (a,b) und $(0,b)$ (siehe Bild 4.3).
Dann hat der Code $\mathcal{C}_{\Pi_3}$ die Dimension

$$k = {}^{\#}(M \cap \Pi_3) = (a+1)(b+1),$$

und für die Minimaldistanz gilt

$$d = (q-1)^2 - (a(q-1) + b(q-1) - ab) = (q-1-a)(q-1-b).$$

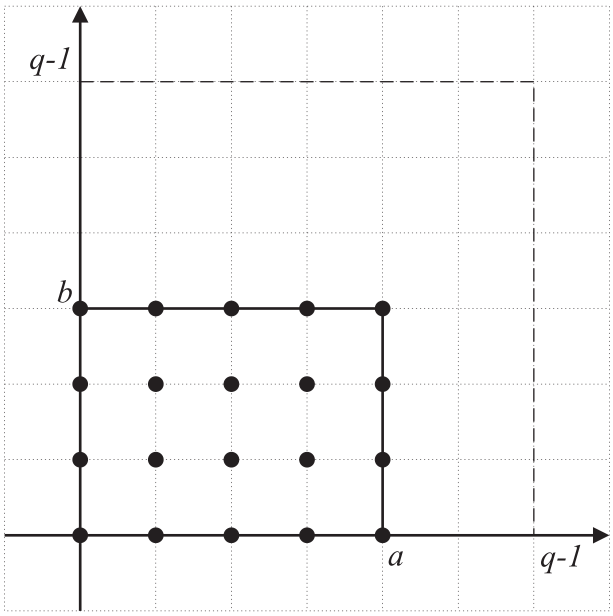

Bild 4.3. Das Polytop Π_3 mit den Ecken $(0,0)$, $(a,0)$, (a,b) und $(0,b)$.

4.2.4. Bemerkung

Im ersten Artikel [5] gab Hansen den Wert für die Minimaldistanz nur als untere Schranke an. Joyner berechnete in seinem Artikel [9] mit dem Computeralgebrasystem MAGMA diverse Hansen-Codes explizit und stellte fest, dass die Minimaldistanz in allen Beispielen mit der unteren Schranke übereinstimmte. Daraufhin stellte er die Vermutung an, die Minimaldistanz entspräche stets diesem Wert. Hansen gibt in seinem Artikel [6] einen Beweis für diese Vermutung an, in dem er jeweils ein Element minimaler Hamming-Norm angibt.

4.3 Anwendung der Theorie torischer Varietäten auf torische Codes

Nun sollen die Erkenntnisse aus Kapitel 3 benutzt werden, um die Parameter der Hansen-Codes, insbesondere in den konkreten Beispielen, zu bestimmen. Dabei wird der torische Code als Bild des Vektorraums $\Gamma(V_\Delta, O(D_h)) = H^0(V_\Delta, O(D_h))$ der globalen Schnitte von $O(D_h)$ unter einer Auswertungsabbildung identifiziert. Diese Abbildung ist injektiv, also entspricht die Dimension des torischen Codes der Dimension von $\Gamma(V_\Delta, O(D_h))$. Die Minimaldistanz erhält man, indem man die Schnittzahl von Divisoren berechnet.

Diese Beweisstrategie ist analog zum eindimensionalen Fall (siehe Abschnitt 2.5).

Im Abschnitt 3.6 haben wir die Trägerfunktion eines Polytops eingeführt und mit ihrer Hilfe den verfeinerten normalen Fächer des Polytops bestimmt. Dies soll hier für die drei Standardbeispiele (die Polytope Π_1, Π_2, und Π_3) berechnet werden.

Beispiel 1:

Sei Π_1 das Polytop aus Satz 4.2.1 (siehe Bild 4.1). Die eindimensionalen Kegel des normalen Fächers werden dann erzeugt von den Facettennormalen $(1, 0)$, $(-1, 1)$ und $(-1, -1)$.

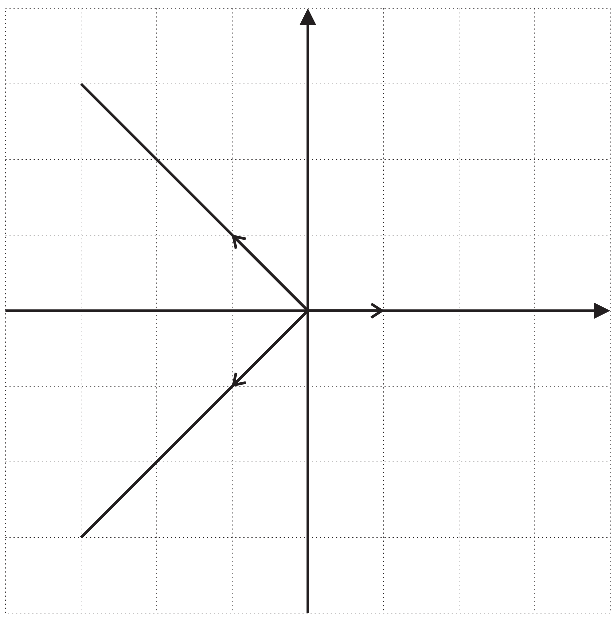

Bild 4.4. Der normale Fächer von Π_1.

Da jedoch $(-1,1)$ und $(-1,-1)$ keine $\mathbb{Z}$-Basis von N bilden, muss der Fächer noch verfeinert werden. Daher nimmt man noch den eindimensionalen Kegel $\mathbb{R}(-1,0)$ dazu. Damit ergibt sich als verfeinerter normaler Fächer von Π_1

$$\Delta = \{\{0\}, \tau_1, \tau_2, \tau_3, \tau_4, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

mit $\tau_1 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\tau_2 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} -1 \\ 1 \end{pmatrix}$, $\tau_3 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $\tau_4 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} -1 \\ -1 \end{pmatrix}$, $\sigma_1 = \tau_1 + \tau_2$, $\sigma_2 = \tau_2 + \tau_3$, $\sigma_3 = \tau_3 + \tau_4$ und $\sigma_4 = \tau_4 + \tau_1$.

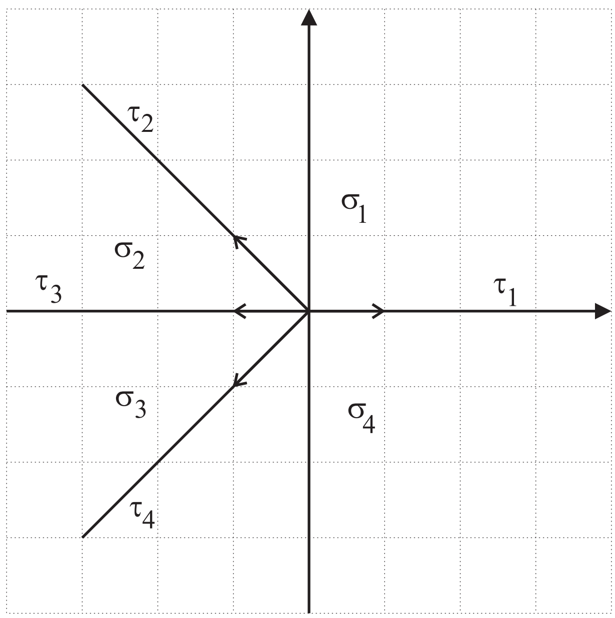

Bild 4.5. Der verfeinerte normale Fächer von Π_1.

Die Trägerfunktion von Π_1 läßt sich dann als $h_{\Pi_1}(n) = (\lambda_\sigma | n)$ für $n \in \sigma$ schreiben:

$$h_{\Pi_1}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} a \\ a \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} a \\ a \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ 2a \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

Beispiel 2:

Sei Π_2 das Polytop aus Satz 4.2.2 (siehe Bild 4.2). Die eindimensionalen Kegel des normalen Fächers werden dann erzeugt von den Facettennormalen $(1,0)$, $(0,1)$ und $(-1,-1)$. Der Fächer muss nicht mehr verfeinert werden, also ergibt sich als verfeinerter normaler Fächer von Π_2

$$\Delta = \{\{0\}, \tau_1, \tau_2, \tau_3, \sigma_1, \sigma_2, \sigma_3\}$$

mit $\tau_1 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\tau_2 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\tau_3 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} -1 \\ -1 \end{pmatrix}$, $\sigma_1 = \tau_1 + \tau_2$, $\sigma_2 = \tau_2 + \tau_3$ und $\sigma_3 = \tau_3 + \tau_1$.

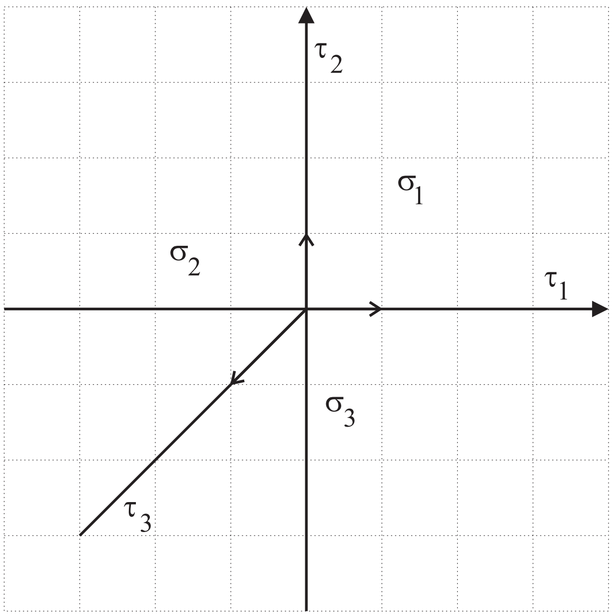

Bild 4.6. Der verfeinerte normale Fächer von Π_2.

Die Trägerfunktion von Π_2 ist dann in der Form $h_{\Pi_2}(n) = (\lambda_\sigma | n)$ für $n \in \sigma$ gegeben durch:

$$h_{\Pi_2}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} a \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} 0 \\ a \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3. \end{cases}$$

Beispiel 3:

Sei Π_3 das Polytop aus Satz 4.2.3 (siehe Bild 4.3). Die eindimensionalen Kegel des normalen Fächers werden dann erzeugt von den Facettennormalen $(1, 0)$, $(0, 1)$, $(-1, 0)$ und $(0, -1)$. Der Fächer muss nicht mehr verfeinert werden, also ergibt sich als verfeinerter normaler Fächer von Π_3

$$\Delta = \{\{0\}, \tau_1, \tau_2, \tau_3, \tau_4, \sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

mit $\tau_1 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\tau_2 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\tau_3 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} -1 \\ 0 \end{pmatrix}$, $\tau_4 = \mathbb{R}_{\geq 0} \cdot \begin{pmatrix} 0 \\ -1 \end{pmatrix}$, $\sigma_1 = \tau_1 + \tau_2$, $\sigma_2 = \tau_2 + \tau_3$, $\sigma_3 = \tau_3 + \tau_4$ und $\sigma_4 = \tau_4 + \tau_1$.

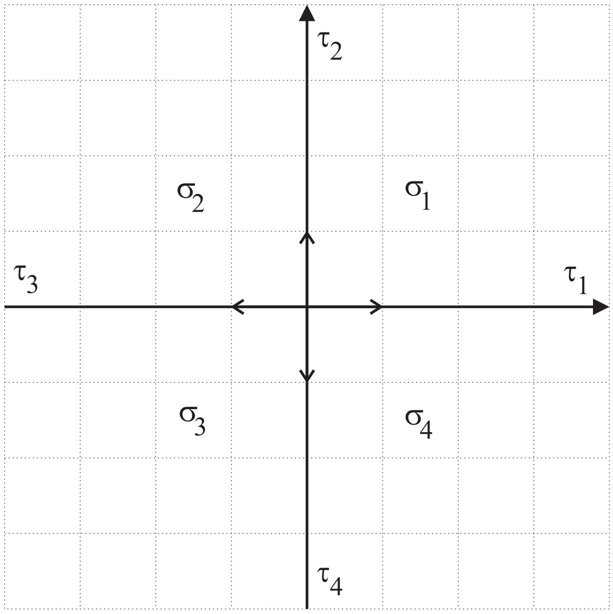

Bild 4.7. Der verfeinerte normale Fächer von Π_3.

Die Trägerfunktion von Π_3 ist dann in der Form $h_{\Pi_3}(n) = (\lambda_\sigma | n)$ für $n \in \sigma$ gegeben durch:

$$h_{\Pi_2}\begin{pmatrix} n_1 \\ n_2 \end{pmatrix} = \begin{cases} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_1, \\ \begin{pmatrix} a \\ 0 \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_2, \\ \begin{pmatrix} a \\ b \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_3, \\ \begin{pmatrix} 0 \\ b \end{pmatrix} \cdot \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} & \text{für } \begin{pmatrix} n_1 \\ n_2 \end{pmatrix} \in \sigma_4. \end{cases}$$

4.3.1 Bestimmung der Parameter der Hansen-Codes

Aus Formel (1) auf Seite 53 folgt für torische Flächen und einen eindimensionalen Kegel τ

$$U_\tau = (\mathbb{F}_q^\times) \times \mathbb{F}_q$$

Im Abschnitt 3.7 haben wir gesehen, dass der zum eindimensionalen Kegel τ gehörende Orbit gegeben ist durch

$$O_\tau = \mathbb{F}_q^\times.$$

$V(\tau)$ ist der Abschluss von O_τ in V_Δ, es gilt

$$V(\tau) = \mathbb{P}^1(\mathbb{F}_q).$$

Durch die Δ-lineare Trägerfunktion h ist ein Weil-Divisor D_h gegeben:

$$D_h = - \sum_{\tau \in \Delta(1)} h(n(\tau))V(\tau), \tag{1}$$

dabei ist $\Delta(1)$ die Menge der eindimensionalen Kegel in Δ.

Setze insbesondere

$$D_u = \mathrm{div}(\chi^{-u}).$$

4.3.1. Satz

Sei h eine Δ-lineare Trägerfunktion mit zugehörigem Cartier-Divisor (siehe Abschnitt 4.3.1, Gleichung (1)) und konvexem Polytop (siehe Abschnitt 3.6). Der Vektorraum $\Gamma(V, O_V(D_h))$ der globalen Schnitte des Geradenbündels $O_V(D_h)$ hat die Dimension $^{\#}(M \cap \Pi_h)$, und eine Basis ist gegeben durch $\{\chi^u | u \in M \cap \Pi_h\}$.

Zum Beweis:

Hier soll kein vollständiger Beweis angegeben werden, sondern lediglich die Idee skizziert werden.

Zunächst wird die affine Situation mit $V = U_\sigma$ behandelt, da die χ^u dort explizit bekannt sind.

Offenbar sind die $\{\chi^u | u \in M \cap \Pi_h\}$ Elemente von $\Gamma(U_\sigma, O(D_h))$.

Es ist zu zeigen, dass die $\{\chi^u | u \in M \cap \Pi_h\}$

- linear unabhängig sind und
- $\Gamma(U_\sigma, O(D_h))$ erzeugen.

Man kann die $\{\chi^u | u \in M \cap \Pi_h\}$ als Charaktere von $T(\mathbb{F}_q)$ nach $\mathbb{F}_q^\times$ auffassen, und Charaktere sind stets linear unabhängig.

Da Δ ein vollständiger Fächer ist[1], ist V eigentlich (über $\mathbb{C}$: kompakt), also ist $\Gamma(V, O_V(D_h))$ ein endlichdimensionaler Vektorraum.

Da der Divisor D_h T-invariant ist, ist auch $\Gamma(U_\sigma, O(D_h))$ invariant unter der Torusaktion. Da T eine kommutative Gruppe ist, zerfällt $\Gamma(U_\sigma, O(D_h))$ unter der Aktion in eindimensionale invariante Unterräume.

Auf den eindimensionalen Unterräumen ist die Aktion durch Multiplikation mit einem Element der multiplikativen Gruppe des Grundkörpers gegeben, also durch einen Charakter χ^u. Damit erzeugen die Charaktere $\{\chi^u | u \in M \cap \Pi_h\}$ den Vektorraum $\Gamma(U_\sigma, O(D_h))$.

Nun bliebe noch zu zeigen, wie man die lokale Information der U_σ zu einen Gesamtbild auf V zusammensetzt. Das wird hier nicht durchgeführt.

Einen vollständigen Beweis findet man bei [3], Seite 66, Lemma oder [13], Seite 72, Lemma 2.3.

4.3.2. Bemerkung

$\Gamma(V, O_V(D_h))$ ist der Vektorraum der rationalen Funktionen auf V_Δ mit $\mathrm{div} f + D_h \geq 0$, also in der Terminologie von Abschnitt 2.2:

$$\Gamma(V, O_V(D_h)) = \mathcal{L}(D_h).$$

[1] siehe Seite 57, Bemerkung 3.5.3

4.3.3. Bemerkung

Für unsere Beispiele zu den Polytopen Π_1, Π_2 und Π_3 bedeutet das:
Beispiel 1:

$$D_h = aV(\tau_3) + 2aV(\tau_4)$$

$$\dim \Gamma(V, O_V(D_h) = (a+1)^2$$

Beispiel 2:

$$D_h = aV(\tau_3)$$

$$\dim \Gamma(V, O_V(D_h) = \frac{(a+1)(a+2)}{2}$$

Beispiel 3:

$$D_h = aV(\tau_3) + bV(\tau_4)$$

$$\dim \Gamma(V, O_V(D_h) = (a+1)(b+1)$$

Um die Parameter der Codes berechnen zu können, müssen wir die Schnittzahl $(D_h; V(\tau_i))$ des Cartier-Divisors D_h mit $V(\tau_i)$ für einen eindimensionalen Kegel τ_i bestimmen. Dazu verfahren wir wie in [13], Seite 80, Lemma 2.11 mit den anschließenden Beispielen:

τ_i ist der Schnitt von zwei zweidimensionalen Kegeln σ_{i-1} und σ_i, sei $n(\tau_i)$ ein primitives Element von τ_i. In den benachbarten eindimensionalen Kegeln τ_{i-1} und τ_{i+1} wählt man primitive Elemente $n_{i-1}, n_{i+1} \in N$. Da unsere Fächer verfeinert sind, bilden die Paare $(n_{i-1}, n(\tau_i))$ und $(n_{i+1}, n(\tau_i))$ $\mathbb{Z}$ -Basen von N. Daher gibt es eine ganze Zahl ν_i mit

$$n_{i-1} + n_{i+1} + \nu_i n(\tau_i) = 0, \quad \sigma_{i-1} = \mathbb{R}_{\geq 0} n_{i-1} + \tau, \quad \sigma_i = \mathbb{R}_{\geq 0} n_{i+1} + \tau.$$

Nach Abschnitt 3.6 ist h linear auf τ_i, sei $\lambda_{\tau_i} \in M$ mit $h(n) = (\lambda_{\tau_i} | n)$ für $n \in \tau_i$. Setze $\bar{h} = h - \lambda_{\tau_i}$. Für die Schnittzahl ergibt sich damit

$$(D_h; V(\tau_i)) = -(\bar{h}(n_{i-1}) + \bar{h}(n_{i+2})). \tag{2}$$

$V(\tau_i)$ ist selbst ein irreduzibler Cartierdivisor, und für seine Selbstschnittzahl folgt ebenfalls nach [13], Seite 80, Lemma 2.11

$$(V(\tau_i);V(\tau_i)) = \nu_i. \tag{3}$$

Um nun die Parameter der torischen Codes zu bestimmen, bemerkt man, dass diese durch Auswertung rationaler Funktionen auf V_Δ entstehen:

Sei $T = \overline{\mathbb{F}}_q^\times \times \overline{\mathbb{F}}_q^\times$. Für jedes $t \in T$ betrachten wir nun die Evaluationsabbildung E an der Stelle t:

$$\begin{array}{rcl} E : \Gamma(V, O_V(D_h)) & \to & \overline{\mathbb{F}}_q^\times \\ f & \mapsto & f(t) \end{array}$$

Um den Code $\mathcal{C}_\Pi$ als Bild der Evaluationsabbildung E zu erhalten, wertet man nur die über dem Grundkörper definierten Funktionen, also die Frobenius-invarianten Funktionen, auf dem algebraischen Torus $T(\mathbb{F}_q) = \mathbb{F}_q^\times \times \mathbb{F}_q^\times$ aus.

$$\begin{array}{rcl} \Gamma(V, O_V(D_h))^{\mathrm{Frob}} & \to & \mathcal{C}_\Pi \subset (\mathbb{F}_q^\times)^{(q-1)^2} \\ f & \mapsto & (f(t))_{t \in T(\mathbb{F}_q)} \end{array}$$

Die Erzeugenden des Codes (vgl. Abschnitt 4.1, Gleichung (1)) sind die Bilder der Basiselemente:

$$E : \chi^u \mapsto (\chi^u(t))_{t \in T(\mathbb{F}_q)}$$

Zeigt man nun, dass die Auswertungsabbildung injektiv ist, dann folgt mit Bemerkung 4.3.3 auf Seite 77, dass die Dimension der torischen Codes der in den Sätzen 4.2.1 bis 4.2.3 behaupteten entspricht.

Sei $u_1 = (1,0)$. Die rationalen Punkte von $T = \overline{\mathbb{F}}_q^\times \times \overline{\mathbb{F}}_q^\times$ liegen auf den $q-1$ Geraden in V_Δ, die durch $\displaystyle\prod_{\eta \in \mathbb{F}_q^\times} (\chi^{u_1} - \eta) = 0$ gegeben sind.

Sei $0 \neq f \in \Gamma(V, O_V(D_h))$ mit $f \equiv 0$ auf genau $l < q-1$ dieser Geraden.

Da χ^{u_1} und $\chi^{u_1} - \eta$ die gleichen Pole haben, sind ihre Nullstellendivisoren linear äquivalent:

$$(\mathrm{div}(\chi^{u_1} - \eta))_0 \sim (\mathrm{div}(\chi^{u_1}))_0$$

Daher gilt

$$\operatorname{div}(f) + D_h - l(\operatorname{div}(\chi^{u_1}))_0 \succeq 0,$$

oder gleichbedeutend

$$f \in \Gamma(V, O_V(D_h - l(\operatorname{div}(\chi^{u_1}))_0)).$$

Daraus folgt

$$f \cdot (\chi^{u_1})^l \in \Gamma(V, O_V(D_h)).$$

Nach Satz 4.3.1 bilden die $\{\chi^{u_i} | u_i \in M \cap \Pi_h\}$ eine Basis von $\Gamma(V, O_V(D_h))$, also gilt

$$f = \sum_{u_i \in M \cap \Pi_h} \mu_i \chi^{u_i}.$$

Multipliziert man nun f mit $(\chi^{u_1})^l$, so bleibt man in $\Gamma(V, O_V(D_h))$, also gilt

$$f \cdot (\chi^{u_1})^l = \sum_{u_i \in M \cap \Pi_h} \mu_i \chi^{u_i + l u_1} = \sum_{u_i \in M \cap \Pi_h} \kappa_i \chi^{u_i}.$$

Daher muss für die i mit $\mu_i \neq 0$ auch $u_i + l u_1$ noch in $M \cap \Pi_h$ liegen. Aus der Geometrie der Polytope Π_1, Π_2 und Π_3 folgt damit

$$l \leq a.$$

Auf den anderen $q - 1 - l$ Geraden ist die Anzahl der Nullstellen von f nach [7] beschränkt durch die Schnittzahl

$$(D_h - l(\operatorname{div}(\chi^{u_1}))_0; (\operatorname{div}(\chi^{u_1}))_0).$$

Das gewählte Element $u_1 \in M$ ist innere Normale für alle drei Polytope Π_1, Π_2 und Π_3, und daher gilt

$$\operatorname{div}(\chi^{u_1}) = V(\tau_i)$$

für ein geeignetes τ_i (das in unseren Beispielen jeweils τ_1 ist). An dieser Darstellung kann man direkt ablesen, dass der Divisor $\operatorname{div}(\chi^{u_1})$ keine Pole hat (der einzige nichtverschwindende Koeffizient ist positiv). Also gilt

$$\operatorname{div}(\chi^{u_1})_0 = \operatorname{div}(\chi^{u_1})$$

Für die gesuchte Schnittzahl gilt dann

$$\begin{aligned}(D_h - l(\operatorname{div}(\chi^{u_1}))_0; (\operatorname{div}(\chi^{u_1}))_0) &= (D_h - l\operatorname{div}(\chi^{u_1}); \operatorname{div}(\chi^{u_1}))\\ &= (D_h - lV(\tau_1); V(\tau_1))\\ &= (D_h; V(\tau_1)) \;-\; l \cdot (V(\tau_1); V(\tau_1))\end{aligned}$$

Diese Schnittzahlen kann man nun nach Gleichung (2) und (3) berechnen.

In allen Beispielen ist h auf τ gleich Null, also gilt für alle Beispiele $\bar{h} = h$.

Beispiel 1:

Sei $n(\tau_1) = (1, 0)$, $n_4 = (-1, -1)$, $n_2 = (-1, 1)$.

Es gilt $h(n_4) = -2a$ und $h(n_2) = 0$. Daher erhält man

$$(D_h; V(\tau_1)) = 2a.$$

Weiterhin gilt

$$\begin{pmatrix}-1\\-1\end{pmatrix} + \begin{pmatrix}-1\\1\end{pmatrix} + 2 \cdot \begin{pmatrix}1\\0\end{pmatrix} = 0,$$

also

$$(V(\tau_1); V(\tau_1)) = 2.$$

Zusammen ergibt sich $(D_h - lV(\tau_1); V(\tau_1)) = 2a - 2l$.

Beispiel 2:

Sei nun $n(\tau_1) = (1, 0)$, $n_3 = (-1, -1)$, $n_2 = (0, 1)$.

Es gilt $h(n_3) = -a$ und $h(n_2) = 0$. Daher erhält man

$$(D_h; V(\tau_1)) = a.$$

Weiterhin gilt

$$\begin{pmatrix}-1\\-1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} + 1 \cdot \begin{pmatrix}1\\0\end{pmatrix} = 0,$$

also

$$(V(\tau_1); V(\tau_1)) = 1.$$

und insgesamt $(D_h - lV(\tau_1); V(\tau_1)) = a - l$.

Beispiel 3:

Sei $n(\tau_1) = (1, 0)$, $n_4 = (0, -1)$, $n_2 = (0, 1)$.

Es gilt $h(n_4) = -b$ und $h(n_2) = 0$. Daher erhält man

$$(D_h; V(\tau_1)) = b.$$

Weiterhin gilt

$$\begin{pmatrix}0\\-1\end{pmatrix} + \begin{pmatrix}0\\1\end{pmatrix} + 0 \cdot \begin{pmatrix}1\\0\end{pmatrix} = 0,$$

also

$$(V(\tau_1); V(\tau_1)) = 0.$$

Zusammen ergibt sich $(D_h - lV(\tau_1); V(\tau_1)) = b$.

Zusammengefasst ergeben sich in den Beispielen 1-3 die Schnittzahlen $2a - 2l$, $a - l$ und b.

Berücksichtigt man $0 < l \leq a$, so läßt sich die Anzahl der rationalen Nullstellen der Funktion f in den drei Beispielen folgendermaßen abschätzen:

Beispiel 1:

$$l(q - 1) + (q - 1 - l)(2a - 2l) \leq (q - 1)2a < (q - 1)^2 \tag{4}$$

Beispiel 2:

$$l(q - 1) + (q - 1 - l)(a - l) \leq (q - 1)a < (q - 1)^2 \tag{5}$$

Beispiel 3:

$$l(q-1)+(q-1-l)b \leq (q-1)a+(q-1)b-ab < (q-1)^2 \tag{6}$$

Also hat nur die Nullfunktion $(q-1)^2$ Nullstellen, und damit ist die Auswertungsabbildung

$$\begin{array}{rcl} \Gamma(V, O_V(D_h))^{\mathrm{Frob}} & \to & \mathcal{C}_\Pi \subset (\mathbb{F}_q^\times)^{(q-1)^2} \\ f & \mapsto & (f(t))_{t\in T(\mathbb{F}_q)} \end{array}$$

injektiv und die Dimensionen der Codes $\mathcal{C}_{\Pi_i}$ entsprechen den in den Sätzen 4.2.1 bis 4.2.3 behaupteten.

Für die Minimaldistanz erhält man mit dieser Methode eine Abschätzung nach unten, die durch die Werte in den Sätzen 4.2.1 bis 4.2.3 gegeben ist, wie man aus den Ungleichungen (4) bis (6) ablesen kann.

Um die Gleichheit zu zeigen, reicht es aus, ein Element mit Hamming-Norm d anzugeben. Wir benutzen die gleichen Funktionen wie Hansen in [6].

Beispiel 1:

Gesucht ist ein Codewort mit Hamming-Norm $(q-1)^2 - 2a(q-1)$, also eine Funktion $f \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$, die in $2a(q-1)$ Punkten gleich Null ist.

Seien $s_1, \ldots, s_{2a} \in \mathbb{F}_q^*$ paarweise verschieden. Die Funktion

$$(y-s_1)\cdot\ldots\cdot(y-s_{2a}) \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$$

ist Null in genau den $2a(q-1)$ Punkten

$$(x, s_i), \quad x \in \mathbb{F}_q^\times, i = 1, \ldots, 2a,$$

erfüllt also die Bedingung.

Beispiel 2:

Gesucht ist ein Codewort mit Hamming-Norm $(q-1)^2 - a(q-1)$, also eine Funktion $f \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$, die in $(a+b)(q-1)$ Punkten gleich Null ist.

Seien $s_1, \ldots, s_a \in \mathbb{F}_q^*$ paarweise verschieden. Die Funktion

$$(y-s_1)\cdot\ldots\cdot(y-s_a) \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$$

ist Null in genau den $a(q-1)$ Punkten

$$(x, s_i), \quad x \in \mathbb{F}_q^\times, i = 1, \dots, a,$$

erfüllt also die Bedingung.

Beispiel 3:

Gesucht ist ein Codewort mit Hamming-Norm $(q-1-a)(q-1-b)$, also eine Funktion $f \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$, die in $(a+b)(q-1)-ab$ Punkten gleich Null ist.

Seien $s_1, \dots, s_a \in \mathbb{F}_q^*$ paarweise verschieden und $t_1, \dots, t_b \in \mathbb{F}_q^*$ paarweise verschieden. Die Funktion

$$(x-s_1) \cdot \ldots \cdot (x-s_a)(y-t_1) \cdot \ldots \cdot (y-t_b) \in \Gamma(V, O_V(D_h))^{\mathrm{Frob}}$$

ist Null in genau den $(a+b)(q-1)-ab$ Punkten

$$(s_i, y), (x, t_i), \quad x, y \in \mathbb{F}_q^\times, i = 1, \dots, a, i = 1, \dots, b,$$

erfüllt also die Bedingung.

4.4 Beziehung der Parameter torischer Codes zur Gilbert-Varshamov-Schranke

Die Parameter der speziellen torischen Codes aus Abschnitt 4.2 sollen in diesem Abschnitt mit der Gilbert-Varshamov-Schranke aus Abschnitt 1.2.1 in Beziehung gesetzt werden. Dazu werden systematisch für die ersten möglichen Werte von q die Parameter n, k und d nach den Sätzen aus Abschnitt 4.2 bestimmt. Zu q, n und d wird dann $A(n,d)$ (die Gilbert-Varshamov-Schranke für die Anzahl der Elemente des Codes) bestimmt.[2] Da die Hansen-Codes lineare Codes sind, ist die Anzahl der Elemente gegeben durch q^k. Um den Wert $A(n,d)$ mit k vergleichen zu können, ist in der Tabelle der Wert $\log_q(A(n,d))$ aufgeführt.

Die Parameterkombinationen, bei denen die Hansen-Codes die Gilbert-Varshamov-Schranke übertreffen, sind fett gedruckt.

Für jede der drei Klassen von Codes wurde die Zeile mit dem kleinsten möglichen q bereits in Abschnitt 4.1.1 als explizites Beispiel berechnet.

4.4.1 Der Hansen-Code zu Π_1

Π_1 ist das Polytop mit den Ecken $(0,0)$, (a,a) und $(0,2a)$. Ist $a < \frac{q-1}{2}$, dann hat der zu Π_1 gehörende Hansen-Code nach Abschnitt 4.2 die Parameter $n = (q-1)^2$, $k = (a+1)^2$ und $d = (q-1)^2 - 2a(q-1)$.

q	a	n	k	d	$\log_q A(n,d)$
2	-	-	-	-	-
3	-	-	-	-	-
4	1	9	4	3	4.77
5	1	16	4	8	4.05
7	**1**	**36**	**4**	**24**	**3.58**
7	2	36	9	12	15.45
8	**1**	**49**	**4**	**35**	**3.51**
8	2	49	9	21	15.34
8	3	49	16	7	35.46
9	**1**	**64**	**4**	**48**	**3.48**
9	2	64	9	32	15.48
9	3	64	16	16	34.90

[2] Zur Bestimmung der Gilbert-Varshamov-Schranke wurde das Computeralgebra-Programm Derive verwendet.

q	a	n	k	d	$\log_q A(n,d)$
11	**1**	**100**	**4**	**80**	**3.50**
11	2	100	9	60	16.10
11	3	100	16	40	35.68
11	4	100	25	20	62.42
13	**1**	**144**	**4**	**120**	**3.57**
13	2	144	9	96	16.94
13	3	144	16	72	37.33
13	4	144	25	48	64.02
13	5	144	36	24	97.99

Der Hansen-Code zu Π_1 ist also im Bereich von q zwischen 7 und 13 jeweils nur für $k = 4$ besser als die Gilbert-Varshamov-Schranke.

4.4.2 Der Hansen-Code zu Π_2

Π_2 ist das Polytop mit den Ecken $(0,0)$, $(a,0)$ und $(a,0)$. Ist $a < q-1$, dann hat der zu Π_2 gehörende Hansen-Code nach Abschnitt 4.2 die Parameter $n = (q-1)^2$, $k = \frac{(a+1)(a+2)}{2}$ und $d = (q-1)^2 - a(q-1)$.

q	a	n	k	d	$\log_q A(n,d)$
2	-	-	-	-	-
3	**1**	**4**	**3**	**2**	**2**
4	**1**	**9**	**3**	**6**	**1.30**
4	**2**	**9**	**6**	**3**	**4.77**
5	**1**	**16**	**3**	**12**	**0.99**
5	**2**	**16**	**6**	**8**	**4.05**
5	**3**	**16**	**10**	**4**	**9.45**
7	**1**	**36**	**3**	**30**	**0.72**
7	**2**	**36**	**6**	**24**	**3.58**
7	**3**	**36**	**10**	**18**	**8.51**
7	4	36	15	12	15.45
7	5	36	21	6	24.78
8	**1**	**49**	**3**	**42**	**0.64**
8	**2**	**49**	**6**	**35**	**3.51**
8	**3**	**49**	**10**	**28**	**8.48**
8	4	49	15	21	15.34
8	5	49	21	14	24.17
8	6	49	28	7	35.46

q	a	n	k	d	$\log_q A(n,d)$
9	**1**	**64**	**3**	**56**	**0.58**
9	**2**	**64**	**6**	**48**	**3.48**
9	**3**	**64**	**10**	**40**	**8.55**
9	4	64	15	32	15.48
9	5	64	21	24	24.21
9	6	64	28	16	34.90
9	7	64	36	8	48.15
11	**1**	**100**	**3**	**90**	**0.50**
11	**2**	**100**	**6**	**80**	**3.50**
11	**3**	**100**	**10**	**70**	**8.85**
11	4	100	15	60	16.10
11	5	100	21	50	25.06
11	6	100	28	40	35.68
11	7	100	36	30	48.04
11	8	100	45	20	62.42
11	9	100	55	10	79.56
13	**1**	**144**	**3**	**132**	**0.45**
13	**2**	**144**	**6**	**120**	**3.57**
13	**3**	**144**	**10**	**108**	**9.25**
13	4	144	15	96	16.94
13	5	144	21	84	26.34
13	6	144	28	72	37.33
13	7	144	36	60	49.88
13	8	144	45	48	64.02
13	9	144	55	36	79.95
13	10	144	66	24	97.99
13	11	144	78	12	119.00

Der Hansen-Code zu Π_2 ist also im untersuchten Bereich von $q \leq 13$ für $k \leq 10$ besser als die Gilbert-Varshamov-Schranke.

4.4.3 Der Hansen-Code zu Π_3

Π_3 ist das Polytop mit den Ecken $(0,0)$, $(a,0)$, (a,b) und $(0,b)$. Gilt $a < q-1$ und $b < q-1$, dann hat der zu Π_3 gehörende Hansen-Code nach Abschnitt 4.2 die Parameter $n = (q-1)^2$, $k = (a+1)(b+1)$ und $d = (q-1)^2 - a(q-1) - b(q-1) + ab$.

Da der Code zum Parameterpaar (a,b) gleich dem zum Paar (b,a) ist, kann ohne Einschränkung $a \geq b$ angenommen werden.

q	a	b	n	k	d	$\log_q A(n,d)$
2	-	-	-	-	-	-
3	**1**	**1**	**4**	**4**	**1**	**4.00**
4	**1**	**1**	**9**	**4**	**4**	**3.32**
4	2	1	9	6	2	6.60
4	**2**	**2**	**9**	**9**	**1**	**9.00**
5	**1**	**1**	**16**	**4**	**9**	**3.08**
5	2	1	16	6	6	6.42
5	2	2	16	9	4	9.45
5	3	1	16	8	3	11.28
5	3	2	16	12	2	13.41
5	**3**	**3**	**16**	**16**	**1**	**16.00**
7	**1**	**1**	**36**	**4**	**25**	**2.96**
7	2	1	36	6	20	6.65
7	2	2	36	9	16	10.60
7	3	1	36	8	15	11.72
7	3	2	36	12	12	15.45
7	3	3	36	16	9	19.76
7	4	1	36	10	10	18.25
7	4	2	36	15	8	21.34
7	4	3	36	20	6	24.78
7	4	4	36	25	4	28.67
7	5	1	36	12	5	26.66
7	5	2	36	18	4	28.67
7	5	3	36	24	3	30.84
7	5	4	36	30	2	33.24
7	**5**	**5**	**36**	**36**	**1**	**36.00**

q	a	b	n	k	d	$\log_q A(n,d)$
9	**1**	**1**	**64**	**4**	**49**	**2.99**
9	2	1	64	6	42	7.10
9	2	2	64	9	36	11.79
9	3	1	64	8	35	12.67
9	3	2	64	12	30	17.49
9	3	3	64	16	25	23.02
9	4	1	64	10	28	19.62
9	4	2	64	15	24	24.21
9	4	3	64	20	20	29.29
9	4	4	64	25	16	34.90
9	5	1	64	12	21	27.97
9	5	2	64	18	18	32.03
9	5	3	64	24	15	36.40
9	5	4	64	30	12	41.14
9	5	5	64	36	9	46.31
9	6	1	64	14	14	37.93
9	6	2	64	21	12	41.14
9	6	3	64	28	10	44.53
9	6	4	64	35	8	48.15
9	6	5	64	42	6	52.05
9	6	6	64	49	4	56.32
9	7	1	64	16	7	50.06
9	7	2	64	24	6	52.05
9	7	3	64	32	5	54.13
9	7	4	64	40	4	56.32
9	7	5	64	48	3	58.64
9	7	6	64	56	2	61.16
9	**7**	**7**	**64**	**64**	**1**	**64.00**

Der Hansen-Code zu Π_3 ist also im betrachteten Bereich von $q \leq 9$ jeweils nur für $k = 4$ und für $k = n$ mindestens so gut wie die Gilbert-Varshamov-Schranke.

Symbolverzeichnis

Neben den benutzten Standardbezeichnungen werden hier auch einige Symbole aufgeführt, die in der gesamten Arbeit einheitlich verwendet werden.

$\mathcal{C}$	ein Code
$\mathcal{C}_\Pi$	der Code zum Polytop Π
$\mathbb{C}$	die komplexen Zahlen
$\mathbb{C}^*$	die komplexen Zahlen ungleich Null
$\mathbb{C}^\times$	die multiplikative Gruppe der komplexen Zahlen
$d_h(x, y)$	die Hamming-Distanz von x und y
Δ	ein Fächer
$\mathbb{F}_p$	der endliche Körper mit p Elementen für eine Primzahl p
$\mathbb{F}_q$	der endliche Körper mit q Elementen für eine Primzahlpotenz $q = p^r$
$\mathrm{Hom}_{\mathrm{alg}}$	Algebrenhomomorphismen
$\mathrm{Hom}_{\mathrm{hg}}$	Halbgruppenhomomorphismen
$\mathbb{F}_q^\times$	die multiplikative Gruppe von $\mathbb{F}_q$
$[n, k, d]$-Code	linearer Code mit Länge n, Dimension k und Minimaldistanz d
Π	ein Polytop
σ	ein Kegel

Literaturverzeichnis

[1] COX, DAVID A.: *Tutorial on Toric Varieties.* Workshop on Algebraic Geometry and Geometric Modelling, 2002.

[2] DUMMIT, DAVID S. UND FOOTE, RICHARD M.: *Abstract Algebra.* Zweite Auflage, Prentice Hall, 1999.

[3] FULTON, WILLIAM: *Introduction to Toric Varieties.* Princeton University Press, 1993.

[4] GUNNING, R. C.: *Lectures on Riemann Surfaces.* Princeton University Press, 1966.

[5] HANSEN, JOHAN P.: *Toric Surfaces and Error-correcting Codes.* In J. Buchmann et al, eds.: Coding Theory, Crytography and Related Areas, Springer, 2002.

[6] HANSEN, JOHAN P.: *Toric Varieties, Hirzebruch Surfaces and Error-Correcting Codes.* Applicable Algebra in Engineering, Communication and Computing 13, 2002.

[7] HANSEN, SØREN HAVE: *Error-Correcting Codes from higher dimensional varieties.* Preprint Series No. 4, University of Aarhus, 1998.

[8] HIRZEBRUCH, FRIEDRICH: *Codierungstheorie und ihre Beziehung zu Geometrie und Zahlentheorie.* Rheinisch-Westfälische Akademie der Wissenschaften, Vorträge N 370. Westdeutscher Verlag, 1989.

[9] JOYNER, DAVID: *Toric Codes over Finite Fields.* Preprint, 2002.

[10] KAUP, LUDGER: *Vorlesungen über Torische Varietäten.* Konstanzer Schriften in Mathematik und Informatik, Nr. 130, 2001.

[11] LINT, JACOBUS HENDRICUS VAN: *Introduction to Coding Theory.* Dritte Auflage, Springer, 1999.

[12] LÜTKEBOHMERT, WERNER: *Codierungstheorie.* Vieweg, 2003.

[13] ODA, TADAO: *Convex Bodies and Algebraic Geometry.* Springer, 1985.

[14] SILVERMAN, J.H. : *The Arithmetic of Elliptic Curves.* Dritte Auflage, Springer, 1992.

[15] TSFASMAN, M.A., VLADUT, S.G. UND ZINK, T.: *On Goppa Codes which are better than the Varshamov-Gilbert bound.* Math. Nach., 109, pp. 34-38, 1987.

[16] WALKER, JUDY: *Codes and Curves.* Student Mathematica Library, 2000.