Fachbereich 03 – Mathematik Universität Bremen

Diplomarbeit

Codierung mittels Algebraischer Geometrie

vorgelegt von
Arne Grenzebach

Dezember 2008

Gutachter:
Prof. Dr. Jens Gamst
Prof. Dr. Eberhard Oeljeklaus

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungsverzeichnis

MDS	maximum distance separable code
RM	Reed-Muller-Code
GRM	Verallgemeinerter Reed-Muller-Code
RS	Reed-Solomon-Code
GRS	Verallgemeinerter Reed-Solomon-Code

Einleitung

In dieser Arbeit untersuchen wir Eigenschaften von Codes mit Mitteln der Algebraischen Geometrie. Unser Ziel ist es, eine untere Schranke für den Minimalabstand von bestimmten algebraisch geometrischen Codes – sogenannten Auswerte-Codes – anzugeben. Der Name rührt daher, daß man die Codewörter eines solchen Codes $C(\Gamma)_a$ erhält, indem homogene Polynome vom Grad a an allen Punkten einer endlichen Punktmenge $\Gamma \subset \mathbb{P}^m$ ausgewertet werden.

Wir folgen hier den Ausführungen im Artikel „Cayley–Bacharach and Evaluation Codes on Complete Intersections“ von Gold, Little und Schenck (2005). Entscheidendes Hilfsmittel ist eine moderne Formulierung des Satzes von Cayley-Bacharach in der Sprache der Schemata. Der Satz ist nach A. Cayley und I. Bacharach benannt, die sich im 19. Jahrhundert mit Schnitten von Kurven in der projektiven Ebene $\mathbb{P}^2$ beschäftigten. Die Wurzeln dieses Satzes reichen zurück bis Pappus von Alexandria, der im 4. Jahrhundert nach Christus eine erste Version bewies. Einen Überblick über verschiedene Varianten findet man im Artikel „Cayley-Bacharach Theorems and Conjectures“ von Eisenbud, Green und Harris (1996).

In den angesprochenen Versionen des Satzes ist die Punktmenge Γ ein vollständiger Durchschnitt von Hyperflächen. Wesentlich ist nun, daß Γ in gewissen Fällen keine unabhängigen Bedingungen auf Hyperflächen vom Grad a liefern kann. Gerade diese Tatsache hat Einfluß auf den Minimalabstand und erlaubt so eine Fehlerkorrektur.

Um eine untere Schranke für den Minimalabstand d von Auswerte-Codes $C(\Gamma)_a$ zu gewinnen, benutzen wir die Hilbertfunktion und den Satz von Cayley-Bacharach; Γ ist dabei ein reduzierter vollständiger Durchschnitt von Hyperflächen H_i vom Grad d_i im projektiven Raum $\mathbb{P}^m$. Unser Hauptresultat ist folgende Abschätzung:

$$C(\Gamma)_a \text{ hat Minimalabstand } d \geq s - a + 2, \text{ falls } 1 \leq a \leq s = \sum d_i - m - 1.$$

In dem dieser Arbeit zugrunde liegenden Artikel von Gold u. a. (2005) wird der Artikel „Linkage and Codes on Complete Intersections“ von Hansen (2003) verallgemeinert. Dort wird, ohne den Satz von Cayley-Bacharach anzuwenden, eine ähnliche Schranke für Auswerte-Codes im $\mathbb{P}^2$ hergeleitet.

Gliederung der Arbeit: Wir legen in Kapitel 1 einige Bezeichnungen fest, die wir im Laufe der Arbeit immer wieder verwenden werden. Außerdem erinnern wir kurz an den projektiven Raum, an graduierte Ringe und an die Lokalisation von Moduln („Bruchrechnung“).

Grundbegriffe der Codierungstheorie erläutern wir in Kapitel 2. Hier führen wir die Auswerte-Codes ein und behandeln dann Reed-Muller-Codes, Reed-Solomon-Codes und geometrische Goppa-Codes.

Das Kapitel 3 ist der projektiven Algebraischen Geometrie gewidmet; dabei betrachten wir insbesondere nulldimensionale Schemata und den Satz von Cayley-Bacharach.

Die vorgestellten Mittel der Algebraischen Geometrie benutzen wir im letzten Teil der Arbeit (Kapitel 4), um unser Hauptresultat zu gewinnen, also um Minimalabstände von Auswerte-Codes abzuschätzen, die durch einen nulldimensionalen reduzierten vollständigen Durchschnitt Γ gegeben sind.

Wir setzen gute Kenntnisse in Algebra voraus; zum Beispiel sollten der Hilbertsche Basissatz und der Hilbertsche Nullstellensatz bekannt sein, die wir ohne Referenz benutzen werden. Außerdem werden Grundkenntnisse über Schemata benötigt. Aus Platzgründen können wir den Satz von Cayley-Bacharach hier nicht beweisen, da dazu Aussagen über Gorensteinringe aus der Kommutativen Algebra benutzt werden.

Definitionen und Beispiele numerieren wir kapitelweise, getrennt von Sätzen, Lemmata, Korollaren und Notizen durch. Im Anhang verwenden wir für die Numerierung Buchstaben anstelle von Zahlen. Wir kennzeichnen das Beweisende mit dem Symbol ■ und das Ende einer Notiz bzw. eines Beispiels mit $\Diamond$.

Danksagung: Herrn Prof. Dr. Jens Gamst danke ich für die interessante Aufgabenstellung sowie für die freundliche und kompetente Betreuung meiner Diplomarbeit. Herrn Prof. Dr. Eberhard Oeljeklaus danke ich für seine Bereitschaft, das Zweitgutachten zu erstellen, und für viele hilfreiche Gespräche und konstruktive Verbesserungsvorschläge.

Ich danke meinen Brüdern Gerrit und Claas Grenzebach, die beide viel zum Gelingen dieser Arbeit beigetragen haben. Claas hat meine komplette Arbeit gelesen und diverse Verbesserungen angeregt. Mit Gerrit habe ich viele fruchtbare Diskussionen geführt.

Bei meinen Eltern möchte ich mich dafür bedanken, daß sie mir mein Studium finanziert und mich in jeder Hinsicht unterstützt haben.

1. Präliminarien

Vorab legen wir einige Bezeichnungen fest, die im folgenden immer wieder verwendet werden. Außerdem erinnern wir kurz an den projektiven Raum (vgl. Beutelspacher u. Rosenbaum, 2004; Fulton, 1969; Silvermann u. Tate, 1992), an graduierte Ringe (vgl. Matsumura, 1980, Kap. 4, § 10) sowie an die Lokalisation von Moduln (vgl. Kunz, 1997, Anhang B).

- $^{\#}\Gamma$ bezeichne die Anzahl der Elemente einer endlichen Menge Γ. Für einen Vektorraum V sei $V^* = V \setminus \{0\}$.

- Wir arbeiten bei Problemen der Codierungstheorie über einem endlichen Körper $\mathbb{F}_q$ mit q Elementen (q Primzahlpotenz).

  Ansonsten ist ein beliebiger Körper K unser Grundkörper. K^m ist der m-dimensionale Vektorraum der m-Tupel $(a_1, \ldots, a_m)$ mit $a_i \in K$, welcher auch *m-dimensionaler affiner Raum* über K genannt und mit $\mathbb{A}_K^m = \mathbb{A}^m(K) = \mathbb{A}^m$ bezeichnet wird.

- Mit $\mathbb{P}_K^m = \mathbb{P}^m(K) = \mathbb{P}^m$ wird der *m-dimensionale projektive Raum* über K bezeichnet, also der Raum aller Ursprungsgeraden im K^{m+1}:

  $$\mathbb{P}^m = \left(K^{m+1}\right)^* \Big/ \sim \quad \text{mit } x \sim y :\Leftrightarrow \exists\, \lambda \in K^* \colon y = \lambda \cdot x.$$

  Die Äquivalenzklassen schreibt man als $p = (p_0 : \ldots : p_m)$ und nennt dies die *homogenen Koordinaten* von $p \in \mathbb{P}^m$.

  Identifiziert man die Punkte $(a_1, \ldots, a_m) \in \mathbb{A}^m$ und $(1 : a_1 : \ldots : a_m) \in \mathbb{P}^m$ miteinander, so findet man den $\mathbb{A}^m$ im $\mathbb{P}^m$ wieder. Die restlichen Elemente des $\mathbb{P}^m$ sind Punkte mit homogenen Koordinaten $(0 : p_1 : \ldots : p_m)$, d. h.

  $$\mathbb{P}^m \cong \mathbb{A}^m \dot\cup \mathbb{P}^{m-1}.$$

  Bezüglich dieser Einbettung werden die Punkte des $\mathbb{P}^{m-1}$ *unendlich ferne Punkte* genannt, weil sie als Schnittpunkte von parallelen Geraden im $\mathbb{A}^m$ interpretiert werden können. Insofern stellt der $\mathbb{P}^m$ eine Vervollständigung des $\mathbb{A}^m$ dar.

- Unter einem Ring verstehen wir stets einen kommutativen Ring mit Einselement.

  Ein *graduierter Ring* ist ein Ring S mit einer Zerlegung in eine direkte Summe $S = \bigoplus_{a \in \mathbb{N}} S_a$ abelscher Gruppen S_a, wobei für $a, b \in \mathbb{N}$ gilt: $S_a \cdot S_b \subset S_{a+b}$. Die Elemente von S_a heißen *homogen* vom Grad a.

Ein *graduierter Modul* M ist ein S-Modul mit einer Zerlegung in eine direkte Summe $M = \bigoplus_{a\in\mathbb{N}} M_a$, wobei für $a, b \in \mathbb{N}$ gilt: $S_a \cdot M_b \subset M_{a+b}$.

- Sei S ein graduierter Ring. Ein Ideal $\mathfrak{a} \subset S$ nennt man *homogen*, falls gilt: $\mathfrak{a} = \bigoplus_{a\in\mathbb{N}}(\mathfrak{a} \cap S_a) =: \bigoplus_{a\in\mathbb{N}} \mathfrak{a}_a$, mit anderen Worten, falls für jedes Element $f = \sum f_a \in \mathfrak{a}$ auch alle homogenen Komponenten f_a in $\mathfrak{a}$ liegen. Dies ist genau dann der Fall, wenn $\mathfrak{a}$ von homogenen Elementen erzeugt wird. Ferner sind Summen, Produkte, Schnitte und Radikale von homogenen Idealen selbst homogen.

  Um zu testen, ob ein homogenes Ideal $\mathfrak{a}$ ein Primideal ist, genügt es, für zwei homogene Elemente f, g zu zeigen, daß aus $f \cdot g \in \mathfrak{a}$ stets $f \in \mathfrak{a}$ oder $g \in \mathfrak{a}$ folgt.

- Bekannte Beispiele für graduierte Ringe sind Polynomringe über einem Körper K. Passend zum $\mathbb{P}^m$ betrachten wir Polynome in $m+1$ Unbestimmten:

$$R := K[X_0, \ldots, X_m] = \bigoplus_{a\in\mathbb{N}} R_a.$$

  Die homogenen Komponenten R_a enthalten hier die homogenen Polynome vom Grad a und das Nullpolynom; sie sind außerdem endlichdimensionale K-Vektorräume. Das homogene Ideal

$$R_+ := \bigoplus_{\substack{a\in\mathbb{N}\\ a>0}} R_a$$

  heißt *irrelevantes Ideal* (vgl. Hartshorne, 1977, S. 11).

  Weitere Beispiele für graduierte Ringe sind Quotienten von graduierten Ringen nach homogenen Idealen. Im Falle eines homogenen Ideals $I = \bigoplus_{a\in\mathbb{N}} I_a$ des Polynomringes R hat man offenbar:

$$R/I = \bigoplus_{a\in\mathbb{N}} R_a/I_a.$$

  Man setzt daher: $\left(R/I\right)_a := R_a/I_a$.

- Auf dem affinen Raum kann man Polynome als Funktionen auffassen, denn man kann ein Polynom $f \in R$ an allen Stellen $x \in \mathbb{A}^{m+1}$ auswerten.

  Die Punkte des projektiven Raumes $\mathbb{P}^m$ sind wie beschrieben als Äquivalenzklassen gegeben. Funktionen auf dem $\mathbb{P}^m$ müssen daher für alle Repräsentanten einer Äquivalenzklasse denselben Wert liefern, um wohldefiniert

zu sein: $f(\lambda \cdot x) = f(x)$ für alle $\lambda \in K^*$. Dies erfüllen Quotienten von homogenen Polynomen gleichen Grades, denn für $f, g \in R_a$ mit $g \neq 0$ hat man:

$$\frac{f}{g}(\lambda x) = \frac{f(\lambda x)}{g(\lambda x)} = \frac{\lambda^a f(x)}{\lambda^a g(x)} = \frac{f(x)}{g(x)}.$$

Darüber hinaus ist es sinnvoll, von Nullstellen von homogenen Polynomen zu reden. Ist nämlich $f(x) = 0$ für ein $f \in R_a$ und einen Repräsentanten x, so folgt für alle $\lambda \in K^*$:

$$f(\lambda x) = \lambda^a f(x) = 0.$$

Im allgemeinen setzen wir für $f \in R$:

$$f(x) = 0 :\Leftrightarrow f_a(x) = 0 \text{ für alle homogenen Komponenten } f_a \text{ von } f.$$

- Mit Γ wollen wir stets eine Menge $\{p_1, \ldots, p_n\}$ von n verschiedenen Punkten im $\mathbb{P}^m$ bezeichnen. Der Menge Γ ordnen wir das (homogene) *Verschwindungsideal* I_Γ zu:

$$\begin{aligned} I_\Gamma &:= \big\langle \{f \in R \mid f \text{ homogen}, \forall\, p \in \Gamma \colon f(p) = 0\} \big\rangle \\ &= \{f \in R \mid \forall\, p \in \Gamma \colon f(p) = 0\}. \end{aligned}$$

  Zum Beispiel wird das Verschwindungsideal zu $\Gamma = \mathbb{A}^m_{\mathbb{F}_q}$ (mit $n = {}^{\#}\Gamma = q^m$ Punkten) von den homogenen Polynomen $X_0^{q-1}X_j - X_j^q$ erzeugt:

$$I_{\mathbb{A}^m} = \big\langle X_0^{q-1}X_1 - X_1^q, \ldots, X_0^{q-1}X_m - X_m^q \big\rangle.$$

- Sei A ein Ring, M ein A-Modul und $T \subset A \setminus \{0\}$ eine multiplikativ abgeschlossene Teilmenge von A. Die *Lokalisation* M_T von M bezüglich T ist die Menge der *Brüche* $\frac{v}{t}$ mit *Zähler* $v \in M$ und *Nenner* $t \in T$:

$$M_T := \left\{ \frac{v}{t} \;\middle|\; v \in M, t \in T \right\}.$$

  Ein Bruch $\frac{v}{t}$ ist dabei eine Äquivalenzklasse zu folgender Äquivalenzrelation auf $M \times T$: $(v,t) \sim (v',t') :\Leftrightarrow \exists\, s \in T \colon s(t'v - tv') = 0$. M_T ist ein A-Modul mit den üblichen Bruchrechnungsregeln. Für $M = A$ ist A_T sogar ein Ring.

  Im Falle eines graduierten Moduls M über einem graduierten Ring S kann man auch die *homogene Lokalisation* bezüglich einer Nennermenge $T \subset S$ aus homogenen Elementen betrachten:

$$M_{(T)} := \left\{ \frac{v}{t} \;\middle|\; v \in M \text{ und } t \in T \text{ homogen vom gleichen Grad} \right\}.$$

Speziell für ein nicht nilpotentes $f \in A$ bzw. für ein Primideal $\mathfrak{p} \subset A$ sei:

$$A_f := A_T \text{ zu } T := \{1, f, f^2, \ldots\}, \qquad A_\mathfrak{p} := A_T \text{ zu } T := A \setminus \mathfrak{p}.$$

Entsprechend führen wir für ein homogenes, nicht nilpotentes $f \in S$ bzw. für ein homogenes Primideal $\mathfrak{p} \subset S$ folgende Bezeichner ein:

$$S_{(f)} := S_{(T)} \text{ zu } T := \{1, f, f^2, \ldots\}, \qquad S_{(\mathfrak{p})} := S_{(T)} \text{ zu } T := S \setminus \mathfrak{p}.$$

In einem Integritätsring ist $\langle 0 \rangle$ ein Primideal. Ist A ein solcher, so liefert die Lokalisation $A_{\langle 0 \rangle}$ von A nach $\langle 0 \rangle$ nichts anderes als den Quotientenkörper von A. Der Quotientenkörper des Polynomringes $K[X]$ ist echt größer als der Grundkörper K; hier gilt: $K = (K[X])_{(\langle 0 \rangle)}$.

2. Codierungstheorie

In der Codierungstheorie werden Problemstellungen aus der Nachrichtenverarbeitung mit Methoden der Informatik, Stochastik und insbesondere der abstrakten Algebra bearbeitet. Eine schematische Darstellung der Nachrichtenübertragung zeigt Abbildung 1: Von einer Quelle (Telefon, Computer, CD, Raumsonde) soll eine Nachricht (irgendwelche Informationen) über einen Kanal (Telefon- oder Glasfaserkabel, Funkverbindung) an einen Empfänger übermittelt werden. Dazu muß die Nachricht allerdings erst mit den Zeichen dargestellt werden, die durch den Kanal gesendet werden können. Diesen Prozeß nennt man *Codierung*, die Menge der möglichen Zeichen heißt *Alphabet*. Der Empfänger erhält die übermittelte Nachricht und muß die Codierung rückgängig machen. Die *decodierte* Nachricht muß aber nicht mehr mit der ursprünglich gesendeten Nachricht übereinstimmen, da während der Übertragung Störungen Fehler verursachen können. Wird z. B. das Alphabet $\{0, 1\}$ verwendet, so könnte etwa statt einer 0 auch eine 1 empfangen werden.

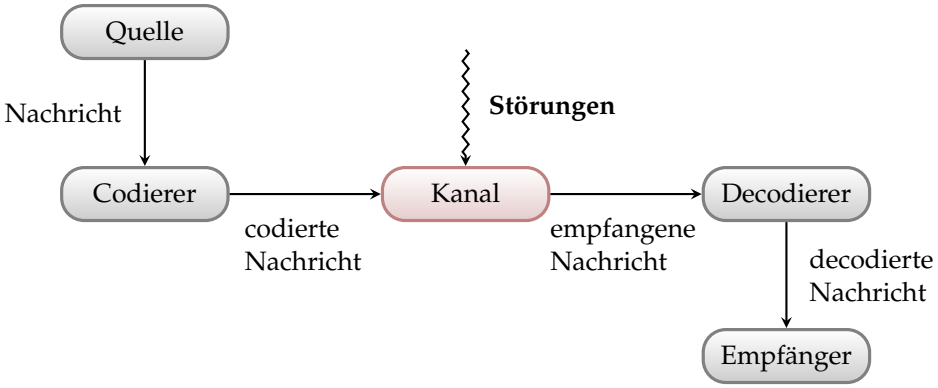


Abbildung 1: Schematische Darstellung der Nachrichtenübertragung

Die Aufgabe der Codierungstheorie ist nun, die Codierung so zu gestalten, daß Übertragungsfehler erkannt und korrigiert werden können. Dazu werden einer Nachricht bei der Codierung zusätzliche redundante Informationen hinzugefügt, die es dem Decodierer bei einer fehlerhaft übermittelten Nachricht erlauben, auf die ursprünglich gesendete zurückzuschließen. Die Existenz von derartigen Codes, mit denen eine im wesentlichen fehlerfreie[†] Kommunikation auch über einen gestörten Kanal möglich ist, garantiert das Theorem von Shannon.

[†] „Im wesentlichen fehlerfrei“ bedeutet hier, daß die Wahrscheinlichkeit, daß trotz Korrektur Fehler verbleiben, durch Wahl eines geeigneten Codes theoretisch beliebig klein wird.

Das genannte Theorem bewies Claude Elwood Shannon 1948 in seinem Artikel „Mathematical Theory of Communication“ (Shannon, 1948), welcher den Beginn der Codierungstheorie markiert. Der Artikel ist erschienen zu einer Zeit, in der die ersten Computer entwickelt wurden. Um auf einem Computer Rechungen ausführen zu können, müssen Daten übermittelt werden. Nun waren die ersten Computer nur in der Lage, Fehler zu erkennen; sie konnten diese aber nicht korrigieren, weshalb Rechnungen bei Auftreten eines Übertragungsfehlers abgebrochen werden mußten. Mit dem Wissen, daß es gute Codes hinsichtlich der Fehlerkorrektur gibt, versuchten die Wissenschaftler damals, auch solche zu konstruieren. Einer dieser Wissenschaftler war Richard W. Hamming, der die sogenannten *Hamming-Codes* erfand und 1950 im Artikel „Error Detection and Error Correction Codes“ publizierte (Hamming, 1950). Die Hamming-Codes können alle Übertragungsfehler korrigieren, wenn in jedem empfangenen Wort höchstens ein Fehler vorkommt.

Im restlichen Teil dieser Arbeit werden wir uns nicht mehr mit der Informationstheorie beschäftigen. Wer dennoch mehr wissen möchte, findet eine ausführliche Behandlung des Shannonschen Theorems bei van Lint (1999) im Kapitel 2 oder auch bei Lütkebohmert (2003). Die Ursprünge dieses Theorems sind im Artikel von Lüke (1999) dargelegt. Interessant ist auch die Einleitung des bereits erwähnten Artikels von Hamming (Hamming, 1950), da Hamming hier den Entwicklungsstand der ersten Computer und den Unterschied zu Rechenanlagen der damaligen Telefonzentren beschreibt.

Im folgenden Abschnitt führen wir die für diese Arbeit benötigten Grundbegriffe der Codierungstheorie ein und stellen die Reed-Muller-, die Reed-Solomon- sowie die geometrischen Goppa-Codes vor.

2.1. Grundbegriffe der Codierungstheorie

Definition 2.1: *Für $a = (a_1, \ldots, a_n)$ und $b = (b_1, \ldots, b_n)$ aus $\mathbb{F}_q^n$ sei*

$$d(a, b) := {}^{\#}\{i \mid a_i \neq b_i\}.$$

*Die hierdurch gegebene Abbildung d heißt **Hammingabstand** auf $\mathbb{F}_q^n$. Das **Gewicht** von einem Element $a \in \mathbb{F}_q^n$ ist der Abstand von a zur 0:*

$$d(a, 0) := {}^{\#}\{i \mid a_i \neq 0\}.$$

Wie man leicht nachrechnet, ist der Hammingabstand d eine Metrik auf $\mathbb{F}_q^n$.

Definition 2.2: *Ein* ***Code***[†] *C (über dem Alphabet $\mathbb{F}_q$) ist ein linearer Unterraum des $\mathbb{F}_q^n$, dessen Elemente als* ***Codewörter*** *bezeichnet werden. Wir nennen n die* ***(Wort-)Länge*** *und $\dim_{\mathbb{F}_q} C$ die* ***Dimension*** *von C. Ein* ***$[n,k]$-Code*** *ist ein Code der Länge n und der Dimension k. Unter dem* ***Minimalabstand*** *$d(C)$ eines Codes C verstehen wir die Größe*

$$\begin{aligned} d(C) &:= \min\{d(a,b) \mid a,b \in C \text{ und } a \neq b\} \\ &= \min\{d(c,0) \mid 0 \neq c \in C\}. \end{aligned}$$

Dementsprechend ist ein ***$[n,k,d]$-Code*** *ein $[n,k]$-Code mit Minimalabstand d.*

Ein $[n,k]$-Code C über $\mathbb{F}_q$ besitzt als k-dimensionaler $\mathbb{F}_q$-Vektorraum q^k Codewörter. Mit einem solchen Code können also höchstens q^k verschiedene Wörter codiert werden; die Codierung ist dabei eine geschickte Zuordnung (mittels einer injektiven linearen Abbildung) der Wörter (in $\mathbb{F}_q^k$), aus denen eine Nachricht zusammengesetzt ist, zu den Codewörtern (in $C \subset \mathbb{F}_q^n$).

Eine zu sendende Nachricht können wir uns jetzt als Folge von Codewörtern vorstellen, während die empfangenen Wörter beliebige Elemente des $\mathbb{F}_q^n$ sein können. Da jetzt aber pro übertragenem Wort nicht die k Stellen der ursprünglichen Wörter der Nachricht übermittelt werden, sondern die n Stellen der Codewörter, liegt die *Informationsrate* bei k/n. Maximal wird die Informationsrate natürlich für $k = n$. Dann sind aber alle Wörter des $\mathbb{F}_q^n$ Codewörter, so daß Übertragungsfehler nicht erkannt und erst recht nicht korrigiert werden können. Eine Korrektur kann nur für $n > k$ erfolgen und wird gerade durch die zusätzlichen, redundanten Stellen ermöglicht. Man nennt daher $n - k$ die *Redundanz* des Codes.

Zur Korrektur verwendet man die *Nächste-Nachbarn-Decodierung*. Nächste Nachbarn bestimmen sich dabei über den Hammingabstand, denn dieser zählt, an wie vielen Stellen sich zwei Wörter unterscheiden. Bei der Decodierung wollen wir einem empfangenen Wort w natürlich das Codewort zuordnen, das w am „ähnlichsten“ ist. Gibt es nur ein Codewort v mit geringstem Hammingabstand zu w, so nutzen wir v zur Korrektur von w und erhalten damit eine eindeutige Decodierung. Ein empfangenes Codewort wird auf diese Weise sich selbst zugeordnet. Gibt es keinen (eindeutig bestimmten) nächsten Nachbarn, so ist eine korrigierende Decodierung nicht möglich.

Offenbar hat man dann die beste Chance, Fehler zu korrigieren, wenn die Codewörter untereinander einen möglichst großen Hammingabstand besitzen. Ein guter Code führt daher zu einer möglichst gleichmäßigen Verteilung der Codewörter

[†] Allgemeiner wird auch eine nichtleere Teilmenge $C \subset A^n$ als **Code** bezeichnet, wobei $A \neq \emptyset$ eine beliebige endliche Menge ist. Da dann alle Codewörter die gleiche Länge n haben, ist C ein **Blockcode** der **Blocklänge** n. Falls $A = \mathbb{F}_q$ und $C \subset \mathbb{F}_q^n$ ein linearer Unterraum ist, heißt C **linearer Code**. In dieser Arbeit beschränken wir uns auf lineare Codes.

auf den $\mathbb{F}_q^n$. Besonders schlecht ist es also, jedes Wort einer Nachricht durch Hinzufügen von $n-k$ Nullen zu einem Codewort zu machen.

Ist eine Nächste-Nachbarn-Decodierung möglich, so werden die Übertragungsfehler berichtigt. Wie der folgende Satz zeigt, ist die Anzahl der korrigierbaren Fehler mit dem Minimalabstand des Codes verknüpft:

Satz 2.1: *Sei C ein $[n,k,d]$-Code. Treten bei der Übertragung eines Codewortes höchstens $\lfloor (d-1)/2 \rfloor$ Fehler auf,*[†] *so lassen sich diese korrigieren. Eine reine Fehlererkennung ist bis zu $d-1$ aufgetretenen Fehlern möglich.*

Beweis: Treten s Fehler bei der Übertragung eines Codewortes v auf, so unterscheidet sich das empfangene Wort w von v an s Stellen, d. h. $d(v,w) = s$. Da der Minimalabstand des Codes d ist, kann w für $1 \leq s \leq d-1$ kein Codewort sein und wird somit als Fehler erkannt.

Sei nun $s = d(v,w) \leq t := \lfloor (d-1)/2 \rfloor$. Für ein von v verschiedenes Codewort u gilt dann: $d(u,w) \geq |d(u,v) - d(v,w)| \geq d - t \geq t+1$. Folglich ist v das nächste Codewort zu w, so daß die Nächste-Nachbarn-Decodierung die Fehler korrigiert. Mit anderen Worten: Das empfangene Wort w kann dann eindeutig einem Codewort zugeordnet werden (was der Fehlerkorrektur entspricht), wenn sich die um die Codewörter gelegten Hamming-Kugeln mit Radius s nicht schneiden. Dies ist offensichtlich für $s \leq \lfloor (d-1)/2 \rfloor$ der Fall. ∎

Ziel der algebraischen Codierungstheorie muß also sein, solche Codes zu konstruieren, deren Dimension und Minimalabstand im Vergleich zur Länge groß sind. Denn dann ist einerseits die Informationsrate hoch, und es können andererseits viele Fehler korrigiert werden. Dies ist aber nicht uneingeschränkt möglich, da grob gesagt die Dimension eines Codes klein ist (in Bezug auf die Länge), falls der Minimalabstand groß ist. Die einfachste Schranke hierfür ist folgende:

Satz 2.2 (Singleton-Schranke)**:** *Für einen $[n,k,d]$-Code gilt: $d \leq n-k+1$.*

Beweis: Punktiert man den Code $(d-1)$-mal, d. h. läßt man an $(d-1)$ festen Positionen die Einträge der Codewörter weg, so bleiben die Codewörter verschieden. Man erhält also einen $[n-d+1,k]$-Code, weshalb gilt: $k \leq n-d+1$. ∎

Definition 2.3: *$[n,k,d]$-Codes, für die die Singleton-Schranke angenommen wird, d. h. für die $k = n-d+1$ ist, heißen **MDS-Codes** (maximum distance separable codes).*

MDS-Codes erfüllen die obige Anforderung an eine geschickte Codierung: Hier sind die Codewörter so gleichmäßig verteilt, daß Hammingkugeln mit Radius

[†]Für $r \in \mathbb{R}$ bezeichnet $\lfloor r \rfloor := \max\{k \in \mathbb{Z} \mid k \leq r\}$ die Gaußklammer.

$\lfloor (d-1)/2 \rfloor$, die um alle Codewörter gelegt werden, den ganzen $\mathbb{F}_q^n$ disjunkt ausschöpfen.

Im allgemeinen ist es viel schwieriger, eine untere Schranke für den Minimalabstand d eines Codes anzugeben. Mit Hilfe des Theorems von Cayley-Bacharach wird uns dies aber für einige Auswerte-Codes gelingen.

2.2. Auswerte-Codes

Auswerte-Codes sind Codes, die durch Auswerten von Polynomen an endlich vielen Stellen gebildet werden. Affine Auswerte-Codes werden z. B. in Høholdt u. a. (1998) betrachtet. Da wir nur Auswerte-Codes für den projektiven Raum benutzen werden, beschränken wir uns bei der Definition auf diesen Fall (vgl. Hansen, 1994, 2003). Zuvor erinnern wir noch an die in den Präliminarien (☞ Kapitel 1) getroffene Konvention, daß $\Gamma = \{p_1, \ldots, p_n\}$ eine Menge von n verschiedenen Punkten im $\mathbb{P}^m$ ist, und daß R_a alle homogenen Polynome in $m+1$ Unbestimmten über $\mathbb{F}_q$ vom Grad a und das Nullpolynom enthält.

Definition 2.4: *Sei $f_\Gamma \in R_a$ mit $f_\Gamma(p) \neq 0$ für alle $p \in \Gamma$. Der zu Γ assoziierte **Auswerte-Code** $C(\Gamma)_a$ ist definiert als das Bild folgender linearer Auswerteabbildung*

$$e_a(\Gamma)\colon R_a \to \mathbb{F}_q^n, \quad f \mapsto \left(\tfrac{f(p_1)}{f_\Gamma(p_1)}, \ldots, \tfrac{f(p_n)}{f_\Gamma(p_n)}\right).$$

$C(\Gamma)_a$ ist also ein linearer Code der Blocklänge n. Bei Wahl eines anderen f_Γ erhält man einen zu $C(\Gamma)_a$ isomorphen Code, d. h. durch die Punktmenge Γ ist der Code bis auf Isomorphie festgelegt.

Der Kern der Auswerteabbildung $e_a(\Gamma)$ ist der Vektorraum $(I_\Gamma)_a = I_\Gamma \cap R_a$. Nach der aus der linearen Algebra bekannten Rangformel gilt dann:

$$^{\#}\Gamma \geq k_a = \dim_{\mathbb{F}_q} C(\Gamma)_a = \dim_{\mathbb{F}_q} R_a - \dim_{\mathbb{F}_q} (I_\Gamma)_a.$$

Schöner läßt sich die Dimension über die *Hilbertfunktion* beschreiben. Bevor wir in Satz 2.8 auf Seite 13 dazu kommen, führen wir die Hilbertfunktion ein und untersuchen einige ihrer Eigenschaften.

2.2.1. Die Hilbertfunktion

Definition 2.5: *Sei I ein homogenes Ideal im Polynomring $R = K[X_0, \ldots, X_m]$ über einem beliegiben Körper K. Die **Hilbertfunktion** von R/I ist die Funktion*

$$H_{R/I}\colon \mathbb{N} \to \mathbb{N}, \quad H_{R/I}(a) := \dim_K \left(R/I\right)_a.$$

Entspricht I dem einer Punktmenge Γ zugeordneten Verschwindungsideal I_Γ (☞ Kapitel 1), so schreiben wir für die Hilbertfunktion auch H_Γ.

Notiz 2.3: Wegen $\left(R/I\right)_a \cong R_a/I_a$ (☞ Kapitel 1) gilt für die Hilbertfunktion:

$$H_{R/I}(a) = \dim_K R_a - \dim_K I_a = \operatorname{codim}_K I_a.$$

Häufig wird die Hilbertfunktion auch hierüber definiert. ◊

Lemma 2.4: *Ist Γ eine endliche Punktmenge im $\mathbb{P}^m$, so gilt für $a \geq {}^{\#}\Gamma - 1$:*

$$H_\Gamma(a) = {}^{\#}\Gamma.$$

Beweis: Wie vereinbart schreiben wir $\Gamma = \{p_1, \ldots, p_n\}$. Mindestens eine Koordinate p_{j_k} eines jeden $p_j = (p_{j_0} : \ldots : p_{j_m}) \in \Gamma$ ist nicht Null.

Zu je zwei verschiedenen Punkten $p_i, p_j \in \Gamma$ gibt es ein homogenes Polynom f_{ij} vom Grad 1 (d. h. eine Linearform) mit $f_{ij}(p_i) = 0$ und $f_{ij}(p_j) \neq 0$. Aus den f_{ij} gewinnt man für jedes $j \in \{1, \ldots, n\}$ ein Polynom

$$f_j := X_{j_k}^{a-(n-1)} \cdot \prod_{\substack{i=1 \\ i \neq j}}^{n} f_{ij},$$

das homogen vom Grad a ist und $f_j(p_i) = 0$ für $i \neq j$ sowie $f_j(p_j) \neq 0$ erfüllt. Da sich alle Polynome vom Grad a, die auf Γ nicht identisch verschwinden, modulo $(I_\Gamma)_a$ durch diese f_j darstellen lassen und da die f_j linear unabhängig sind, folgt:

$${}^{\#}\Gamma = n = \dim_K {R_a}\!\diagup_{(I_\Gamma)_a} = H_\Gamma(a). \qquad \blacksquare$$

Offenbar ist die Hilbertfunktion einer endlichen Punktmenge für große a konstant. Dies ist im Hinblick auf den Satz von Hilbert interessant:

Satz 2.5 (Hilbert)**:** *Sei I ein homogenes Ideal im Polynomring R. Dann gibt es genau ein Polynom $P_{R/I}(a)$, so daß für alle genügend großen $a \in \mathbb{N}$ gilt: $P_{R/I}(a) = H_{R/I}(a)$. $P_{R/I}(a)$ heißt daher **Hilbertpolynom**.*

Beweis: Siehe Eisenbud u. Harris (2001, S. 128). ■

Notiz 2.6: Für eine endliche Punktmenge Γ ist das Hilbertpolynom $P_\Gamma(a)$ gemäß obigem Lemma 2.4 konstant:

$$P_\Gamma(a) := P_{R/I_\Gamma}(a) \equiv {}^{\#}\Gamma. \qquad \Diamond$$

Wir können die Aussage des Lemmas 2.4 leicht umformulieren. Dazu betrachten wir die von der Auswerteabbildung $e_a(\Gamma)$, $a \in \mathbb{N}$, herrührende exakte Sequenz von $\mathbb{F}_q$-Vektorräumen:

$$0 \to (I_\Gamma)_a = \operatorname{Ker} e_a(\Gamma) \to R_a \xrightarrow{e_a(\Gamma)} \mathbb{F}_q^n \to \operatorname{Coker} e_a(\Gamma) \to 0.$$

Bei einer exakten Sequenz verschwindet stets die alternierende Summe der Dimensionen; wegen $H_\Gamma(a) = \dim R_a - \dim(I_\Gamma)_a$ und $\dim \mathbb{F}_q^n = n = {}^\#\Gamma$ ist also:

$$\begin{aligned} 0 &= \dim R_a - \dim(I_\Gamma)_a + \dim \operatorname{Coker} e_a(\Gamma) - \dim \mathbb{F}_q^n \\ &\Longrightarrow\ H_\Gamma(a) = {}^\#\Gamma - \dim \operatorname{Coker} e_a(\Gamma). \end{aligned}$$

Zu Lemma 2.4 ist daher äquivalent:

Lemma 2.7: *Ist Γ eine endliche Punktmenge im $\mathbb{P}^m$, so gilt für $a \geq {}^\#\Gamma - 1$:*

$$\dim \operatorname{Coker} e_a(\Gamma) = 0.$$

2.2.2. Parameter eines Auswerte-Codes

Wie schon bemerkt, hat der Auswertecode $C(\Gamma)_a$ die Länge $n = {}^\#\Gamma$ und die Dimension $k_a = \dim R_a - \dim I_a$, was nach Notiz 2.3 auf der vorherigen Seite dem Wert $H_\Gamma(a)$ der Hilbertfunktion entspricht. Wir haben damit gezeigt:

Satz 2.8: *Die Hilbertfunktion gibt die Dimension des Auswerte-Codes $C(\Gamma)_a$ an:*

$$k_a = \dim C(\Gamma)_a = H_\Gamma(a).$$

Lemma 2.9: *Sei $\Gamma' \subset \Gamma$ eine Teilmenge von Punkten, und sei $C(\Gamma')_a$ die Menge der Codewörter, die an den Stellen 0 sind, die zu den Punkten in Γ' gehören, d. h.*

$$C(\Gamma')_a = \left\{ e_a(\Gamma)(f) \;\middle|\; f \in R_a \text{ mit } f(p) = 0 \text{ für alle } p \in \Gamma' \right\}.$$

Dann gilt für die Dimension von $C(\Gamma')_a$:

$$\dim C(\Gamma')_a = H_\Gamma(a) - H_{\Gamma'}(a).$$

Beweis: Wegen $\Gamma' \subset \Gamma$ ist $I_\Gamma \subset I_{\Gamma'} \subset R$. Schränkt man die Auswerteabbildung $e_a(\Gamma)$ auf $R_a \cap I_{\Gamma'} = (I_{\Gamma'})_a$ ein, so erhält man die exakte Sequenz:

$$0 \to (I_\Gamma)_a \to (I_{\Gamma'})_a \xrightarrow{e_a(\Gamma)} C(\Gamma')_a \to 0.$$

Das liefert mit Notiz 2.3 die Behauptung:

$$\dim C(\Gamma')_a = \dim(I_{\Gamma'})_a - \dim(I_\Gamma)_a = -H_{\Gamma'}(a) + H_\Gamma(a). \qquad \blacksquare$$

Falls nun $\dim C(\Gamma')_a \neq 0$ ist für ein $\Gamma' \subset \Gamma$ mit ${}^\#\Gamma' = \ell$, so enthält $C(\Gamma)_a$ ein von Null verschiedenes Codewort mit mindestens $\ell = {}^\#\Gamma'$ Nullen, weshalb $d \leq n - \ell$ ist. Negation ergibt folgenden Satz und eine untere Schranke für den Minimalabstand:

Satz 2.10: *Genau dann enthält $C(\Gamma)_a$ keine Codewörter ($\neq 0$) mit mindestens ℓ Nullen, wenn für alle Teilmengen $\Gamma' \subset \Gamma$ mit ${}^{\#}\Gamma' = \ell$ gilt:*

$$H_\Gamma(a) = H_{\Gamma'}(a).$$

Dann ist $d \geq n - \ell + 1$.

Da nach der Singleton-Schranke (☞ Satz 2.2) stets $d \leq n - k - 1$ ist, folgt:

Satz 2.11: *Der Code $C(\Gamma)_a$ der Länge $n = {}^{\#}\Gamma$ und der Dimension $k_a = H_\Gamma(a)$ ist genau dann ein MDS-Code, wenn für alle $\Gamma' \subset \Gamma$ mit ${}^{\#}\Gamma' = k_a$ gilt:*

$$H_\Gamma(a) = H_{\Gamma'}(a).$$

Wir können also entscheiden, wann ein Auswerte-Code ein MDS-Code ist.

Bemerkung: Sei $k_a = H_\Gamma(a) = \dim_K R_a/(I_\Gamma)_a$ Dann sind äquivalent:

- Für alle $\Gamma' \subset \Gamma$ mit ${}^{\#}\Gamma' = k_a$ gilt: $H_\Gamma(a) = H_{\Gamma'}(a)$.
- Jedes $f \in R_a$, das in k_a Punkten von Γ verschwindet, verschwindet bereits identisch auf Γ.

2.3. Reed-Muller-Codes

Reed-Muller-Codes sind ursprünglich binäre Codes, die mittels einer $(u, u+v)$-Konstruktion induktiv aus einfachen Codes konstruiert werden (vgl. Lütkebohmert, 2003, Kap. 1.5). Einen schönen Überblick über verschiedene Weiterentwicklungen dieser Codes findet man bei Delsarte u. a. (1970).

Wir betrachten hier die sogenannten *verallgemeinerten (affinen) Reed-Muller-Codes*; sie sind Beispiele für Auswerte-Codes, wie wir sehen werden (vgl. Rentería u. Tapia-Recillas, 1997 oder auch Assmus u. Key, 1992, Kap. 5, insb. Kap. 5.4). Im folgenden seien $P_1, \ldots, P_n$ die $n = q^m$ Elemente des affinen Raumes $\mathbb{A}^m(\mathbb{F}_q)$.

Definition 2.6: *Für jedes $a \in \mathbb{N}$, $a \leq m(q-1)$, ist der **verallgemeinerte (affine) Reed-Muller-Code** der Ordnung a, kurz **GRM-Code**, folgender Unterraum im $\mathbb{F}_q^n$:*

$$GRM(a, m) := \left\{ \big(g(P_1), \ldots, g(P_n)\big) \;\middle|\; g \in \mathbb{F}_q[X_1, \ldots, X_m],\ \operatorname{grad} g \leq a \right\}.$$

Notiz 2.12: Der affine Raum $\mathbb{A}^m(\mathbb{F}_q) = \{P_1, \ldots, P_n\}$ kann vermöge der Einbettung aus Kapitel 1

$$\phi\colon \mathbb{A}^m(\mathbb{F}_q) \to \mathbb{P}^m(\mathbb{F}_q), \quad (a_1, \ldots, a_m) \mapsto (1 : a_1 : \ldots : a_m)$$

mit $\Gamma = \{p_1, \ldots, p_n\} \subset \mathbb{P}^m(\mathbb{F}_q)$ identifiziert werden, wobei wir $p_j = \phi(P_j)$ setzen. Sei nun $a \in \mathbb{N}$, $a \leq m(q-1)$. Dann gilt mit $f_\Gamma := X_0^a \in R_a$:

$$\begin{aligned} GRM(a,m) &= \big\{ \big(g(P_1), \ldots, g(P_n)\big) \;\big|\; g \in \mathbb{F}_q[X_1, \ldots, X_m],\ \operatorname{grad} g \leq a \big\} \\ &= \Big\{ \Big(\tfrac{f(p_1)}{f_\Gamma(p_1)}, \ldots, \tfrac{f(p_n)}{f_\Gamma(p_n)} \Big) \;\Big|\; \underbrace{f \in \mathbb{F}_q[X_0, \ldots, X_m],\ \operatorname{grad} f = a}_{\text{d. h. } f \in R_a} \Big\} = C(\Gamma)_a. \end{aligned}$$

$\Diamond$

Der verallgemeinerte Reed-Muller-Code $GRM(a,m)$ ist also ein Code der Länge $n = q^m$ und besitzt nach Satz 2.8 als Auswerte-Code die Dimension $k = H_\Gamma(a)$. Für den Minimalabstand gilt:

Satz 2.13: *Ist $a = \ell(q-1) + r < m(q-1)$ mit $0 \leq r < q-1$, so hat der verallgemeinerte Reed-Muller-Code $GRM(a,m)$ den Minimalabstand $d = (q-r)q^{m-\ell-1}$.*

Beweis: Siehe Assmus u. Key (1992, S. 166, Cor. 5.5.4). ■

2.4. Reed-Solomon-Codes

Die Reed-Solomon-Codes gehören zu den meistverwandten Codes überhaupt, da sie sich besonders für die Korrektur von Fehlern eignen, die in ganzen Paketen auftreten (sogenannten „bursts“), und sich auch relativ einfach decodieren lassen. Sie werden daher in vielen Bereichen der Datenübertragung eingesetzt, etwa bei der Kommunikation mit Raumsonden oder zur Fehlerkorrektur beim Einlesen von Daten einer CD.

Neben den Reed-Solomon-Codes, die häufig als Spezialfall ($n = q-1$) von *BCH-Codes* eingeführt werden (vgl. Lütkebohmert, 2003, Kap. 4), gibt es noch die *verallgemeinerten Reed-Solomon-Codes* (vgl. van Lint, 1999, S. 99 oder van Lint u. van der Geer, 1988, S. 20).

Definition 2.7: *Sei $k \leq n = q-1$, und sei α ein primitives Element der multiplikativen Gruppe $\mathbb{F}_q^*$, d. h. $\mathbb{F}_q^* = \{\alpha^1, \ldots, \alpha^n\}$. Dann heißt*

$$RS_k(\alpha) = \big\{ \big(f(\alpha^1), \ldots, f(\alpha^n)\big) \;\big|\; f \in \mathbb{F}_q[X],\ \operatorname{grad} f < k \big\}$$

***Reed-Solomon-Code** oder kurz **RS-Code**.*

Ein RS-Code ist also das Bild der Abbildung:

$$\mathcal{L}_k \to \mathbb{F}_q^n, \quad f \mapsto \big(f(\alpha^1), \ldots, f(\alpha^n)\big),$$

wobei $\mathcal{L}_k := \big\{ f \in \mathbb{F}_q[X] \;\big|\; \operatorname{grad} f < k \big\}$ den k-dimensionalen Vektorraum der Polynome vom Grad $< k$ bezeichnet. Diese Abbildung ist $\mathbb{F}_q$-linear und injektiv, da ein Polynom $f \in \mathbb{F}_q[X] \setminus \{0\}$ vom Grad $< n$ weniger als n Nullstellen hat. Das gibt: $\mathcal{L}_k \cong RS_k(\alpha)$, weshalb $RS_k(\alpha)$ ein $[n,k]$-Code über $\mathbb{F}_q$ ist.

Da für das Gewicht eines Codewortes $c \in RS_k(\alpha)$ gilt

$$\begin{aligned} d(c,0) &= n - {}^{\#}\{i \in \{1,\dots,n\} \mid f(\alpha^i) = 0\} \\ &\geq n - \operatorname{grad} f \geq n - (k-1), \end{aligned}$$

erfüllt der Minimalabstand d von $RS_k(\alpha)$ die Ungleichung $d \geq n - k + 1$. Mit der Singleton-Schranke (☞ Satz 2.2) folgt, daß die RS-Codes MDS-Codes sind.

Reed-Solomon-Codes lassen sich leicht verallgemeinern:

Definition 2.8: *Sei $k \leq n < q$, seien $\boldsymbol{\alpha} = (\alpha_1,\dots,\alpha_n) \in \mathbb{F}_q^n$ n paarweise verschiedene Punkte und $\boldsymbol{v} = (v_1,\dots,v_n) \in \mathbb{F}_q^n$ mit $v_i \neq 0$ für alle i. Dann heißt*

$$GRS_k(\boldsymbol{\alpha},\boldsymbol{v}) = \big\{\big(v_1 f(\alpha_1),\dots,v_n f(\alpha_n)\big) \;\big|\; f \in \mathbb{F}_q[X],\ \operatorname{grad} f < k\big\}$$

***Verallgemeinerter Reed-Solomon-Code** oder kurz **GRS-Code**.*

Wie bei den RS-Codes zeigt man, daß $GRS_k(\boldsymbol{\alpha},\boldsymbol{v})$ ein MDS-Code der Länge n und der Dimension k ist.

Beispiel 2.1: Wir betrachten die Punktmenge

$$\Gamma = \{p_1,\dots,p_n\} := \{(r_0 : 0 : \dots : 0 : r_m) \in \mathbb{P}^m \mid r_0 \neq 0, r_m \in \mathbb{F}_q\}$$

mit $n := {}^{\#}\Gamma = q$ Elementen. Die Menge Γ entspricht $\mathbb{F}_q$, denn die Abbildung

$$\varphi\colon \Gamma \to \mathbb{F}_q, \quad (r_0 : 0 : \dots : 0 : r_m) \mapsto r_m \cdot (r_0)^{-1} = \tfrac{r_m}{r_0}$$

ist bijektiv mit Umkehrung $\varphi^{-1}\colon r \mapsto (1 : 0 : \dots : 0 : r)$. Für ein $f \in R_a$ gilt daher: $f(X_0,\dots,X_m) \circ \varphi^{-1} = f(1,0,\dots,0,X_m) =: g(X_m) \in \mathbb{F}_q[X_m]$. Mit diesen Bezeichnern ist $f(p_j) = (f \circ \varphi^{-1})(\varphi(p_j)) = g(\varphi(p_j))$, weshalb für den zu Γ mit $f_\Gamma := X_0^a \in R_a$ gebildeten Auswerte-Code folgt:

$$\begin{aligned} C(\Gamma)_a &= \left\{ \left(\tfrac{f(p_1)}{f_\Gamma(p_1)},\dots,\tfrac{f(p_n)}{f_\Gamma(p_n)} \right) \;\middle|\; f \in R_a \right\} \\ &\cong \Big\{ \big(g(\varphi(p_1)),\dots,g(\varphi(p_n))\big) \;\Big|\; g \in \mathbb{F}_q[X],\ \operatorname{grad} g \leq a \Big\}. \end{aligned}$$

Das ist offenbar ein verallgemeinerter Reed-Solomon-Code, mit $P_j := \varphi(p_j)$ gilt:

$$C(\Gamma)_a = GRS_{a+1}\big((P_1,\dots,P_n),(1,\dots,1)\big). \qquad \Diamond$$

2.5. Geometrische Goppa-Codes

Bei den *geometrischen Goppa-Codes*, welche übrigens manchmal auch *geometrische Reed-Solomon-Codes* genannt werden, handelt es sich um Codes, die mit *algebraischen Kurven* gebildet werden. Bevor wir allerdings diese Codes definieren (☞ Kapitel 2.5.5 auf Seite 22), führen wir die hierfür benötigten Begriffe ein. Dabei orientieren wir uns an Lütkebohmert (2003, Kap. 6), van Lint (1999, Kap. 10) – gekürzte Version von Høholdt u. a. (1998, Kap. 2) – sowie Stichtenoth (1993, Kap. I; Kap. II; Anhang B) und Fulton (1969, Kap. 8).

Im folgenden bezeichne $\mathbb{F}$ den algebraischen Abschluß von $\mathbb{F}_q$.

2.5.1. Algebraische Kurven

Für unsere Zwecke genügt es, eine Varietät als gemeinsame Nullstellenmenge der Polynome eines Primideals anzusehen. Alles weitere zu Varietäten findet man bei Hartshorne (1977, Kap. I).

Definition 2.9: *Eine **affine (bzw. projektive) Varietät** ist ein Nullstellengebilde*

$$\mathcal{X} = V(\mathfrak{p}) = \left\{ x \in \mathbb{A}_{\mathbb{F}}^m \text{ (bzw. } \mathbb{P}_{\mathbb{F}}^m) \;\middle|\; \forall\, f \in \mathfrak{p} \colon f(x) = 0 \right\}$$

für ein Primideal $\mathfrak{p} \subset \mathbb{F}[X_1, \ldots, X_m]$ (bzw. homogenes Primideal $\mathfrak{p} \subset \mathbb{F}[X_0, \ldots, X_m]$).[†] *Varietäten $\mathcal{X}$ der Dimension*[‡] *1 heißen **affine (bzw. projektive) algebraische Kurven**.*

*Wird $\mathfrak{p}$ erzeugt von den Polynomen $f_1, \ldots, f_r$, und sind deren Koeffizienten alle in $\mathbb{F}_q$, so sagen wir, $\mathcal{X}$ ist eine **Kurve über** $\mathbb{F}_q$, die durch die Gleichungen $f_i = 0$ $(1 \leq i \leq r)$ gegeben wird. Die Punkte von $\mathcal{X}$, für die alle Koordinaten in $\mathbb{F}_q$ liegen, heißen **rationale Punkte**.*

Für die Konstruktion von Codes über Kurven werden wir rationale Punkte benötigen, denn dann liegen die Koordinaten im gewählten Alphabet $\mathbb{F}_q$.

Definition 2.10: *Eine algebraische Kurve $\mathcal{X}$ sei gegeben durch die Gleichungen $f_i = 0$ $(1 \leq i \leq r)$. Ist für einen Punkt $x \in \mathcal{X}$ wenigstens eine der partiellen Ableitungen $\partial_{X_j} f_i$ nicht Null, so heißt x ein **nicht singulärer Punkt** der Kurve. Eine Kurve heißt **glatt** oder **nicht singulär**, wenn alle Punkte nicht singulär sind.*

[†] Mit dieser Definition sind algebraische Kurven stets *irreduzibel*, vgl. Hartshorne (1977, S. 3; S. 4).

[‡] Siehe Definition 3.15 auf Seite 34, ähnlich wie bei Schemata wird der affine Raum topologisiert, indem Mengen $V(\mathfrak{a})$ zu einem Ideal $\mathfrak{a}$ als abgeschlossen angesehen werden (Hartshorne, 1977, S. 2 bzw. S. 10).

Beispiel 2.2: Der eindimensionale projektive Raum $\mathbb{P}^1_{\mathbb{F}}$ läßt sich zum Beispiel folgendermaßen in den $\mathbb{P}^2_{\mathbb{F}}$ einbetten:

$$\mathbb{P}^1_{\mathbb{F}} \cong \{(x : y : z) \in \mathbb{P}^2_{\mathbb{F}} \mid x = 0\} = V(\langle X \rangle).$$

Da $\langle X \rangle$ ein Primideal in $\mathbb{F}[X, Y, Z]$ ist und da außerdem $\partial_X X \equiv 1$ ist, ist die *projektive Gerade* $\mathbb{P}^1_{\mathbb{F}}$ eine glatte Kurve in der *projektiven Ebene* $\mathbb{P}^2_{\mathbb{F}}$.

Unabhängig von einer Einbettung gilt für die projektive Gerade:

$$\mathbb{P}^1_{\mathbb{F}} = \{(1 : \alpha) \mid \alpha \in \mathbb{F}\} \cup \{(0 : 1)\} = V(\langle 0 \rangle).$$

Da $\langle 0 \rangle$ ein Primideal ist, sehen wir erneut, daß $\mathbb{P}^1_{\mathbb{F}}$ eine Varietät ist.

Über $\mathbb{F}_q$ erhält man keine Varietät, weil $\mathbb{P}^1(\mathbb{F}_q) = V\big(\langle X \cdot Y^q - X^q \cdot Y \rangle\big)$ gilt, aber $\langle X \cdot Y^q - X^q \cdot Y \rangle$ kein Primideal ist.

Über $\mathbb{F}_q$ ist sogar jedes Nullstellengebilde endlich, also nicht irreduzibel, falls es mehr als einem Punkt enthält. ◊

2.5.2. Funktionen auf algebraischen Kurven

Wie in den Präliminarien beschrieben (☞ Kapitel 1), lassen sich Polynome auf dem affinen Raum als Funktionen auffassen, nicht aber auf dem projektiven Raum. Hier bilden Quotienten von homogenen Polynomen gleichen Grades wohldefinierte Funktionen.

Ganz ähnlich kann man sogenannte *rationale Funktionen* auf algebraischen Kurven oder allgemeiner auf Varietäten definieren. Dafür benötigen wir die in den Präliminarien eingeführte Notation der Lokalisation:

Definition 2.11: *Sei $\mathcal{X} = V(\mathfrak{p})$ eine affine Varietät. Der **(affine) Koordinatenring** von $\mathcal{X}$ ist der Ring $A = \mathbb{F}[X_1, \ldots, X_m]/\mathfrak{p}$, und man nennt*

$$\begin{aligned}\mathbb{F}(\mathcal{X}) := A_{\langle 0 \rangle} &= \textit{ Quotientenkörper von } A \\ &= \left\{ \frac{F}{G} \;\middle|\; F, G \in A, \quad G \neq 0 \right\}\end{aligned}$$

*den **Funktionenkörper** von $\mathcal{X}$. Die Elemente von $\mathbb{F}(\mathcal{X})$ heißen **rationale Funktionen**.*

Definition 2.12: *Sei $\mathcal{X} = V(\mathfrak{p})$ eine projektive Varietät. Der **(projektive oder homogene) Koordinatenring** von $\mathcal{X}$ ist der Ring $S = \mathbb{F}[X_0, \ldots, X_m]/\mathfrak{p} = \bigoplus_{a \in \mathbb{N}} S_a$, und*

$$\mathbb{F}(\mathcal{X}) := S_{(\langle 0 \rangle)} = \left\{ \frac{F}{G} \;\middle|\; F, G \in S_a \textit{ für ein } a \in \mathbb{N}, \quad G \neq 0 \right\}$$

*heißt **Funktionenkörper** von $\mathcal{X}$. Die Elemente von $\mathbb{F}(\mathcal{X})$ werden **rationale Funktionen** genannt.*

Für eine rationale Funktion $\frac{F}{G}$ ist dann also $\frac{F(x)}{G(x)}$ für $x \in \mathcal{X}$ definiert, falls $G(x) \neq 0$.

Beispiel 2.3: Da die projektive Gerade über $\mathbb{F}$ gemäß Beispiel 2.2 durch $\langle 0 \rangle$ gegeben ist, ist der Koordinatenring der ganze Polynomring $\mathbb{F}[X, Y]$. Hier besteht der Funktionenkörper also gerade aus den Quotienten von homogenen Polynomen gleichen Grades:

$$\mathbb{F}(\mathbb{P}^1_{\mathbb{F}}) = \left\{ \frac{F}{G} \;\middle|\; F, G \in \mathbb{F}[X, Y] \text{ homogen vom gleichen Grad und } G \neq 0 \right\}. \quad \Diamond$$

Definition 2.13: *Sei nun $\mathcal{X} = V(\mathfrak{p})$ eine affine oder projektive Varietät. Dann bezeichnet*

$$\mathcal{O}_{\mathcal{X},x} := \left\{ \frac{F}{G} \in \mathbb{F}(\mathcal{X}) \;\middle|\; G(x) \neq 0 \right\}$$

*die Menge der in einem Punkt $x \in \mathcal{X}$ **regulären Funktionen**. Dementsprechend sind die auf einer offenen Menge $U \subset \mathcal{X}$ regulären Funktionen die Funktionen in*

$$\mathcal{O}_{\mathcal{X}}(U) := \bigcap_{x \in U} \mathcal{O}_{\mathcal{X},x}.$$

Bemerkung: Für jedes $x \in \mathcal{X}$ ist $\mathcal{O}_{\mathcal{X},x}$ ein lokaler Ring, dessen maximales Ideal $\mathfrak{m}_x$ gerade aus den Funktionen in $\mathcal{O}_{\mathcal{X},x}$ besteht, die in x verschwinden.

> Ab jetzt sei $\mathcal{X}$ eine glatte projektive Kurve über einem algebraisch abgeschlossenen Körper $\mathbb{F}$ wie in Definition 2.9.

Dann ist $\mathcal{O}_{\mathcal{X},x}$ sogar ein *diskreter Bewertungsring* (vgl. Lütkebohmert, 2003, S. 169, Satz 8.1.5 oder Fulton, 1969, Kap. 3.2, Thm. 1). Die zugehörige *Bewertung* ist eine Abbildung $\mathrm{ord}_x \colon \mathbb{F}(\mathcal{X}) \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$, die jeder rationalen Funktion in $\mathbb{F}(\mathcal{X})$ ihre Null- bzw. Polstellenordnung im Punkt x zuordnet (vgl. Lütkebohmert, 2003, S. 109 oder Høholdt u. a., 1998, Kap. 2.2).[†]

2.5.3. Divisoren

Definition 2.14: *Ein **Divisor** D auf $\mathcal{X}$ ist eine formale Summe $D = \sum_{x \in \mathcal{X}} n_x x$ mit $n_x \in \mathbb{Z}$ und $n_x = 0$ für fast alle Punkte x. Der **Träger** eines Divisors D ist die Menge der Punkte mit Koeffizienten $\neq 0$: $\operatorname{supp} D := \{x \in \mathcal{X} \mid n_x \neq 0\}$. Ein Divisor D heißt **effektiv**, falls alle Koeffizienten n_x nicht negativ sind; wir schreiben dann $D \succcurlyeq 0$. Der **Grad** eines Divisors D ist $\deg(D) := \sum n_x$.*

[†]Genauer hat man zunächst nur eine *diskrete Bewertung* auf dem Quotientenkörper $Q(\mathcal{O}_{\mathcal{X},x})$, d. h. eine surjektive Abbildung $\mathrm{ord}_x \colon Q(\mathcal{O}_{\mathcal{X},x}) \to \mathbb{Z} \cup \{\infty\}$ mit $\mathrm{ord}_x(h) = \infty \iff h = 0$ und

$$\mathrm{ord}_x(fg) = \mathrm{ord}_x(f) + \mathrm{ord}_x(g), \qquad \mathrm{ord}_x(f+g) \geq \min\{\mathrm{ord}_x(f), \mathrm{ord}_x(g)\}.$$

Dabei ist: $\mathcal{O}_{\mathcal{X},x} = \{h \in Q(\mathcal{O}_{\mathcal{X},x}) \mid \mathrm{ord}_x(h) \geq 0\}$ und $\mathfrak{m}_x = \{h \in Q(\mathcal{O}_{\mathcal{X},x}) \mid \mathrm{ord}_x(h) > 0\}$. Die Bewertung läßt sich dann durch $\mathrm{ord}_x(F/G) := \mathrm{ord}_x(F) - \mathrm{ord}_x(G)$ von $Q(\mathcal{O}_{\mathcal{X},x})$ auf den Funktionenkörper $\mathbb{F}(\mathcal{X})$ fortsetzen. Für ein $H \in \mathbb{F}(\mathcal{X})$ sagt man dann bei $\mathrm{ord}_x(H) = r > 0$: „$H$ hat eine *Nullstelle* der Ordnung r in x“ und bei $\mathrm{ord}_x(H) = -r < 0$: „$H$ hat einen *Pol* der Ordnung r in x“.

Wie erwähnt, haben wir für eine glatte projektive Kurve $\mathcal{X}$ und jedes $x \in \mathcal{X}$ eine Bewertung ord_x auf dem Funktionenkörper $\mathbb{F}(\mathcal{X})$.

Definition 2.15: *Sei $f \in \mathbb{F}(\mathcal{X}) \setminus \{0\}$ eine rationale Funktion. Weil $\mathrm{ord}_x(f) = 0$ ist für fast alle $x \in \mathcal{X}$, können wir den durch f bestimmten Divisor*

$$\mathrm{div}(f) := \sum_{x \in \mathcal{X}} \mathrm{ord}_x(f) \cdot x$$

definieren. Er wird ***Hauptdivisor*** *genannt.*

Ein Hauptdivisor $\mathrm{div}(f)$ enthält also Informationen über die Nullstellen und über die Pole der rationalen Funktion f. Es gilt:

Satz 2.14: *Für Hauptdivisoren ist:* $\deg \mathrm{div}(f) = 0$.

Beweis: Siehe Lütkebohmert (2003, S. 199, Satz 8.3.8). ■

Sei $D = \sum n_i x_i - \sum m_j y_j$ ein Divisor, wobei alle $n_i, m_j > 0$ seien. Gibt es nun rationale Funktionen, die in den y_j Nullstellen von mindestens der Ordnung m_j und nur in den x_j Pole von höchstens der Ordnung n_j haben? Dies ist der Fall, falls $\mathcal{L}(D)$ (☞ Definition 2.16) nicht nulldimensional ist.

Definition 2.16: *Für einen Divisor D auf $\mathcal{X}$ setzen wir:*

$$\mathcal{L}(D) := \big\{ f \in \mathbb{F}(\mathcal{X}) \;\big|\; \mathrm{div}(f) + D \succcurlyeq 0 \big\}.$$

Gemäß dem nachfolgenden Satz ist der Vektorraum $\mathcal{L}(D)$ endlichdimensional:

Satz 2.15: *Für einen Divisor D auf $\mathcal{X}$ gilt:*

$$\dim \mathcal{L}(D) \leq \max\{0; 1 + \deg(D)\}.$$

Beweis: Siehe Lütkebohmert (2003, S. 199, Satz 8.3.9). ■

Genauer läßt sich die Dimension von $\mathcal{L}(D)$ mit Hilfe der *regulären Differentialformen* bestimmen (vgl. Fulton, 1969, Kap. 8.4). Wir benutzen hier jedoch den Satz von Riemann, über den auch das *Geschlecht* einer Kurve ohne weitere Theorie definiert werden kann, sowie ein Korollar des Satzes von Riemann-Roch.

Satz 2.16 (Riemann)**:** *Es gibt eine natürliche Zahl g, so daß für alle Divisoren D auf $\mathcal{X}$ gilt:*

$$\dim \mathcal{L}(D) \geq \deg(D) + 1 - g.$$

Die kleinste dieser Zahlen g heißt ***Geschlecht*** *der Kurve $\mathcal{X}$.*

Beweis: Siehe Fulton (1969, Kap. 8.3) oder Lütkebohmert (2003, S. 201, Satz 8.3.12). ■

Bemerkung: Für den Nulldivisor $D_0 = 0$ auf $\mathcal{X}$ enthält $\mathcal{L}(D_0)$ alle rationalen Funktionen $f \in \mathbb{F}(\mathcal{X})$, deren Hauptdivisoren $\operatorname{div}(f)$ effektiv sind. Das erfüllen wegen $\deg \operatorname{div}(f) = 0$ aber nur die konstanten rationalen Funktionen, das heißt, $1 = \dim \mathcal{L}(D_0) \geq 0 + 1 - g$. Das zeigt, daß das Geschlecht g jeder projektiven Kurve $\mathcal{X}$ nicht negativ, also tatsächlich eine natürliche Zahl ist.

Korollar 2.17: *Für einen Divisor D auf $\mathcal{X}$ mit* $\deg(D) > 2g - 2$ *gilt:*

$$\dim \mathcal{L}(D) = \deg(D) + 1 - g.$$

Beweis: Siehe Fulton (1969, Kap. 8.6, Cor. 2) oder auch Lütkebohmert (2003, S. 197, Kor. 8.3.3 oder S. 114, Kor. 6.1.14). ∎

2.5.4. Änderungen für endliche Körper

Da in der Codierungstheorie nur ein endliches Alphabet (ein $\mathbb{F}_q$) zur Verfügung steht, müssen wir die bisher für den algebraischen Abschluß $\mathbb{F}$ von $\mathbb{F}_q$ beschriebene Theorie ein wenig anpassen (vgl. Stichtenoth, 1993, Anhang B.11 & B.12).

Wie bereits erwähnt, sprechen wir von einer Kurve $\mathcal{X}$ über $\mathbb{F}_q$, wenn das Primideal $\mathfrak{p}$ von Polynomen erzeugt wird, deren Koeffizienten alle in $\mathbb{F}_q$ liegen. Die Menge $\mathcal{X}(\mathbb{F}_q)$ der *rationalen Punkte* auf $\mathcal{X}$ läßt sich elegant über die Galoisgruppe $\operatorname{Gal}(\mathbb{F}/\mathbb{F}_q)$ beschreiben, also über die Gruppe der Automorphismen von $\mathbb{F}$, die $\mathbb{F}_q$ punktweise fest lassen. Analog führt man $\mathbb{F}_q$*-rationale Funktionen* von $\mathcal{X}$ ein:

$$\begin{aligned}\mathcal{X}(\mathbb{F}_q) &= \left\{x \in \mathcal{X} \;\middle|\; \forall\, \sigma \in \operatorname{Gal}(\mathbb{F}/\mathbb{F}_q)\colon \sigma(x) = x\right\} \\ &= \left\{x \in \mathcal{X} \;\middle|\; \text{alle Koordinaten von } x \text{ liegen in } \mathbb{F}_q\right\}, \\ \mathbb{F}_q(\mathcal{X}) &= \left\{f \in \mathbb{F}(\mathcal{X}) \;\middle|\; \forall\, \sigma \in \operatorname{Gal}(\mathbb{F}/\mathbb{F}_q)\colon \sigma(f) = f\right\}.\end{aligned}$$

Ein Divisor $D = \sum_{x \in \mathcal{X}} n_x x$ auf $\mathcal{X}$ heißt *definiert über* $\mathbb{F}_q$, falls $\sigma(D) = D$ für alle $\sigma \in \operatorname{Gal}(\mathbb{F}/\mathbb{F}_q)$, also wenn stets $n_{\sigma(x)} = n_x$ gilt. Beachte, D ist insbesondere galoisinvariant, wenn alle x rational sind. Die Forderung $\sigma(D) = D$ ist allgemeiner, denn mit x muß der ganze Galoisorbit von x im Träger liegen, und auf diesem muß zusätzlich die Vielfachheit n_x konstant sein.

Für einen über $\mathbb{F}_q$ definierten Divisor D bilden wir:

$$\mathcal{L}_{\mathbb{F}_q}(D) = \mathbb{F}_q(\mathcal{X}) \cap \mathcal{L}(D).$$

Laut Stichtenoth (1993, Anhang B.12) gilt:

$$\dim_{\mathbb{F}_q}(\mathcal{L}_{\mathbb{F}_q}(D)) = \dim_{\mathbb{F}}(\mathcal{L}(D)),$$

weshalb wir den Satz von Riemann und das Korollar aus dem Satz von Riemann-Roch auch für $\mathcal{L}_{\mathbb{F}_q}(D)$ anwenden können.

2.5.5. Codierung mit algebraischen Kurven

Wir können nun die *geometrischen Goppa-Codes* definieren. V. D. Goppa hat allerdings in Goppa (1981) ursprünglich den hierzu dualen Code eingeführt, wobei *Residuen von Differentialen* benutzt werden. Wir richten uns bei der Bezeichnung nach Stichtenoth (1993, S. 42, Def. II.2.1) und Lütkebohmert (2003, S. 115, Def. 6.2.1).

Andere Autoren nennen diese Codes auch *algebraisch geometrische Codes*, kurz *AG-Codes* (vgl. Tsfasman u. Vlăduţ, 1991, S. 266, Kap. 3.1.1) oder *geometrische (verallgemeinerte) Reed-Solomon-Codes* (vgl. van Lint, 1999, S. 160, Def. 10.6.2).

Sei $\mathcal{X}$ eine glatte projektive algebraische Kurve über $\mathbb{F}_q$ vom Geschlecht g. Seien $x_1, \ldots, x_n$ paarweise verschiedene rationale Punkte auf $\mathcal{X}$ und sei D der Divisor $D = x_1 + x_2 + \ldots + x_n$. Sei $G = \sum_{x \in \mathcal{X}} n_x x$ ein weiterer Divisor mit zu D disjunktem Träger, d. h. $n_{x_j} = 0$ für alle j.

Definition 2.17: *Der zu den Divisoren D und G assoziierte* ***geometrische Goppa-Code*** *$C_{\mathcal{L}}(D, G)$ ist das Bild der linearen Abbildung:*

$$e_{D,G} \colon \mathcal{L}(G) \to \mathbb{F}_q^n, \quad f \mapsto \big(f(x_1), \ldots, f(x_n)\big).$$

$e_{D,G}$ ist wohldefiniert, denn für $f \in \mathcal{L}(G)$ hat man stets $\operatorname{ord}_{x_j}(f) \geq 0$, weil die Träger von D und G disjunkt sind.

Die Länge des Codes $C_{\mathcal{L}}(D, G)$ ist offensichtlich $n = \deg D$.

Satz 2.18: *$C_{\mathcal{L}}(D, G)$ ist ein $[n, k, d]$-Code mit den Parametern:*

$$k = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D), \qquad d \geq n - \deg(G).$$

Beweis: Die Auswerteabbildung $e_{D,G}$ ist eine surjektive Abbildung von $\mathcal{L}(G)$ nach $C_{\mathcal{L}}(D, G) = \operatorname{Im}(e_{D,G})$ mit Kern

$$\operatorname{Ker}(e_{D,G}) = \big\{ f \in \mathcal{L}(G) \;\big|\; \operatorname{ord}_{x_j}(f) > 0 \text{ für } j = 1, \ldots, n \big\} = \mathcal{L}(G - D).$$

Folglich ist $k = \dim \operatorname{Im}(e_{D,G}) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D)$.

Zum Beweis der Aussage über den Minimalabstand wählen wir ein $f \in \mathcal{L}(G)$ mit Gewicht $d(e_{D,G}(f), 0) = d$. Dann verschwindet f in $n - d$ Punkten $x_{j_1}, \ldots, x_{j_{n-d}}$, weshalb $\operatorname{div}(f) + G - x_{j_1} - \ldots - x_{j_{n-d}}$ ein effektiver Divisor ist. Betrachtet man den Grad, so erhält man, da Hauptdivisoren Grad Null haben (☞ Satz 2.14):

$$\begin{aligned} 0 &\leq \deg\big(\operatorname{div}(f) + G - x_{j_1} - \ldots - x_{j_{n-d}}\big) \\ &= \deg \operatorname{div}(f) + \deg(G) - (n - d) = \deg(G) - n + d. \end{aligned}$$

∎

Korollar 2.19: *Gilt* $\deg(G) < n = \deg(D)$*, so ist die Auswerteabbildung* $e_{D,G}$ *injektiv.* $C_{\mathcal{L}}(D,G)$ *hat dann die Parameter:*

$$k = \dim \mathcal{L}(G) \geq \deg(G) + 1 - g, \qquad d \geq n - \deg(G).$$

Für $2g - 2 < \deg(G) < \deg(D)$ *hat man sogar Gleichheit:* $k = \deg(G) + 1 - g$.

Beweis: Nach Annahme ist $\deg(G - D) = \deg(G) - n < 0$, weshalb nach Satz 2.15 gilt: $\mathrm{Ker}(e_{D,G}) = \mathcal{L}(G - D) = \{0\}$; also ist $e_{D,G}$ injektiv und $k = \dim \mathcal{L}(G)$.

Die restlichen Behauptungen folgen unmittelbar mit dem Satz von Riemann (☞ Satz 2.16) und dem Korollar aus dem Satz von Riemann-Roch (☞ Korollar 2.17). ■

Beispiel 2.4: Sei $\mathcal{X}$ die projektive Gerade über $\mathbb{F}_q$, d. h. $\mathcal{X} = \mathbb{P}^1$ (☞ Beispiel 2.2 auf Seite 17 sowie Beispiel 2.3 auf Seite 19), und sei $n = q - 1$. Für ein erzeugendes Element β der zyklischen Gruppe $\mathbb{F}_q^*$ sind die Punkte $x_j = (1 : \beta^j)$, $j \in \{1, \ldots, n\}$, rational auf $\mathcal{X}$. Diese geben den Divisor $D := \sum_{j=1}^{n} x_j$. Sei $G = ax_0 + bx_\infty$ mit $x_0 = (1:0), x_\infty = (0:1)$ und $a, b \geq 0$.

Da $\mathcal{L}_{\mathbb{F}_q}(G)$ alle $\mathbb{F}_q$-rationalen Funktionen – hier also alle Quotienten von homogenen Polynomen gleichen Grades – enthält, die in x_0 bzw. x_∞ höchstens Pole der Ordnung a bzw. b haben, bilden

$$\left(\tfrac{Y}{X}\right)^i, \quad -a \leq i \leq b$$

eine $\mathbb{F}_q$-Basis von $\mathcal{L}_{\mathbb{F}_q}(G)$, d. h. $\dim_{\mathbb{F}_q}(\mathcal{L}_{\mathbb{F}_q}(G)) = a + b + 1 = \deg(G) + 1$.

Der zu D und G assoziierte geometrische Goppa-Code $C_{\mathcal{L}}(D,G)$ hat dann die Dimension $k = a + b + 1$ (☞ Korollar 2.19). Man erhält:

$$\begin{aligned} C_{\mathcal{L}}(D,G) &= \left\{ \big(h(x_1), \ldots, h(x_n)\big) \;\middle|\; h \in \mathcal{L}_{\mathbb{F}_q}(G) \right\} \qquad \left| \begin{array}{l} h \in \mathbb{F}_q\text{-Lin.-Komb. von } \left(\tfrac{Y}{X}\right)^i \\ x_j = (1 : \beta^j) \end{array} \right. \\ &= \left\{ \big(h(\beta^1), \ldots, h(\beta^n)\big) \;\middle|\; h \in \mathbb{F}_q[Z],\ \mathrm{grad}\, f < k = a + b + 1 \right\} \\ &= RS_k(\beta). \end{aligned}$$

Der geometrische Goppa-Code $C_{\mathcal{L}}(D,G)$ liefert also einen Reed-Solomon-Code.

In Buch von Stichtenoth (1993, Kap. II.3, Prop. II.3.3) wird sogar bewiesen, daß jeder verallgemeinerte Reed-Solomon-Code einem geometrischen Goppa-Code entspricht. ◊

Als letztes betrachten wir *Hermitesche Codes*. Das sind spezielle geometrische Goppa-Codes, die zu Divisoren von *Hermiteschen Kurven* gebildet werden.

Beispiel 2.5 (Hermitesche Codes)**:** Wir betrachten die glatte Kurve:

$$\mathcal{X}_q = V(f) \subset \mathbb{P}^2_{\mathbb{F}} \quad \text{mit } f(X,Y,Z) = Y^{q+1} - X^q Z - X Z^q.$$

Diese *Hermitesche Kurve* hat das Geschlecht $g = \frac{1}{2}(q^2 - q)$ (vgl. van Lint, 1999, S. 158, Theorem 10.4.6 oder Stichtenoth, 1993, S. 211 und S. 247). Auf $\mathcal{X}_q$ gibt es einen eindeutig bestimmten unendlich fernen Punkt[†], nämlich $x_\infty := (1 : 0 : 0)$. Darüber hinaus liegen genau q^3 affine $\mathbb{F}_{q^2}$-rationale Punkte $x_j = (\alpha_j : \beta_j : 1)$ auf X_q (☞ Satz A.2 im Anhang); α_j und β_j erfüllen dabei: $\beta_j^{q+1} = \alpha_j^q + \alpha_j$.

Ein *Hermitescher Code* C_r mit $r \in \mathbb{Z}$ ist der zu den Divisoren $D = \sum_{j=1}^{q^3} x_j$ und $G = r x_\infty$ assoziierte geometrische Goppa-Code $C_{\mathcal{L}}(D,G)$. Dieser Code hat die Blocklänge $n = \deg D = q^3$. Gemäß Korollar 2.19 gilt für die Dimension und für den Minimalabstand von C_r, wenn $0 \le r < q^3$ ist:

$$k_r \ge r + 1 - \tfrac{1}{2}(q^2 - q), \qquad\qquad d_r \ge q^3 - r.$$

Für $q^2 - q - 2 < r < q^3$ gilt sogar $k_r = r + 1 - \frac{1}{2}(q^2 - q)$.

In gewissen Fällen kennt man sogar den tatsächlichen Minimalabstand (siehe auch Stichtenoth, 1988, Theorem 5):

Behauptung: Für $r = i \cdot q$ mit $0 \le i \le q^2$ hat der Hermitesche Code $C_r = C_{\mathcal{L}}(D, r x_\infty)$ den Minimalabstand $d_r = q^3 - r$.

Beweis: Da stets $d_r \ge q^3 - r$ ist, genügt es zu zeigen, daß es für $r = i \cdot q$ mit $0 \le i \le q^2$ eine rationale Funktion $0 \ne f \in \mathcal{L}(r x_\infty)$ gibt, die genau r verschiedene einfache Nullstellen besitzt.

Division mit Rest liefert jedenfalls die Darstellung[‡]

$$r = i \cdot q = s(q+1) + t \quad \text{mit } 0 \le t \le q \text{ und } s \le q^2 - q.$$

Es gibt dann paarweise verschiedene Elemente $\alpha_1, \ldots, \alpha_t \in \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\}$ und $\alpha_{t+1}, \ldots, \alpha_{t+s} \in \{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha \ne 0\}$, vergleiche Lemma A.1 im Anhang.

Dann hat die durch

$$\prod_{j=1}^{t+s} \frac{X - \alpha_j Z}{Z}$$

induzierte rationale Funktion $f \in \mathcal{L}(r x_\infty)$ auf $\mathcal{X}_q$ die folgenden Nullstellen:

$$\begin{aligned} &(\alpha_j : 0 : 1) \quad \text{für } 1 \le j \le t, \\ &(\alpha_j : \beta_j : 1) \quad \text{für } t+1 \le j \le t+s. \end{aligned}$$

[†]Das Polynom f ist die Homogenisierung des Polynoms $Y^{q+1} - X^q - X$; folglich sind die unendlich fernen Punkte auf $\mathcal{X}_q$ die Punkte, deren Z-Koordinate Null ist. Das erfüllt nur $x_\infty = (1 : 0 : 0)$.

[‡]Für $s > q^2 - q$ hat man: $r = s(q+1) + t \ge (q^2 - q + 1)(q+1) = q^3 + 1 > r$, Widerspruch.

Im zweiten Fall gibt es zu jedem j genau $q+1$ verschiedene β_j mit $\beta_j^{q+1} = \alpha_j^q + \alpha_j$. Insgesamt erhält man daher $t \cdot 1 + s \cdot (q+1) = r$ unterschiedliche einfache Nullstellen. ◊

Speziell für $r = (q-\lambda)(q^2+q)$ mit $0 \leq \lambda \leq q-1$ hat der Hermitesche Code C_r also die Parameter (es gilt hier $q^2 - q - 2 < r < q^3$):

$$n = q^3, \qquad k_r = q^3 + \tfrac{1-2\lambda}{2}(q^2+q) + 1, \qquad d_r = (\lambda-1)q^2 + \lambda q.$$

Weitere Betrachtungen zur Struktur von Hermiteschen Codes findet man im Artikel von Little, Saints und Heegard (1997). ◊

3. Projektive Algebraische Geometrie

In diesem Kapitel stellen wir die zur Abschätzung von Minimalabständen von Auswerte-Codes (☞ Kapitel 4 auf Seite 45) benötigten Grundlagen der Algebraischen Geometrie zusammen. Insbesondere behandeln wir nulldimensionale Schemata.

Wir orientieren uns hauptsächlich an den Büchern von Hartshorne (1977) und Kunz (1997). Eine ausführliche Behandlung des Satzes von Cayley-Bacharach findet man im Artikel von Eisenbud u. a. (1996).

3.1. Spektren von Ringen

Definition 3.1: *Für einen Ring A bzw. für einen graduierten Ring $S = \bigoplus_{a\in\mathbb{Z}} S_a$ mit irrelevantem Ideal $S_+ = \bigoplus_{a>0} S_a$ ist das* ***Primspektrum*** $\operatorname{Spec} A$ *bzw. das* ***homogene Primspektrum*** $\operatorname{Proj} S$ *folgendermaßen definiert:*

$$\operatorname{Spec} A := \{\mathfrak{p} \subset A \mid \mathfrak{p} \text{ Primideal}\}, \qquad \operatorname{Proj} S := \left\{ \mathfrak{p} \subset \operatorname{Spec} S \;\middle|\; \begin{array}{c} \mathfrak{p} \text{ homogen}, \\ \mathfrak{p} \not\supset S_+ \end{array} \right\}.$$

Diese Primspektren werden mit der ***Zariskitopologie*** *zu topologischen Räumen; die* ***abgeschlossenen Mengen*** *sind hier die Primoberideale eines Ideals $\mathfrak{a} \subset A$ bzw. homogenen Ideals $\mathfrak{b} \subset S$:*

$$V(\mathfrak{a}) := \{\mathfrak{p} \in \operatorname{Spec} A \mid \mathfrak{a} \subset \mathfrak{p}\}, \qquad V_+(\mathfrak{b}) := \{\mathfrak{p} \in \operatorname{Proj} S \mid \mathfrak{b} \subset \mathfrak{p}\}.$$

Eine Basis der Topologie bilden die ***offenen Basismengen*** *$D(g)$ zu $g \in A$ bzw. $D_+(f)$ zu homogenem $f \in S_+$:*

$$D(g) := \{\mathfrak{p} \in \operatorname{Spec} A \mid g \notin \mathfrak{p}\}, \qquad D_+(f) := \{\mathfrak{p} \in \operatorname{Proj} S \mid f \notin \mathfrak{p}\}.$$

Nach Definition ist die Zariskitopologie auf $\operatorname{Proj} S$ die Relativtopologie der Zariskitopologie auf $\operatorname{Spec} S$.

Definition 3.2: *Eine (nichtleere) Teilmenge Y eines topologischen Raumes X nennt man* ***irreduzibel****, wenn sie nicht dargestellt werden kann als Vereinigung $Y = Y_1 \cup Y_2$ zweier echter Teilmengen von Y, die in Y abgeschlossen sind.*

Beispiel 3.1: Ist A bzw. S ein Integritätsring, z. B. $A = S = K[X_0, \ldots, X_m]$, so sind $\operatorname{Spec} A$ und $\operatorname{Proj} S$ irreduzibel. Denn wäre $\operatorname{Proj} S = V_+(\mathfrak{a}) \cup V_+(\mathfrak{b}) = V_+(\mathfrak{ab})$, so wäre $\mathfrak{ab}$ in jedem (homogenen) Primideal enthalten. Weil $\langle 0\rangle$ ein Primideal ist, hätte man $\mathfrak{ab} = \langle 0\rangle$, also o. B. d. A. $\mathfrak{a} = \langle 0\rangle$. Aber $V_+(\langle 0\rangle) = \operatorname{Proj} S$. ◊

Satz 3.1: *Jede (nichtleere) irreduzible abgeschlossene Teilmenge Y von* Spec A *(bzw.* Proj S*) besitzt genau einen* ***generischen Punkt*** $\mathfrak{p} \in$ Spec A *(bzw.* $\mathfrak{p} \in$ Proj S*), d. h. es gibt genau ein* $\mathfrak{p}$*, so daß Y die abgeschlossene Hülle von* $\{\mathfrak{p}\}$ *ist.*

Beweis: Siehe Kunz (1997, S. 69, Satz 1.14; S. 74). ∎

Definition 3.3: *Ein topologischer Raum X heißt* ***noethersch****, falls jede* ***absteigende Kette*** $Y_1 \supset Y_2 \supset \ldots$ *von abgeschlossenen Mengen stationär wird, d. h. es gibt $r \in \mathbb{N}$ mit $Y_r = Y_{r+1} = \ldots$*

Notiz 3.2: Ist A ein noetherscher Ring, so ist Spec A ein noetherscher topologischer Raum. Ebenso ist Proj S ein noetherscher topologischer Raum, falls S ein noetherscher graduierter Ring ist. Viele Beispiele werden durch Polynomringe über Körpern geliefert, denn diese sind gemäß dem Hilbertschen Basissatz noethersch. ◊

Satz 3.3: *In einem noetherschen topologischen Raum kann jede (nichtleere) abgeschlossene Teilmenge Y als endliche Vereinigung $Y = Y_1 \cup \ldots \cup Y_r$ von irreduziblen abgeschlossenen Teilmengen Y_j geschrieben werden. Die (bezüglich Inklusion) maximalen irreduziblen Teilmengen heißen* ***irreduzible Komponenten*** *von X.*

Beweis: Siehe Hartshorne (1977, S. 5, Prop. 1.5). ∎

3.2. Garben und Schemata

3.2.1. Garben

Definition 3.4: *Sei X ein topologischer Raum. Eine* ***Prägarbe*** $\mathscr{F}$ *von Ringen auf X ordnet jeder offenen Menge $U \subset X$ einen Ring $\mathscr{F}(U)$ zu, und für jede Inklusion von offenen Mengen $V \subset U$ genügt eine* ***Restriktionsabbildung*** $\varrho_{U,V} \colon \mathscr{F}(U) \to \mathscr{F}(V)$ *den Bedingungen:*

$$\varrho_{U,U} = id, \qquad \varrho_{V,W} \circ \varrho_{U,V} = \varrho_{U,W} \text{ für alle } W \subset V \subset U.$$

Wir setzen $\mathscr{F}(\emptyset) = 0$ und schreiben $\sigma|_V$ anstelle von $\varrho_{U,V}(\sigma)$ für $\sigma \in \mathscr{F}(U)$.

Die Elemente von $\mathscr{F}(U)$ heißen ***Schnitte*** *von $\mathscr{F}$ über U; ist $U = X$, so spricht man von* ***globalen Schnitten****. Bisweilen bezeichnen wir den Ring $\mathscr{F}(U)$ mit $\Gamma(U, \mathscr{F})$.*

Definition 3.5: *Eine Prägarbe $\mathscr{F}$ auf einem topologischen Raum X heißt* ***Garbe****, wenn für jede offene Überdeckung $U = \bigcup V_i$ einer offenen Menge $U \subset X$ gilt:*

(G1) Ist $\sigma \in \mathscr{F}(U)$ ein Element mit $\sigma|_{V_i} = 0$ für alle i, so ist $\sigma = 0$.

(G2) Hat man für jedes i ein Element $\sigma_i \in \mathscr{F}(V_i)$ mit $\sigma_i|_{V_i \cap V_j} = \sigma_j|_{V_i \cap V_j}$ für alle i, j, so gibt es ein $\sigma \in \mathscr{F}(U)$ mit $\sigma|_{V_i} = \sigma_i$ für jedes i.
(σ ist eindeutig bestimmt wegen der ersten Bedingung.)

Eine Garbe ist für offene Mengen definiert. Man möchte aber, da der zugrunde liegende topologische Raum X aus Punkten besteht, das Verhalten einer Garbe in den Punkten $x \in X$ kennen. Daher betrachtet man:

Definition 3.6: *Für eine Prägarbe $\mathscr{F}$ (von Ringen) und einen Punkt $x \in X$ ist der **Halm** $\mathscr{F}_x$ von $\mathscr{F}$ in x definiert als der direkte Limes der Ringe $\mathscr{F}(U)$ für alle offenen Umgebungen U von x in X:*

$$\mathscr{F}_x = \varinjlim_{\substack{U \subset X \text{ offen}, \\ x \in U}} \mathscr{F}(U) = {}^{F}\!/_{\sim} \quad \text{mit } F = \dot{\bigcup_{\substack{U \subset X \text{ offen}, \\ x \in U}}} \mathscr{F}(U).$$

Dabei ist $\sigma \in \mathscr{F}(U)$ genau dann äquivalent zu $\tau \in \mathscr{F}(V)$, geschrieben $\sigma \sim \tau$, wenn es eine offene Umgebung $W \subset U \cap V$ von x gibt mit $\varrho_{U,W}(\sigma) = \sigma|_W = \tau|_W = \varrho_{V,W}(\tau)$.

*Der Halm einer Garbe von Ringen ist selbst ein Ring; die Elemente σ_x (Äquivalenzklassen bezüglich $\sim$) des Halmes $\mathscr{F}_x$ sind die **Keime** von Schnitten von $\mathscr{F}$ in x.*

Definition 3.7: *Ein **Morphismus** $\varphi\colon \mathscr{F} \to \mathscr{G}$ von Prägarben auf einem topologischen Raum X besteht aus einer Kollektion von Ringhomomorphismen $\varphi_U\colon \mathscr{F}(U) \to \mathscr{G}(U)$ zu $U \subset X$ offen, so daß für jede Inklusion $V \subset U$ das Diagramm*

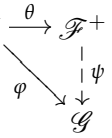
$$\begin{array}{ccc} \mathscr{F}(U) & \xrightarrow{\varphi_U} & \mathscr{G}(U) \\ {\scriptstyle \varrho^{\mathscr{F}}_{U,V}}\downarrow & & \downarrow{\scriptstyle \varrho^{\mathscr{G}}_{U,V}} \\ \mathscr{F}(V) & \xrightarrow{\varphi_V} & \mathscr{G}(V) \end{array}$$

*kommutiert. Ein **Morphismus** von Garben ist analog definiert.*

Definition 3.8: *Sei $\varphi\colon \mathscr{F} \to \mathscr{G}$ ein Morphismus von Garben. Die **Kerngarbe** $\operatorname{Ker}\varphi$ von φ ist die durch $U \mapsto \operatorname{Ker}(\varphi_U)$ gegebene Garbe. Sie ist eine **Untergarbe** von $\mathscr{F}$.*

Bei der Kerngarbe haben wir Glück, daß die naheliegende Definition eine Garbe liefert. Analoge Definitionen für Bild oder Cokern führen nur zu Prägarben. Ebenso ist für eine Untergarbe $\mathscr{F}$ von $\mathscr{G}$ der Quotient $U \mapsto \mathscr{G}(U)/\mathscr{F}(U)$ im allgemeinen auch nur eine Prägarbe.

Zu jeder Prägarbe $\mathscr{F}$ gibt es aber eine eindeutig bestimmte *assoziierte Garbe* $\mathscr{F}^+$ und einen Morphismus $\theta\colon \mathscr{F} \to \mathscr{F}^+$, so daß gilt: Für jede Garbe $\mathscr{G}$ und für jeden Morphismus $\varphi\colon \mathscr{F} \to \mathscr{G}$ existiert ein eindeutig bestimmter Morphismus $\psi\colon \mathscr{F}^+ \to \mathscr{G}$ mit $\varphi = \psi \circ \theta$. Außerdem ist $\mathscr{F}_\mathfrak{p} = \mathscr{F}^+_\mathfrak{p}$ für alle $\mathfrak{p} \in X$ (vgl. Hartshorne, 1977, S. 64, Prop. 1.2).



Man verwendet dann statt einer Prägarbe $\mathscr{F}$ deren „Garbifizierung“ $\mathscr{F}^+$.

Damit ist auch die Bildgarbe Im φ erklärt, und wir können Eigenschaften eines Morphismus $\varphi\colon \mathscr{F} \to \mathscr{G}$ von Garben definieren: φ heißt *injektiv*, falls Ker $\varphi = 0$ ist, *surjektiv*, falls Im $\varphi = \mathscr{G}$ ist, und *bijektiv*, wenn φ injektiv und surjektiv ist.

Hat man auf einem topologischen Raum eine Garbe gegeben, so kann man ausgehend von dieser weitere Garben definieren.

Definition 3.9: *Sei $\alpha\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen. Für eine Garbe $\mathscr{F}$ auf X wird die* ***direkte Bildgarbe*** *$\alpha_*\mathscr{F}$ auf Y definiert durch:*

$$(\alpha_*\mathscr{F})(V) := \mathscr{F}(\alpha^{-1}(V)) \quad \textit{für offene } V \subset Y.$$

Für eine offene Menge $U \subset X$ ist die ***Einschränkung*** *$\mathscr{F}|_U$ von $\mathscr{F}$ auf U gegeben duch:*

$$\mathscr{F}|_U(W) := \mathscr{F}(W) \qquad \textit{für offene } W \subset U.$$

$\mathscr{F}|_U$ ist eine Garbe.

3.2.2. Schemata

Ein *geringter Raum* $(X, \mathscr{O}_X)$ ist ein topologischer Raum X zusammen mit einer Garbe $\mathscr{O}_X$ von Ringen. Sind alle Halme $\mathscr{O}_{X,x}$ ($x \in X$) eines geringten Raumes $(X, \mathscr{O}_X)$ sogar lokale Ringe[†], so spricht man von einem *lokal geringten Raum*. Solche Garben – dann *Strukturgarben* genannt – lassen sich für die Spektren Spec A und Proj S definieren (siehe Hartshorne, 1977, S. 70 und S. 76). Wir geben hier nur die wesentlichen Eigenschaften dieser Strukturgarben an.

Satz 3.4: *Sei $\mathscr{O}_{\operatorname{Spec} A}$ die Strukturgarbe von* Spec A*, und sei $\mathscr{O}_{\operatorname{Proj} S}$ die Strukturgarbe von* Proj S*. Dann gilt für die Halme zu $\mathfrak{q} \in \operatorname{Spec} A$ bzw. $\mathfrak{p} \in \operatorname{Proj} S$:*

$$\mathscr{O}_{\operatorname{Spec} A,\mathfrak{q}} \cong A_{\mathfrak{q}}, \qquad \mathscr{O}_{\operatorname{Proj} S,\mathfrak{p}} \cong S_{(\mathfrak{p})}.$$

Außerdem gilt für die Schnitte über offenen Basismengen ($g \in A$; $f \in S_+$ homogen):

$$\mathscr{O}_{\operatorname{Spec} A}(D(g)) \cong A_g, \qquad \mathscr{O}_{\operatorname{Proj} S}(D_+(f)) \cong S_{(f)}.$$

Beweis: Siehe Hartshorne (1977, S. 71, Prop. 2.1; S. 76, Prop. 2.5). ∎

Offenbar sind Spec A und Proj S lokal geringte Räume.

[†]Ein kommutativer Ring mit Einselement heißt *lokaler Ring*, wenn er genau ein maximales Ideal besitzt.

Notiz 3.5: Da $1 \in A$ in keinem Primideal von A enthalten ist, ist $D(1) = \operatorname{Spec} A$. Gemäß Satz 3.4 hat man also für die globalen Schnitte von $\operatorname{Spec} A$:

$$\mathscr{O}_{\operatorname{Spec} A}(\operatorname{Spec} A) \cong A. \qquad \Diamond$$

Definition 3.10: *Ein **affines Schema** ist ein lokal geringter Raum $(X, \mathscr{O}_X)$, der isomorph zum Spektrum $(\operatorname{Spec} A, \mathscr{O}_{\operatorname{Spec} A})$ eines Ringes A ist.*

*Ein **projektives Schema** ist ein lokal geringter Raum $(X, \mathscr{O}_X)$, der isomorph zum homogenen Spektrum $(\operatorname{Proj} S, \mathscr{O}_{\operatorname{Proj} S})$ eines graduierten Ringes S ist.*

*Ein **Schema** ist ein lokal geringter Raum $(X, \mathscr{O}_X)$, für den jeder Punkt $x \in X$ eine offene Umgebung U besitzt, so daß der topologische Raum U zusammen mit der eingeschränkten Garbe $\mathscr{O}_X|_U$ isomorph zu einem affinen Schema ist.*

Da die Einschränkung einer Garbe auf eine offene Menge selbst eine Garbe ist, ist ein *offenes Unterschema* von $(X, \mathscr{O}_X)$ ein Schema der Form $(U, \mathscr{O}_X|_U)$ mit $U \subset X$ offen.

Notiz 3.6: Für die offenen Basismengen $D_+(f)$ von $\operatorname{Proj} S$ gilt sogar:

$$\left(D_+(f), \mathscr{O}_{\operatorname{Proj} S}|_{D_+(f)}\right) \cong \left(\operatorname{Spec} S_{(f)}, \mathscr{O}_{\operatorname{Spec} S_{(f)}}\right)$$

(siehe Hartshorne, 1977, S. 76, Prop. 2.5). $\operatorname{Proj} S$ wird also überdeckt von affinen Schemata, weshalb ein projektives Schema tatsächlich ein Schema ist. Die Überdekkung ist endlich, falls der zugrunde liegende Ring S noethersch ist, denn dann ist $\operatorname{Proj} S$ kompakt[†] (siehe Hartshorne, 1977, S. 80, Aufgabe 2.13(a)).

Obige Isomorphie liefert die in Satz 3.4 angegebene Eigenschaft:

$$\mathscr{O}_{\operatorname{Proj} S}(D_+(f)) = \mathscr{O}_{\operatorname{Proj} S}|_{D_+(f)}(D_+(f)) \cong \mathscr{O}_{\operatorname{Spec} S_{(f)}}(\operatorname{Spec} S_{(f)}) = S_{(f)}. \qquad \Diamond$$

Definition 3.11: *Ein Schema $(X, \mathscr{O}_X)$ heißt ...*

*... **irreduzibel**, falls X als topologischer Raum irreduzibel ist.*

*... **reduziert**, falls alle Halme $\mathscr{O}_{X,\mathfrak{p}}$ keine nilpotenten Elemente besitzen.*

*... **integer**, falls X irreduzibel und reduziert ist.*

Beispiel 3.2: Nach Beispiel 3.1 auf Seite 27 ist das projektive Schema $\operatorname{Proj} R$ irreduzibel. $\operatorname{Proj} R$ ist sogar integer, da das *Nilradikal* des Integritätsringes R – das sind alle nilpotenten Elemente, also der Schnitt aller Primideale in R – das Nullideal $\langle 0 \rangle$ ist. $\Diamond$

[†]Bei uns heißt eine Menge *kompakt*, wenn jede offene Überdeckung eine endliche Teilüberdeckung hat. Dies wird in der Algebraischen Geometrie häufig mit *quasi-kompakt* bezeichnet. *Kompakte* Mengen sind dann solche, die quasi-kompakt sind und die Hausdorff-Eigenschaft besitzen.

3.2.3. Abgeschlossene Unterschemata

Definition 3.12: *Ein Morphismus von Schemata* $(f, f^{\#})\colon (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ *heißt* ***abgeschlossene Immersion****, falls gilt:*

- *Es gibt eine abgeschlossene Menge* $Z \subset X$*, so daß* $f\colon Y \to X$ *einen Homöomorphismus* $f\colon Y \to Z$ *induziert.*
- *Der Garbenmorphismus* $f^{\#}\colon \mathscr{O}_X \to f_*\mathscr{O}_Y$ *ist surjektiv.*[†]

Ein ***abgeschlossenes Unterschema*** *von* X *ist ein Schema der Form* $(Y, \mathscr{O}_Y)$ *für eine abgeschlossene Teilmenge* $Y \subset X$ *zusammen mit einer abgeschlossenen Immersion* $(i, i^{\#})\colon (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$*, wobei* $i\colon Y \to X$ *die Inklusion ist.*

Wir betrachten hier nur den projektiven Fall, also abgeschlossene Unterschemata von $(\operatorname{Proj} R, \mathscr{O}_{\operatorname{Proj} R})$ zum Polynomring $R = K[X_0, \ldots, X_m]$. Außerdem setzen wir voraus, daß der Körper K algebraisch abgeschlossen ist. Während man im Affinen eine $1:1$ Beziehung zwischen Idealen und abgeschlossenen Unterschemata hat, kommt es im Projektiven auf folgenden Begriff an:

Definition 3.13: *Für ein homogenes Ideal* I *in* R *heißt das homogene Ideal*

$$\overline{I} := \{f \in R \mid \forall\, i \in \{0, \ldots, m\}\ \exists\, \nu \in \mathbb{N}\colon X_i^{\nu} f \in I\}$$

Sättigung *oder* ***Saturation*** *von* I*. Ein Ideal* I *ist* ***gesättigt*** *oder* ***saturiert****, falls* $\overline{I} = I$*.*

Satz 3.7: *Für jedes homogene Ideal* $I \subset R$ *ist* $\big(\operatorname{Proj} R/I, \mathscr{O}_{\operatorname{Proj} R/I}\big)$ *ein abgeschlossenes (projektives) Unterschema von* $(\operatorname{Proj} R, \mathscr{O}_{\operatorname{Proj} R})$*. Dabei ist* $\operatorname{Proj} R/I$ *homöomorph zu* $V_+(I) \subset \operatorname{Proj} R$*. Zwei homogene Ideale* I, J *definieren zudem genau dann dasselbe abgeschlossene Unterschema, wenn sie die gleiche Sättigung haben:* $\overline{I} = \overline{J}$*.*

Umgekehrt gibt es zu jedem abgeschlossenen Unterschema $(Y, \mathscr{O}_Y)$ *ein gesättigtes Ideal* I*, so daß* Y *das von* I *bestimmte abgeschlossene Unterschema ist.*

Beweis: Siehe Kunz (1997, S. 114, Satz 4.8) oder Hartshorne (1977, S. 125, Aufgabe 5.10). ∎

Beispiel 3.3: Das Ideal $\langle Y\rangle \subset K[X, Y]$ ist ein (homogenes) Primideal und daher gesättigt. Hier ist $K[X, Y]/\langle Y\rangle \cong K[X]$ ein Integritätsring, weshalb das Unterschema $\operatorname{Proj}\big(K[X, Y]/\langle Y\rangle\big)$ reduziert ist. Auch das Ideal $\langle Y^2\rangle \subset K[X, Y]$ ist gesättigt:

$$\overline{\langle Y^2\rangle} = \big\{f \in K[X, Y] \;\big|\; \exists\, \nu, \mu \in \mathbb{N}\colon X^{\nu} f \in \langle Y^2\rangle \text{ und } Y^{\mu} f \in \langle Y^2\rangle\big\} = \langle Y^2\rangle.$$

Weil aber Y in $K[X, Y]/\langle Y^2\rangle$ nilpotent ist, ist $\operatorname{Proj}\big(K[X, Y]/\langle Y^2\rangle\big)$ nicht reduziert.

[†] $f_*\mathscr{O}_Y$ ist die direkte Bildgarbe (☞ Definition 3.9)

Die durch $\langle Y \rangle$ und $\langle Y^2 \rangle$ definierten Unterschemata sind nicht isomorph, da die Halme der zugehörigen Strukturgarben unterschiedlich sind. Dies muß nach obigem Satz auch so sein, da $\langle Y \rangle$ und $\langle Y^2 \rangle$ zwei verschiedene gesättigte Ideale sind. Man beachte, daß die topologischen Räume dieser Unterschemata beide homöomorph zur einpunktigen Menge $\langle Y \rangle = V_+(Y) = V_+(Y^2)$ sind. ◊

Die abgeschlossenen (projektiven) Unterschemata von $(\operatorname{Proj} R, \mathscr{O}_{\operatorname{Proj} R})$ entsprechen nach Satz 3.7 eindeutig den gesättigten Idealen in R. Man definiert daher:

Definition 3.14: *Ist $(Y, \mathscr{O}_Y)$ ein abgeschlossenes Unterschema von $(\operatorname{Proj} R, \mathscr{O}_{\operatorname{Proj} R})$, so nennt man das zugehörige gesättigte Ideal I_Y das **Verschwindungsideal** von Y in R. Der Quotient R/I_Y ist der **homogene Koordinatenring** von Y.*

Zum Abschluß betrachten wir noch das Verschwindungsideal I_Γ einer endlichen Punktmenge Γ, das wir in den Präliminarien (☞ Kapitel 1 auf Seite 3) eingeführt haben. Dieses ist auch das Verschwindungsideal (☞ Definition 3.14) des durch I_Γ gegebenen reduzierten Unterschemas:

Beispiel 3.4: Sei $\Gamma = \{p_1, \ldots, p_n\}$ wieder eine Menge von n verschiedenen Punkten im $\mathbb{P}^m$. Jedem p_j können wir nun ein homogenes Primideal $\mathfrak{q}_j$ in R zuordnen:

$$\text{Punkt } p_j \in \Gamma \quad \mathrel{\widehat{=}} \quad \text{hom. Primideal } \mathfrak{q}_j := \{f \in R \mid f(p_j) = 0\}.$$

Ein solches $\mathfrak{q}_j$ ist sogar *maximal* in dem Sinne, daß $\mathfrak{q}_j$ außer dem irrelevanten Ideal R_+ kein echtes homogenes Primoberideal besitzt.

Das Verschwindungsideal der Punktmenge Γ ist dann der Schnitt der $\mathfrak{q}_j$:

$$I_\Gamma = \{f \in R \mid \forall\, p \in \Gamma\colon f(p) = 0\} = \bigcap_{j=1}^{n} \mathfrak{q}_j.$$

Offenbar ist I_Γ homogen und gesättigt, weshalb I_Γ das Verschwindungsideal eines projektiven abgeschlossenen Unterschemas $Y = \operatorname{Proj} R/I_\Gamma$ von $\operatorname{Proj} R$ ist. Y ist sogar *reduziert*, da I_Γ Schnitt von Primidealen ist und somit R/I_Γ keine nilpotenten Elemente hat. Die Elemente von $Y = \operatorname{Proj} R/I_\Gamma$ entsprechen gemäß Satz 3.7 den Primidealen in $V_+(I_\Gamma)$, also den homogenen Primoberidealen von I_Γ. Das sind aber gerade die $\mathfrak{q}_j$. Mit $\mathfrak{p}_j := \mathfrak{q}_j/I_\Gamma$ hat man also:

$$Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \mathrel{\widehat{=}} \{p_1, \ldots, p_n\} = \Gamma \subset \mathbb{P}^m.$$

Da Y aus diskreten Punkten besteht, ist die Zariskitopologie auf Y die diskrete Topologie, d. h. jede Teilmenge ist offen und abgeschlossen. Die einzigen irreduziblen abgeschlossenen Mengen sind also die einpunktigen Mengen. Folglich ist Y ein nulldimensionales Unterschema im Sinne der nachfolgenden Definition 3.15. ◊

3.3. Nulldimensionale Schemata

Definition 3.15: *Die **Dimension** $\dim X$ eines topologischen Raumes $X \neq \emptyset$ ist das Supremum der Länge r aller Ketten $Y_0 \subset Y_1 \subset \ldots \subset Y_r$ aus (nichtleeren) irreduziblen abgeschlossenen echten Teilmengen Y_j von X.*

*Die **Dimension** eines Schemas ist (wie bei Varietäten) die Dimension des zugehörigen topologischen Raumes.*

Notiz 3.8: Für eine abgeschlossene Teilmenge Y in X gilt:

$$\dim Y \leq \dim X.$$

Die abgeschlossenen Unterschemata eines nulldimensionalen Schemas sind also selbst nulldimensional. ♢

Wie wir im Beispiel 3.4 gesehen haben, liefert eine endliche Punktmenge im $\mathbb{P}^m$ ein nulldimensionales projektives Schema. Umgekehrt gilt:

Satz 3.9: *Sei Y ein nulldimensionales projektives Unterschema von $X = \operatorname{Proj} R$. Dann ist Y eine endliche Menge mit der diskreten Topologie.*

Beweis: Da Y ein noetherscher topologischer Raum ist (☞ Notiz 3.2), wird Y gemäß Satz 3.3 auf Seite 28 überdeckt durch irreduzible abgeschlossene Teilmengen: $Y = Y_1 \cup \ldots \cup Y_r$.

Wäre nun $Y_i \cap Y_j \neq \emptyset$ für $i \neq j$, so gäbe es (☞ Satz 3.3) eine irreduzible abgeschlossene echte Teilmenge in Y_i, was $\dim Y = 0$ widerspricht. Also sind alle Y_j disjunkt und folglich offen. Sie bilden eine Basis der Topologie.

Jedes Y_j besitzt nach Satz 3.1 genau einen generischen Punkt $\mathfrak{p}_j$. Enthielte nun ein Y_j einen weiteren Punkt $\mathfrak{q}$, so wäre wegen der Eindeutigkeit $\overline{\{\mathfrak{q}\}} \neq Y_j$. Folglich wäre $\overline{\{\mathfrak{q}\}} \cap Y_j$ eine echte abgeschlossene Teilmenge von Y_j im Widerspruch zu $\dim Y = 0$. Also ist Y eine endliche Menge mit der diskreten Topologie. ■

Aus dem Satz 3.9 folgt unmittelbar:

Korollar 3.10: *Nulldimensionale projektive Schemata sind Hausdorff-Räume.*

Notiz 3.11: Sei $Y = \operatorname{Proj} R/I_Y$ nulldimensional, also $Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\}$, wobei jedes homogene Primideal $\mathfrak{p}_j$ ein Zariski-abgeschlossener Punkt ist. Gemäß dem schwachen Hilbertschen Nullstellensatz (vgl. Fulton, 1969, Kap. 1.7) haben dann alle Elemente aus $\mathfrak{p}_j$ eine gemeinsame Nullstelle $(p_{j_0}, \ldots, p_{j_m}) \in K^{m+1}$ (beachte: K ist algebraisch abgeschlossen). Da $\mathfrak{p}_j$ homogen ist, ist auch $p_j := (p_{j_0} : \ldots : p_{j_m}) \in \mathbb{P}^m$ gemeinsame Nullstelle. Folglich gilt:

$$\mathfrak{p}_j \subset \mathfrak{q}_j \diagup I_Y \quad \text{mit } \mathfrak{q}_j := \{f \in R \mid f(p_j) = 0\}.$$

Nun ist $\mathfrak{q}_j$ ein homogenes Primideal in R, d. h. $\mathfrak{q}_j / I_Y \in Y$. Wegen $\dim Y = 0$ geht das nur, wenn $\mathfrak{p}_j = \mathfrak{q}_j / I_Y$ gilt. Damit können wir dem Primideal $\mathfrak{p}_j$ eindeutig den Punkt p_j zuordnen. $I_Y = \bigcap_{j=1}^{n} \mathfrak{q}_j$ gilt allerdings nur dann, wenn Y reduziert ist. ◊

Notiz 3.12: Aus Beispiel 3.4 und Notiz 3.11 erhält man zusammenfassend:

Sei K ein algebraisch abgeschlossener Körper und $R = K[X_0, \ldots, X_m]$. Dann gilt für projektive Unterschemata $Y = \operatorname{Proj} R / I_Y$ von $\operatorname{Proj} R$:

$$\dim Y = 0 \iff Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \mathrel{\widehat{=}} \{p_1, \ldots, p_n\} = \Gamma \subset \mathbb{P}^m.$$

Falls $\dim Y = 0$, hat man für $\mathfrak{q}_j = \{f \in R \mid f(p_j) = 0\}$:

$$\mathfrak{p}_j = {}^{\mathfrak{q}_j}\!/_{I_Y}.$$

Verschiedene Unterschemata können zur gleichen Punktmenge Γ führen (vgl. Beispiel 3.3). Wenn Y reduziert ist, gilt $I_Y = \bigcap_{j=1}^{n} \mathfrak{q}_j = I_\Gamma$.

Bilden wir zu einer endlichen Punktmenge Γ ein Unterschema Y, so ist es nach Konstruktion (☞ Beispiel 3.4) bereits reduziert. ◊

Beispiel 3.5: Kommen wir noch einmal auf die durch $\langle Y \rangle$ und $\langle Y^2 \rangle$ gegebenen Unterschemata $(\mathcal{Y}_1, \mathcal{O}_{\mathcal{Y}_1})$ bzw. $(\mathcal{Y}_2, \mathcal{O}_{\mathcal{Y}_2})$ von $\operatorname{Proj} K[X, Y]$ zurück, die wir in Beispiel 3.3 auf Seite 32 betrachtet haben. In beiden Fällen enthält der topologische Raum genau ein Primideal $\mathfrak{p}$, nämlich das von Y erzeugte Ideal:

$$\mathcal{Y}_1 = \operatorname{Proj}\Big({}^{K[X,Y]}\!/_{\langle Y \rangle}\Big) = \Big\{ {}^{\langle Y \rangle}\!/_{\langle Y \rangle} \Big\} = \{\langle 0 \rangle\},$$
$$\mathcal{Y}_2 = \operatorname{Proj}\Big({}^{K[X,Y]}\!/_{\langle Y^2 \rangle}\Big) = \Big\{ {}^{\langle Y \rangle}\!/_{\langle Y^2 \rangle} \Big\}.$$

Also sind die globalen Schnitte gerade die Halme in diesem Punkt $\mathfrak{p}$:

$$\begin{aligned} \mathcal{O}_{\mathcal{Y}_1}(\mathcal{Y}_1) = \mathcal{O}_{\mathcal{Y}_1,\mathfrak{p}} &\cong \Big({}^{K[X,Y]}\!/_{\langle Y \rangle}\Big)_{(\mathfrak{p})} \cong K[X]_{(\langle 0 \rangle)} \\ &= \left\{ \frac{g}{h} \;\middle|\; \begin{array}{l} g \in K[X] \text{ und } h \in K[X] \setminus \langle 0 \rangle \\ \text{homogen vom gleichen Grad} \end{array} \right\} \cong K. \end{aligned}$$

$$\begin{aligned} \mathcal{O}_{\mathcal{Y}_2}(\mathcal{Y}_2) = \mathcal{O}_{\mathcal{Y}_2,\mathfrak{p}} &\cong \Big({}^{K[X,Y]}\!/_{\langle Y^2 \rangle}\Big)_{(\mathfrak{p})} = \Big({}^{K[X,Y]}\!/_{\langle Y^2 \rangle}\Big)_{(\langle Y \rangle / \langle Y^2 \rangle)} \\ &= \left\{ \frac{g}{h} \;\middle|\; \begin{array}{ll} g = \alpha X^i + \beta Y X^{i-1} & \text{mit } \alpha, \beta \in K, \\ h = \gamma X^i & \text{mit } \gamma \in K \end{array} \right\} \\ &= \left\{ \frac{\alpha}{\gamma} + \frac{\beta}{\gamma} \frac{Y}{X} \;\middle|\; \alpha, \beta, \gamma \in K \right\} \cong K^2. \end{aligned}$$

Es gilt also $\dim_K \mathcal{O}_{\mathcal{Y}_2}(\mathcal{Y}_2) = 2 > {}^{\#}\mathcal{Y}_2$ für das nicht reduzierte Schema $\mathcal{Y}_2$ und $\dim_K \mathcal{O}_{\mathcal{Y}_1}(\mathcal{Y}_1) = 1 = {}^{\#}\mathcal{Y}_1$ für das reduzierte Schema $\mathcal{Y}_1$. ◊

Das Beispiel zeigt, daß die Aussage „$\dim_K \mathscr{O}_Y(Y) = {}^{\#}Y$“ des nächsten Satzes ohne die Voraussetzung „reduziert“ falsch ist.

Satz 3.13: *Sei $Y = \operatorname{Proj} R/I_Y$ ein nulldimensionales reduziertes projektives Unterschema von $X = \operatorname{Proj} R$. Dann bilden die globalen Schnitte $\mathscr{O}_Y(Y)$ einen endlichdimensionalen K-Vektorraum, und für dessen Dimension gilt:*

$$\dim_K \mathscr{O}_Y(Y) = {}^{\#}Y =: n, \qquad \text{also: } \Gamma(Y, \mathscr{O}_Y) \cong K^n.$$

Bemerkung: Ist Y ein durch eine endliche Punktmenge $\Gamma \subset \mathbb{P}^m_K$ gegebenes Unterschema, so gilt die Aussage des Satzes 3.13 auch für einen nicht algebraisch abgeschlossenen Körper K. Das Verschwindungsideal I_Y wird nämlich so gewählt, daß Y schon reduziert ist.

Beweis (Satz 3.13): Wie oben sei $Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \mathrel{\widehat{=}} \{p_1, \ldots, p_n\} = \Gamma \subset \mathbb{P}^m$. Wir setzen $S := R/I_\Gamma$ (hier gilt $I_\Gamma = I_Y$, denn Y ist reduziert). Da die einzelnen Primideale $\mathfrak{p}_k$ auch offene Mengen sind, können wir betrachten:

$$\mathscr{O}_Y(\{\mathfrak{p}\}) = \{\sigma\colon \{\mathfrak{p}\} \to S_{(\mathfrak{p})}\} \cong S_{(\mathfrak{p})} \cong \mathscr{O}_{Y,\mathfrak{p}}.$$

Das Garbenaxiom (G2) (☞ Definition 3.5 auf Seite 28) liefert nun für offenes $U \subset Y$:

$$\mathscr{O}_Y(U) \cong \prod_{\mathfrak{p}\in U} S_{(\mathfrak{p})} \cong \prod_{\mathfrak{p}\in U} \mathscr{O}_{Y,\mathfrak{p}}.$$

Insbesondere ist $\mathscr{O}_Y(Y) \cong \prod_{j=1}^n S_{(\mathfrak{p}_j)} \cong \prod_{j=1}^n \mathscr{O}_{Y,\mathfrak{p}_j}$; wir sind also fertig, falls für $k \in \{1, \ldots, n\}$ stets gilt:

$$\dim_K S_{(\mathfrak{p}_k)} = 1 \quad \text{oder äquivalent:} \quad \forall\, \frac{g}{h} \in S_{(\mathfrak{p}_k)}\colon \exists\, \lambda \in K\colon \frac{g}{h} = \lambda \cdot \frac{1}{1}.$$

Sei daher $\frac{g}{h} \in S_{(\mathfrak{p}_k)}$ gegeben, das heißt, $g \in S$, $h \in S \setminus \mathfrak{p}_k$ und g, h homogen vom selben Grad. Wegen $\mathfrak{p}_k = \{f \in S \mid f \text{ homogen}, f(p_k) = 0\}$ ist $h(p_k) \neq 0$.

Setze $\lambda := \frac{g(p_k)}{h(p_k)} \in K$. Wähle $t = 1$, falls $n = 1$, andernfalls $t \in \bigcap_{i\neq k} \mathfrak{p}_i, t \notin \mathfrak{p}_k$ (ein solches t existiert, da zwei Primideale wegen $\dim Y = 0$ nicht echt ineinander enthalten sein können). Dann ist $t(p_k) \neq 0$ und $t(p_i) = 0$ für alle $i \neq k$, also:

$$\forall\, j\colon t(g - \lambda h)(p_j) = 0 \quad \overset{Y \text{ reduziert}}{\Longleftrightarrow} \quad t(g - \lambda h) \equiv 0 \text{ in } S = R/I_\Gamma$$
$$\Longrightarrow \quad \frac{g}{h} = \lambda \cdot \frac{1}{1}.$$

Offenbar ist $S_{(\mathfrak{p})} \cong \mathscr{O}_{Y,\mathfrak{p}}$ für jedes $\mathfrak{p} \in Y$ eindimensional, so daß die Behauptung $\dim_K \mathscr{O}_Y(Y) = {}^{\#}Y$ folgt. ∎

Korollar 3.14: *Sei K algebraisch abgeschlossen. Dann sind die Halme $\mathscr{O}_{Y,\mathfrak{p}}$ eines nulldimensionalen reduzierten Unterschemas Y von $X = \operatorname{Proj} K[X_0, \ldots, X_m]$ eindimensionale K-Vektorräume.*

3.4. Restschemata und vollständiger Durchschnitt von Hyperflächen

3.4.1. Restschemata

Wir haben gesehen, daß über einem algebraisch abgeschlossenen Körper ein nulldimensionales Unterschema Y von Proj R einer endlichen Punktmenge im $\mathbb{P}^m$ entspricht. Ein Unterschema von Y ist dann eine Teilmenge $Y' \subset Y$. Ein *Restschema* Y'' zu Y' sollte nun so etwas sein wie eine komplementäre Teilmenge. Daher wären die beiden folgenden Eigenschaften für ein *Restschema* wünschenswert:

- ${}^{\#}Y' + {}^{\#}Y'' = {}^{\#}Y$.
- Die Bildung von Restschemata ist symmetrisch, d. h. ist Y'' das Restschema zu Y', so ist Y' das Restschema zu Y''.

Definition 3.16: *Sei Y ein nulldimensionales Schema mit Koordinatenring R/I_Y, und sei $Y' \subset Y$ ein abgeschlossenes Unterschema, gegeben durch das Ideal $I_{Y'} \subset R$ ($I_{Y'} \supset I_Y$). Als **Restschema** von Y zu Y' bezeichnen wir das Unterschema Y'', definiert durch das Ideal:*

$$I_{Y''}/I_Y = \operatorname{Ann}\left(I_{Y'}/I_Y\right) \subset R/I_Y.$$

*Dabei verstehen wir unter dem **Annulator** eines Ideals I im Ring A das Ideal:*

$$\operatorname{Ann}(I) = \{f \in A \mid f \cdot g = 0 \text{ für alle } g \in I\}.$$

Im allgemeinen erfüllt ein Restschema allerdings nicht die oben geforderten Eigenschaften. Wir betrachten noch einmal die durch $\langle Y \rangle$ und $\langle Y^2 \rangle$ gegebenen einpunktigen Unterschemata $\mathcal{Y}_1$ bzw. $\mathcal{Y}_2$ von Proj $K[X, Y]$ aus den Beispielen 3.3 und 3.5. Hier ist $\mathcal{Y}_1$ Restschema zu sich selbst in $\mathcal{Y}_2$, denn $\operatorname{Ann}\big(\langle Y \rangle / \langle Y^2 \rangle\big) = \langle Y \rangle / \langle Y^2 \rangle$. Wir haben also ${}^{\#}\mathcal{Y}_1 + {}^{\#}\mathcal{Y}_1 = 2 > 1 = {}^{\#}\mathcal{Y}_2$.

Im Artikel von Eisenbud u. a. (1996, S. 311-313) wird gezeigt, daß beide Eigenschaften gelten, falls Y ein *vollständiger Durchschnitt* von *Hyperflächen* ist.

3.4.2. Vollständiger Durchschnitt von Hyperflächen

Definition 3.17: *Sei $f \in R = K[X_0, \ldots, X_m]$ ein nicht konstantes homogenes Polynom vom Grad a. Die Menge der homogenen Primideale, die f enthalten, bildet dann eine **projektive Hyperfläche** H vom Grad a:*

$$H := V_+(f) = \{\mathfrak{p} \in \operatorname{Proj} R \mid f \in \mathfrak{p}\} \cong \operatorname{Proj} R/\langle f \rangle.$$

Die projektiven Hyperflächen vom Grad a entsprechen also dem Vektorraum R_a der homogenen Polynome vom Grad a.

Um einen *vollständigen Durchschnitt* von Hyperflächen zu definieren, müssen wir wissen, was die *Codimension* eines abgeschlossenen Unterschemas ist. Wir betrachten nur Unterschemata von $X = \operatorname{Proj} R$ zum Polynomring $R = K[X_0, \ldots, X_m]$, also Unterschemata eines *integren* Schemas *vom endlichen Typ über K*.[†] Hier läßt sich die Codimension einer abgeschlossenen Teilmenge $Y \subset X$ folgendermaßen definieren (vgl. Hartshorne, 1977, S. 95, Aufgabe 3.20(d)):

$$\operatorname{codim}(Y, X) := \dim X - \dim Y.$$

Insbesondere gilt dies für abgeschlossene Unterschemata. Da $\operatorname{Proj} K[X_0, \ldots, X_m]$ die Dimension m hat, ist m die Codimension eines nulldimensionalen Unterschemas Y von $\operatorname{Proj} K[X_0, \ldots, X_m]$.

Der Schnitt von Schemata ist definitionsgemäß (vgl. Kunz, 1997, S. 114):

$$\operatorname{Proj}\left(R/I_1\right) \cap \operatorname{Proj}\left(R/I_2\right) := \operatorname{Proj}\left(R/(I_1 + I_2)\right).$$

Jetzt können wir den vollständigen Durchschnitt von Hyperflächen erklären (vgl. Hartshorne, 1977, S. 188, Aufgabe 8.4):

Definition 3.18: *Ein abgeschlossenes Unterschema Y von $X = \operatorname{Proj} R$ heißt* ***vollständiger Durchschnitt****, wenn eine der folgenden äquivalenten Bedingungen erfüllt ist:*

- *Das Verschwindungsideal I_Y von Y kann von $r = \operatorname{codim}(Y, X)$ Elementen erzeugt werden.*
- *Es gibt Hyperflächen $H_1, \ldots, H_r$, so daß $Y = H_1 \cap \ldots \cap H_r$ im Schemasinne gilt.*

Notiz 3.15: Ist Y ein nulldimensionaler vollständiger Durchschnitt

$$Y = H_1 \cap \ldots \cap H_m = V_+(f_1) \cap \ldots \cap V_+(f_m),$$

so besteht Y aus endlich vielen abgeschlossenen Punkten $\mathfrak{p}_j$, welche gerade die homogenen Primoberideale des Verschwindungsideals $I_Y = \sum_{i=1}^{m} \langle f_i \rangle = \langle f_1, \ldots, f_m \rangle$ sind.

Da der Grundkörper algebraisch abgeschlossen ist, sind die Primideale $\mathfrak{p}_j$ nach Notiz 3.11 auf Seite 34 durch Punkte $p_j \in \mathbb{P}^m$ gegeben:

$$\mathfrak{p}_j = \{f \in R \mid f(p_j) = 0\}.$$

Die p_j sind also die gemeinsamen Nullstellen der Erzeuger f_i von I_Y, denn jede gemeinsame Nullstelle gibt ein homogenes Primoberideal von I_Y.

[†] Daß $\operatorname{Proj} R$ integer ist, haben wir bereits in Beispiel 3.2 auf Seite 31 behandelt. $\operatorname{Proj} R$ ist zudem ein Schema *vom endlichen Typ über K*, weil $\operatorname{Proj} R$ eine endliche Überdeckung aus Spektren von ringendlich erzeugten K-Algebren hat (☞ Notiz 3.6 auf Seite 31).

Im Varietätensinne versteht man unter einer *projektiven Hyperfläche* vom Grad a die Menge H^V aller Nullstellen eines nicht konstanten homogenen Polynoms $f \in K[X_0, \ldots, X_m]$ vom Grad a:

$$H^V := \{p \in \mathbb{P}^m \mid f(p) = 0\}, \quad \text{kurz: } H^V : f = 0.$$

Der Schnitt von Hyperflächen ist hier also die gemeinsame Nullstellenmenge der Polynome, welche die Hyperflächen erzeugen.

Insgesamt haben wir für einen nulldimensionalen vollständigen Durchschnitt von Hyperflächen folgenden Zusammenhang:

$$H_1 \cap \ldots \cap H_m = Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \mathrel{\widehat{=}} \{p_1, \ldots, p_n\} = \Gamma = H_1^V \cap \ldots \cap H_m^V.$$

Das heißt, ein nulldimensionaler vollständiger Durchschnitt stimmt mit der gewohnten Vorstellung eines Schnittes von Hyperflächen überein!

Die Anzahl der Elemente des Schnittschemas $Y = H_1 \cap \ldots \cap H_m$ ist also gleich der Anzahl der gemeinsamen Nullstellen der Polynome f_i, und diese ist gemäß dem Satz von Bézout nach oben durch $\prod_{i=1}^m \operatorname{grad} f_i$ beschränkt (vgl. Kunz, 1997, S. 187). Wegen $\operatorname{grad} H_i = \operatorname{grad} f_i$ gilt daher: ${}^{\#}Y \leq \prod_{i=1}^m \operatorname{grad} H_i$.

Ist das Unterschema Y zusätzlich reduziert, so sind alle Halme $\mathcal{O}_{Y,\mathfrak{p}}$ eindimensional (☞ Korollar 3.14 auf Seite 36). Dann enthält Y die maximal mögliche Anzahl von Elementen, d. h. ${}^{\#}Y = \prod_{i=1}^m \operatorname{grad} H_i$ (vgl. Kunz, 1997, S. 189). ◊

Im Zusammenhang mit Hyperflächen wollen wir nun noch eine Sprechweise einführen, die wir benutzen werden, um den Satz von Cayley-Bacharach zu formulieren (☞ Satz 3.16 auf Seite 41).

Weil ein Punkt $p \in \mathbb{P}^m$ stets ein homogenes Primideal $\mathfrak{p} \in R$ definiert, können wir auch im schematheoretischen Bild davon sprechen, daß eine Hyperfläche H den Punkt p enthält; für $H = V_+(f)$ ist dann $f(p) = 0$.

In der Algebraischen Geometrie interessiert man sich für die Familien von Hyperflächen vom Grad a, die eine gegebene Menge $\Gamma \subset \mathbb{P}^m$ von n verschiedenen Punkten enthalten, also für den Kern $(I_\Gamma)_a$ der Auswerteabbildung (☞ Kapitel 2.2)

$$e_a(\Gamma) : R_a \to K^n.$$

Gemäß der Dualitätstheorie der linearen Algebra läßt sich ein Untervektorraum durch seinen Annulator beschreiben. Wegen $R_a / \operatorname{Ker} e_a(\Gamma) \cong \operatorname{Im} e_a(\Gamma)$ gilt hier:

$$\dim \operatorname{Ann}(I_\Gamma)_a = \operatorname{codim}(I_\Gamma)_a = \operatorname{codim} \operatorname{Ker} e_a(\Gamma) = \dim \operatorname{Im} e_a(\Gamma) \leq n = {}^{\#}\Gamma.$$

Das führt zu folgender Sprechweise:

Definition 3.19: *Man sagt: „Γ liefert ℓ Bedingungen auf Hyperflächen vom Grad a“, wenn die Hyperflächen vom Grad a, die Γ enthalten, einen Untervektorraum der Codimension ℓ bilden; in Formeln:*

$$\Gamma \text{ liefert } \ell \text{ Bedingungen auf } R_a \iff \ell = \operatorname{codim}(I_\Gamma)_a = H_\Gamma(a).$$

Dabei ist $H_\Gamma(a)$ die Hilbertfunktion von Γ (☞ Definition 2.5). Die Differenz

$$n - \ell = \dim\left(K^n \big/ \operatorname{Im} e_a(\Gamma)\right) = \dim \operatorname{Coker} e_a(\Gamma)$$

mißt dann das „Unvermögen von Γ, unabhängige Bedingungen auf Hyperflächen vom Grad a zu liefern“.

3.5. Der Satz von Cayley-Bacharach

Benannt ist der Satz nach Arthur Cayley (1821–1895) und I. Bacharach, die sich im 19. Jahrhundert mit Schnitten von Kurven in der projektiven Ebene $\mathbb{P}^2$ beschäftigten. Bereits im 4. Jahrhundert nach Christus formulierte und bewies Pappus von Alexandria eine erste Version dieses Satzes (☞ Satz 3.17). Doch erst mit der von Gérard Desargues (1591–1661) im Jahre 1639 begründeten Theorie des projektiven Raumes ist der Satz in allen Spezialfällen gültig. Etwa zur gleichen Zeit interessierte man sich verstärkt für *Kegelschnitte*, da Johannes Kepler (1571–1630) diese benutzte, um die Planetenbewegung um die Sonne zu beschreiben (vgl. Demtröder, 2003, S. 65). So verwundert es nicht, daß Blaise Pascal (1623–1662) im Jahre 1640 den Satz von Pappus für Kegelschnitte formulierte (☞ Satz 3.18); das hierbei auftretende, in einen Kegelschnitt einbeschriebene Sechseck nannte Pascal *Hexagrammum Mysticum* (vgl. Struik, 1986, S. 163). Einfacher und trotzdem stärker als der Satz von Pascal ist das von Michel Chasles (1793–1880) im Buch „Traité des sections coniques“ (Chasles, 1865) publizierte Resultat (☞ Satz 3.19).

Kegelschnitte sind Hyperflächen vom Grad 2 im $\mathbb{P}^2$, also *Ellipsen*, *Parabeln* oder *Hyperbeln*, wie in Abbildung 2 auf der nächsten Seite gezeigt, oder zwei sich schneidende Geraden. Die entarteten Fälle des einzelnen Punktes bzw. der Doppelgerade wollen wir hier nicht als Kegelschnitt ansehen. Systematisch wurden Kegelschnitte zum ersten Mal von Apollonius von Perga (ca. 262–190 vor Christus) betrachtet, „den man [daher] vielleicht als den frühesten Vertreter der algebraischen Geometrie betrachten kann“ (aus Kunz, 1997, S. 3). Hyperflächen, die Nullstellengebilde von Polynomen 3. Grades sind, nennt man auch *Kubiken*.

Eines ausführliche Betrachtung des Satzes von Cayley-Bacharach ist im Artikel „Cayley-Bacharach Theorems and Conjectures“ von Eisenbud, Green und Harris (1996) zu finden. Insgesamt neun Versionen des Satzes sind hier angegeben – von

Pappus bis hin zu modernen Formulierungen über Schemata und Gorensteinringe. Darüber hinaus werden Vermutungen über mögliche weitergehende Verallgemeinerungen angestellt. Wir werden die in jenem Artikel notierte Version für Schemata verwenden.

Satz 3.16 (Cayley-Bacharach)**:** *Seien $H_1, \ldots, H_m$ Hyperflächen vom Grad $d_1, \ldots, d_m$ im $\mathbb{P}^m$ mit nulldimensionalem vollständigem Durchschnitt $Y = H_1 \cap \ldots \cap H_m$. Ferner seien Y' und Y'' Unterschemata von Y, die zueinander jeweils Restschemata in Y sind. Setze $s = \sum d_i - m - 1$.*

Sei δ die Dimension der Familie von Hyperflächen vom Grad $a \in \{0, \ldots, s\}$, die Y' enthalten (modulo denen, die ganz Y enthalten): $\delta = \dim\big((I_{Y'})_a / (I_Y)_a\big)$.

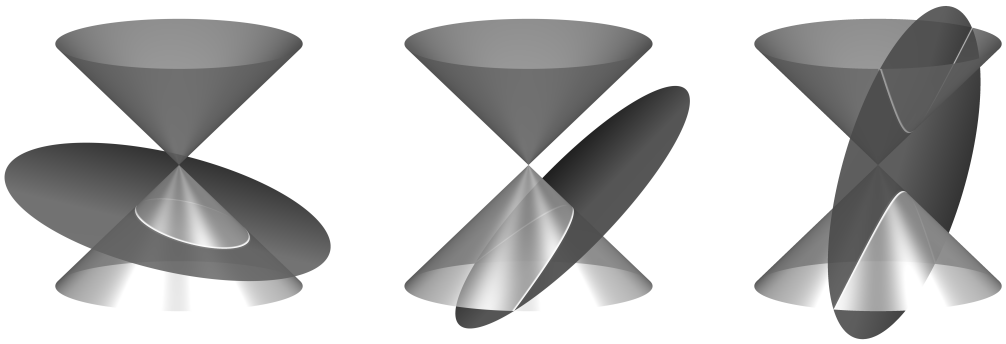
Diese Dimension drückt dann gerade das Unvermögen von Y'' aus, unabhängige Bedingungen auf Hyperflächen vom Grad $s - a$ zu liefern:

$$\delta = \dim\left(\frac{(I_{Y'})_a}{(I_Y)_a}\right) = {}^{\#}(Y'') - \operatorname{codim}(I_{Y''})_{s-a} = \dim \operatorname{Coker} e_{s-a}(Y'').$$

Beweis: Siehe Eisenbud u. a. (1996, S. 314, CB 7). ∎

Falls $\dim \operatorname{Coker} e_{s-a}(Y'') = 0$ gilt, ist also $\dim(I_{Y'})_a = \dim(I_Y)_a$, d. h. Y und Y' liefern gleich viele Bedingungen auf Kurven vom Grad a. Das wiederum bedeutet, daß Hyperflächen, die Y' enthalten, bereits ganz Y enthalten.

Zur Veranschaulichung des Satzes von Cayley-Bacharach leiten wir aus ihm die oben erwähnten Sätze von Pappus, Pascal und Chasles ab.



Ellipse Parabel Hyperbel

Abbildung 2: Kegelschnitte (Bilder erstellt mit `surfex` von Holzer u. Labs, 2008)

3.5.1. Die Sätze von Pappus, Pascal und Chasles

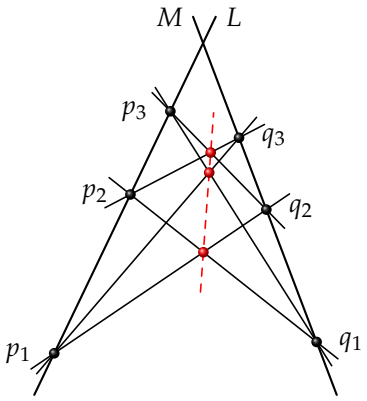


Abbildung 3: Der Satz von Pappus

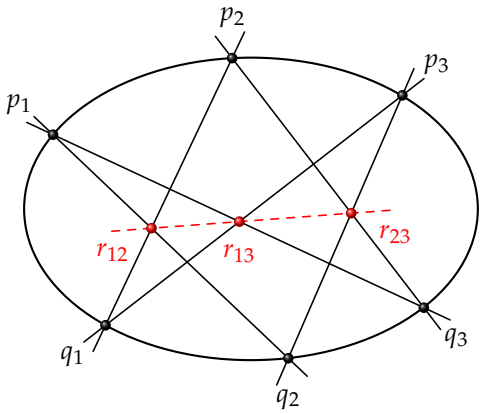


Abbildung 4: Der Satz von Pascal

Satz 3.17 (Pappus)**:** *Seien L und M zwei Geraden in einer Ebene, auf denen jeweils drei verschiedene Punkte p_1, p_2, p_3 bzw. q_1, q_2, q_3 so gewählt seien, daß keiner der Punkte in $L \cap M$ liegt. Dann sind die drei Schnittpunkte r_{ij}, $i \neq j$, der Geraden $\overline{p_i q_j}$ und $\overline{p_j q_i}$ kollinear (☞ Abbildung 3).*

Satz 3.18 (Pascal)**:** *Wenn ein Sechseck einem Kegelschnitt in der projektiven Ebene $\mathbb{P}^2$ einbeschrieben ist, dann schneiden sich die gegenüberliegenden Seiten des Sechsecks in drei kollinearen Punkten (☞ Abbildung 4).*

Satz 3.19 (Chasles)**:** *Seien $C_1, C_2 \subset \mathbb{P}^2$ zwei Kubiken, die sich in neun Punkten schneiden. Enthält eine Kubik $C \in \mathbb{P}^2$ acht der neun Punkte, so enthält sie auch den letzten.*

Beweis (Chasles): Seien C_1, C_2 zwei Kubiken im $\mathbb{P}^2$ mit $\Gamma := C_1 \cap C_2 = \{p_1, \ldots, p_9\}$. Ohne Einschränkung sei $\Gamma' := \{p_1, \ldots, p_8\}$ und $\Gamma'' := \{p_9\}$. Da $I_{\Gamma''}$ ein echtes Ideal ist, hat man: $\dim_K(I_{\Gamma''})_0 = \dim_K(K \cap I_{\Gamma''}) = 0$, weshalb nach dem Satz von Cayley-Bacharach mit $s = 3$, $a = 3$ gilt:

$$\dim\left({}^{(I_{\Gamma'})_3}\!/_{(I_\Gamma)_3}\right) = {}^{\#}(\Gamma'') - \operatorname{codim}(I_{\Gamma''})_{3-3} = 1 - 1 = 0.$$

Offenbar gehören bereits alle Punkte von Γ zu einer Kubik, wenn diese 8 der 9 Punkte enthält. ■

Beweis (Pascal und Pappus): Betrachtet man die Geraden L und M als Kegelschnitt, so ist der Satz von Pappus ein Spezialfall des Satzes von Pascal.

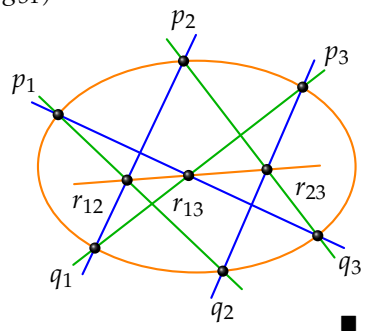
Für den Beweis des Satzes von Pascal sei ein Kegelschnitt C (projektive Hyperfläche vom Grad 2) mit einbeschriebenem Sechseck gegeben, wobei die Eckpunkte des Sechsecks mit $p_1, p_2, p_3, q_1, q_2, q_3$ bezeichnet seien. Die Geraden $\overline{p_iq_j}$ durch p_i und q_j seien gegeben durch homogene Polynome g_{ij} ersten Grades, also $\overline{p_iq_j}\colon g_{ij} = 0$. Für $i \neq j$ bezeichne r_{ij} den Schnittpunkt der Geraden $\overline{p_iq_j}$ mit $\overline{p_jq_i}$.

Mit diesen Bezeichnern schneiden sich die Kubiken

$$C_1 = \overline{p_1q_3} \cup \overline{p_2q_1} \cup \overline{p_3q_2}\colon (g_{13} \cdot g_{21} \cdot g_{32}) = 0,$$
$$C_2 = \overline{p_1q_2} \cup \overline{p_2q_3} \cup \overline{p_3q_1}\colon (g_{12} \cdot g_{23} \cdot g_{31}) = 0$$

in den neun Punkten $p_1, p_2, p_3, q_1, q_2, q_3, r_{12}, r_{13}, r_{23}$.

Außerdem bildet der Kegelschnitt C zusammen mit der Gerade $\overline{r_{12}r_{23}}$ eine Kubik, die acht der neun Punkte enthält. Nach dem Satz von Chasles gehören sogar alle Punkte zu dieser Kubik, d. h. $r_{13} \in C \cup \overline{r_{12}r_{23}}$. Wegen $r_{13} \notin C$ muß gelten: $r_{13} \in \overline{r_{12}r_{23}}$, d. h. die Schnittpunkte r_{ij} sind kollinear.



■

4. Abschätzung von Minimalabständen von Auswerte-Codes

Wir kommen nun zu unserem Hauptresultat, nämlich der Abschätzung des Minimalabstands von Auswerte-Codes. Sei dazu $Y = H_1 \cap \ldots \cap H_m$ ein nulldimensionaler reduzierter vollständiger Durchschnitt von Hyperflächen H_i vom Grad d_i; setze $s = \sum d_i - m - 1$. Wie wir in Notiz 3.12 auf Seite 35 gesehen haben, entspricht das abgeschlossene Unterschema Y einer Punktmenge $\Gamma = \{p_1, \ldots, p_n\} \subset \mathbb{P}^m_{\mathbb{F}}$. Um Codes zu Γ bilden zu können, seien diese Punkte $\mathbb{F}_q$-rational.

$C(\Gamma)_a$ sei der in Kapitel 2.2 definierte Auswerte-Code zu Γ. Sein Minimalabstand unterliegt dann folgender Schranke:

Satz 4.1: *$C(\Gamma)_a$ hat Minimalabstand $d \geq s - a + 2$, falls $1 \leq a \leq s$.*

Bemerkung: Wie in Notiz 3.15 erläutert, sind die Punkte aus $\Gamma \mathrel{\widehat{=}} Y = H_1 \cap \ldots \cap H_m$ die gemeinsamen Nullstellen im $\mathbb{P}^m$ der Polynome f_i, welche die Hyperflächen H_i definieren. Da Y reduziert ist, ist die Anzahl (mit Vielfachheiten gezählt) dieser gemeinsamen Nullstellen gleich dem Produkt der Grade d_i der f_i (☞ Notiz 3.15), also ${}^{\#}\Gamma = \prod d_i$. Für $1 \leq a \leq s = \sum d_i - m - 1$ gilt somit:

$$ {}^{\#}\Gamma - (s - a + 1) \geq {}^{\#}\Gamma - s = \prod d_i - (\sum d_i - m - 1) \geq 0. $$

Beweis (Satz 4.1): Gemäß der Vorbemerkung ist $\ell := {}^{\#}\Gamma - (s - a + 1) \geq 0$. Zu einem beliebigem abg. Unterschema Γ' von Γ mit $\ell = {}^{\#}\Gamma'$ sei Γ'' das Restschema. Dann gilt:

$$ {}^{\#}\Gamma'' = {}^{\#}\Gamma - {}^{\#}\Gamma' = s - a + 1. $$

Offenbar ist $s - a = {}^{\#}\Gamma'' - 1$, weshalb mit Lemma 2.7 auf Seite 13 und dem Satz von Cayley-Bacharach (☞ Satz 3.16) folgt:

$$ \dim \operatorname{Coker} e_{s-a}(\Gamma'') = 0 \iff \dim(I_\Gamma)_a = \dim(I_{\Gamma'})_a \iff H_\Gamma(a) = H_{\Gamma'}(a). $$

Satz 2.10 liefert nun die Behauptung: $d \geq n - \ell + 1 = {}^{\#}\Gamma - {}^{\#}\Gamma' + 1 = s - a + 2$. ∎

Korollar 4.2: *$C(\Gamma)_a$ ist genau dann ein MDS-Code, wenn für jede Teilmenge $\Gamma'' \subset \Gamma$ mit ${}^{\#}\Gamma'' = \dim \operatorname{Coker} e_a(\Gamma)$ gilt:* $\dim \operatorname{Coker} e_{s-a}(\Gamma'') = 0$.

Beweis: $C(\Gamma)_a$ ist ein MDS-Code

$$ \begin{aligned} &\overset{\text{Satz 2.11}}{\iff} \forall\, \Gamma' \subset \Gamma \text{ mit } {}^{\#}\Gamma' = k = \dim C(\Gamma)_a \colon H_\Gamma(a) = H_{\Gamma'}(a) \\ &\iff \forall\, \Gamma' \subset \Gamma \text{ mit } {}^{\#}\Gamma' = k = \dim C(\Gamma)_a \colon \dim(I_\Gamma)_a = \dim(I_{\Gamma'})_a \\ &\underset{\text{Satz 3.16}}{\iff} \forall\, \Gamma'' \subset \Gamma \text{ mit } {}^{\#}\Gamma'' = \underbrace{\dim \operatorname{Coker} e_a(\Gamma)}_{= \dim \mathbb{F}_q^n - \dim C(\Gamma)_a = n - k} \colon \dim \operatorname{Coker} e_{s-a}(\Gamma'') = 0. \end{aligned} $$

∎

4.1. Beispiele

Abschließend betrachten wir drei Beispiele.

Beispiel 4.1: Wir betrachten die Hyperebenen $H_j := V_+(X_j)$ für $1 \leq j < m$ und $H_m := V_+(X_m^q - X_0^{q-1}X_m)$. Der Durchschnitt dieser Hyperflächen ist nulldimensional, vollständig und enthält genau die $\mathbb{F}_q$-rationalen Punkte (☞ Notiz 3.15 auf Seite 38) der Geraden $L := H_1 \cap \ldots \cap H_{m-1}$:

$$\Gamma := H_1 \cap \ldots \cap H_m = \{(r_0 : 0 : \ldots : 0 : r_m) \in \mathbb{P}_{\mathbb{F}}^m \mid r_0, r_m \in \mathbb{F}_q, r_0 \neq 0\}.$$

Wie wir in Beispiel 2.1 auf Seite 16 gesehen haben, ist der zu Γ gebildete Auswerte-Code $C(\Gamma)_a$ ein verallgemeinerter Reed-Solomon-Code der Länge $n = q$ und der Dimension $k = a + 1$.

Da der Grad einer Hyperfläche der Grad des definierenden Polynoms ist, haben wir hier: $s = \left(\sum_{j=1}^m \operatorname{grad} H_j\right) - m - 1 = (m-1) + q - m - 1 = q - 2$. Nach Satz 4.1 erfüllt der Minimalabstand d von $C(\Gamma)_a$ für $1 \leq a \leq s = q - 2$ dann:

$$d \geq s - a + 2 = q - a = n - k + 1.$$

Zusammen mit der Singleton-Schranke (☞ Satz 2.2) haben wir also $d = n - k + 1$, weshalb der verallgemeinerte Reed-Solomon-Code $C(\Gamma)_a$ ein MDS-Code ist. ◊

Beispiel 4.2: Der in Kapitel 2.3 eingeführte verallgemeinerte Reed-Muller-Code $GRM(a, m)$ mit $a \in \mathbb{N}$, $a \leq m(q-1)$, ist der Auswerte-Code zu $\Gamma \cong \mathbb{A}^m(\mathbb{F}_q)$, vergleiche Notiz 2.12 auf Seite 14. Weil wir Γ auch als die Menge der $\mathbb{F}_q$-rationalen Punkte in $\mathbb{A}_{\mathbb{F}}^m \subset \mathbb{P}_{\mathbb{F}}^m$ auffassen können, läßt sich Γ als projektiver vollständiger Durchschnitt realisieren:

$$\Gamma = H_1 \cap \ldots \cap H_m \quad \text{mit } H_j := V_+(X_j^q - X_0^{q-1}X_j).$$

Hierfür ergibt sich $s = m \cdot q - m - 1 = m(q-1) - 1$. Sei nun $a \leq s$; wir können a dann schreiben als $a = \ell(q-1) + r$ mit $\ell < m$ und $0 \leq r < q - 1$.

Gemäß Satz 4.1 ist der Minimalabstand d von $C(\Gamma)_a = GRM(a, m)$ beschränkt:

$$\begin{aligned} d \geq s - a + 2 &= \big(m(q-1) - 1\big) - \big(\ell(q-1) + r\big) + 2 \\ &= (m - \ell)(q-1) - r + 1. \end{aligned}$$

Der exakte Minimalabstand ist $d = (q-r)q^{m-1-\ell}$ (☞ Satz 2.13 auf Seite 15).

- Für $\ell = m - 1$ und $r = 0$ liefert unsere Schranke also den tatsächlichen Minimalabstand $d = q$; hier sind $a = (m-1)(q-1)$ und $s = m(q-1) - 1$.
- Ist dagegen $\ell < m - 1$, so ist unsere untere Schranke wesentlich kleiner als der exakte Minimalabstand. ◊

Dies Beispiel zeigt, daß unser Hauptresultat im allgemeinen eine gute Abschätzung für den Minimalabstand liefert, wenn a etwa so groß wie s ist; die Schranke ist dann allerdings klein. Andernfalls ($a \ll s$) wird die Schranke größer, liefert aber eine schlechtere Abschätzung.

Beispiel 4.3: Im letzten Beispiel vergleichen wir Auswerte-Codes $C(\Gamma)_a$ mit Hermiteschen Codes C_r über $\mathbb{F}_{q^2}$, die wir in Beispiel 2.5 auf Seite 24 behandelt haben. Dabei haben wir gesehen, daß die projektive glatte Kurve

$$\mathcal{X}_q = V(f) \subset \mathbb{P}^2_{\mathbb{F}} \quad \text{mit } f(X,Y,Z) = Y^{q+1} - X^q Z - X Z^q$$

den eindeutig bestimmten unendlich fernen Punkt $x_\infty := (1:0:0)$ enthält sowie q^3 affine $\mathbb{F}_{q^2}$-rationale Punkte $x_j = (\alpha_j : \beta_j : 1)$, wobei $\beta_j^{q+1} = \alpha_j^q + \alpha_j$ gilt.

Die Auswerte-Codes $C(\Gamma)_a$ bilden wir hier zur Punktmenge

$$\Gamma = \mathcal{X}_q \cap V(h) \mathrel{\widehat{=}} V_+(f) \cap V_+(h)$$

in der projektiven Ebene $\mathbb{P}^2_{\mathbb{F}}$ mit

$$h(X,Y,Z) = \prod_{\substack{\alpha \in \mathbb{F}_{q^2} \\ \alpha^q + \alpha \neq 0}} (X - \alpha Z).$$

Dann besteht Γ aus den $n = q^3 - q$ affinen $\mathbb{F}_{q^2}$-rationalen Punkten $x_j = (\alpha_j : \beta_j : 1)$ auf $\mathcal{X}_q$ mit $\beta_j \neq 0$.

Für die Grade der Gleichungen, die Γ definieren, gilt $d_1 := \operatorname{grad} f = q + 1$ und andererseits gemäß Lemma A.1 im Anhang $d_2 := \operatorname{grad} h = q^2 - q$; deswegen ist $s = d_1 + d_2 - 3 = q^2 - 2$.

Nach unserem Hauptresultat(☞ Satz 4.1) ist der Minimalabstand von $C(\Gamma)_a$ nach unten beschränkt durch $d \geq s - a + 2 = q^2 - a$. Die Dimension k_a ist über die Hilbertfunktion (☞ Satz 2.8) gegeben zu: $k_a = \dim C(\Gamma)_a = H_\Gamma(a)$.

Hier können wir die Hilbertfunktion sogar direkt angeben, da f, h eine *reguläre Sequenz*[†] von homogenen Polynomen vom Grad d_1 bzw. d_2 bilden und da f, h den vollständigen Durchschnitt Γ definieren. Nach Lemma 2.5 im Artikel von Hansen (2003) gilt:

$$H_\Gamma(a) = \binom{2+a}{2} - \binom{2+a-d_1}{2} - \binom{2+a-d_2}{2} + \binom{2+a-d_1-d_2}{2}.$$

[†]Polynome $f_1, \ldots, f_m \in K[X_0, \ldots, X_m] = R$ bilden eine *reguläre Sequenz*, falls $\langle f_1, \ldots, f_m \rangle$ ein echtes Ideal in R ist und f_{i+1} für alle i kein Nullteiler in $R/\langle f_1, \ldots, f_i \rangle$ ist (vgl. Eisenbud, 1995, S. 241).

Speziell für $a = q(q-\lambda)$ mit $1 \leq \lambda \leq q-1$ folgt $\binom{2+a-d_2}{2} = \binom{2+(1-\lambda)q}{2} = \delta_{\lambda 1}$ ($\delta_{\lambda 1} = 1$, falls $\lambda = 1$, und $\delta_{\lambda 1} = 0$ sonst). Dann ist die Dimension:

$$k_a = H_\Gamma(a) = q^3 + \tfrac{1-2\lambda}{2}(q^2+q) + 1 - \delta_{\lambda 1}.$$

Für den Minimalabstand ergibt sich: $d \geq q^2 - a = \lambda q$.

Wir vergleichen diesen speziellen Auswerte-Code $C(\Gamma)_a$ nun mit dem Hermiteschen Code C_r zu $r = a(q+1) = (q-\lambda)(q^2+q)$ aus Beispiel 2.5. Die bisher für diese Codes ermittelten Parameter sind in folgender Tabelle zusammengestellt:

	$C(\Gamma)_a$ $a = q(q-\lambda)$	C_r $r = (q-\lambda)(q^2+q)$
n	$q^3 - q$	q^3
k	$q^3 + \frac{1-2\lambda}{2}(q^2+q) + 1 - \delta_{\lambda 1}$	$q^3 + \frac{1-2\lambda}{2}(q^2+q) + 1$
d	$\geq \lambda q$	$(\lambda-1)q^2 + \lambda q$

Dies Beispiel legt erneut nahe, daß unser Hauptresultat im allgemeinen dann eine gute Abschätzung für den Minimalabstand liefert, wenn a etwa so groß wie $s = q^2 - 2$ ist. Hier tritt dieser Fall für $\lambda = 1$ ein; dann hat man:

	$C(\Gamma)_a$ $a = q(q-1)$	C_r $r = (q-1)(q^2+q)$
n	$q^3 - q$	q^3
k	$q^3 - \frac{1}{2}(q^2+q)$	$q^3 - \frac{1}{2}(q^2+q) + 1$
d	$\geq q$	q

$\Diamond$

A. Anhang

Wir zeigen hier die beiden Aussagen, die wir in den Beispielen 2.5 und 4.3 auf den Seiten 24 und 47 benutzen.

Lemma A.1: *Es gilt:* $\#\{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha = 0\} = q$,
mit anderen Worten: $\#\{\alpha \in \mathbb{F}_{q^2} \mid \alpha^q + \alpha \neq 0\} = q^2 - q$.

Beweis: Wir müssen zeigen, daß alle q Nullstellen des Polynoms $X^q + X$ in $\mathbb{F}_{q^2}$ liegen. Dies ist genau dann der Fall, wenn $X^q + X$ das Polynom $X^{q^2} - X$ teilt, denn $\mathbb{F}_{q^2}$ ist der Zerfällungskörper von $X^{q^2} - X$. Wir betrachten:

$$\begin{aligned}(X^{q-1}+1)\cdot\sum_{j=0}^{q}(-1)^{j+1}\cdot X^{j(q-1)} &= \sum_{j=0}^{q}(-1)^{j+1}\cdot X^{(j+1)(q-1)} - \sum_{j=0}^{q}(-1)^{j}\cdot X^{j(q-1)}\\ &= \sum_{j=1}^{q+1}(-1)^{j}\cdot X^{j(q-1)} - \sum_{j=0}^{q}(-1)^{j}\cdot X^{j(q-1)}\\ &= (-1)^{q+1}\cdot X^{(q+1)(q-1)} - 1\\ &= X^{q^2-1} - 1,\end{aligned}$$

$$\Longrightarrow\ \frac{X^{q^2}-X}{X^q+X} = \sum_{j=0}^{q}(-1)^{j+1}\cdot X^{j(q-1)}. \qquad \blacksquare$$

Das Lemma benutzen wir im Beweis des folgenden Satzes:

Satz A.2: *Die Hermitesche Kurve $\mathcal{X}_q = V(f)$ mit $f(X,Y,Z) = Y^{q+1} - X^qZ - XZ^q$ hat genau q^3 affine $\mathbb{F}_{q^2}$-rationale Punkte, das heißt, $f(X,Y,1) = Y^{q+1} - X^q - X$ hat genau q^3 Nullstellen mit Koordinaten in $\mathbb{F}_{q^2}$.*

Beweis: Für gegebenes $\alpha \in \mathbb{F}_{q^2}$ unterscheiden wir zwei Fälle:

$\alpha^q + \alpha = 0$: Offenbar ist nur $(\alpha, 0, 1)$ Nullstelle von $f(X,Y,1)$.

$\alpha^q + \alpha \neq 0$: Über dem algebraischen Abschluß $\mathbb{F}$ von $\mathbb{F}_q$ hat $Y^{q+1} - \alpha^q - \alpha$ genau $q+1$ Nullstellen. Sei β eine von diesen. Dann gilt $\beta \in \mathbb{F}_{q^2}$, denn:

$$\beta^{q^2-1} = \left(\beta^{q+1}\right)^{q-1} = \left(\alpha^q+\alpha\right)^{q-1} = \frac{(\alpha^q+\alpha)^q}{\alpha^q+\alpha} = \frac{\alpha^{q^2}+\alpha^q}{\alpha^q+\alpha} = 1.$$

Gemäß obigem Lemma liefert der erste Fall q und der zweite Fall $(q^2-q)\cdot(q+1)$ Nullstellen. Insgesamt ergibt sich für die Anzahl der Nullstellen also:

$$q + (q^2-q)\cdot(q+1) = q^3. \qquad \blacksquare$$

B. Bemerkungen zum Artikel von Gold, Little und Schenck

Um ihr Hauptresultat im Artikel „Cayley–Bacharach and Evaluation Codes on Complete Intersections“ zu zeigen, zitieren Gold, Little und Schenck die für den Beweis benötigten Aussagen[†] aus anderen Arbeiten; sie übersetzen die Aussagen dabei gleich in die Sprache der Cohomologietheorie. Im Beweis machen die Autoren diese Umformulierung dann wieder rückgängig.

Wie in Kapitel 4 durchgeführt, läßt sich das Hauptresultat mit denselben Aussagen beweisen, ohne diese umzuformulieren. Wahrscheinlich benutzen Gold, Little und Schenck die Cohomologietheorie nur, um die gleichen Bezeichner wie im Artikel „Linkage and Codes on Complete Intersections“ von Hansen zu verwenden, dessen Aussage sie ja verallgemeinern.

An dieser Stelle sollen nun die Begriffe und Sätze aus der Algebraischen Geometrie bzw. aus der Cohomologietheorie eingeführt werden, die zur Umformulierung benötigt werden.

B.1. Algebraische Geometrie

Im folgenden sei S ein graduierter Ring und $(X, \mathscr{O}_X)$ das zugehörige projektive Schema, d. h. X ist das homogene Primidealspektrum von S, kurz: $X = \operatorname{Proj} S$, und $\mathscr{O}_X$ ist die Strukturgarbe.

B.1.1. $\mathscr{O}_X$-Moduln

Eine Garbe $\mathscr{F}$ auf X bezeichnet man dann als *Garbe von $\mathscr{O}_X$-Moduln*, kurz als *$\mathscr{O}_X$-Modul*, wenn $\mathscr{F}(U)$ für jedes offene $U \subset X$ ein $\mathscr{O}_X(U)$-Modul ist und die Restriktionsabbildungen mit der Modulstruktur verträglich sind.

Definition B.1: *Sei $(Y, \mathscr{O}_Y)$ ein abgeschlossenes Unterschema des Schemas $(X, \mathscr{O}_X)$ und sei $i\colon Y \to X$ die Inklusion. Die **Idealgarbe** $\mathscr{I}_Y$ von Y ist der Kern des Garbenmorphismus $i^{\#}\colon \mathscr{O}_X \to i_*\mathscr{O}_Y$, wobei $i_*\mathscr{O}_Y$ die direkte Bildgarbe von $\mathscr{O}_Y$ bezeichnet (☞ Definition 3.9 auf Seite 30).*

Die Idealgarbe $\mathscr{I}_Y$ ist eine Garbe von Idealen, da jedes $\mathscr{I}_Y(U)$ ein Ideal in $\mathscr{O}_X(U)$ ist. Betrachtet man $\mathscr{O}_X$ als $\mathscr{O}_X$-Modul, so ist $\mathscr{I}_Y$ eine Garbe von $\mathscr{O}_X$-Moduln.

Ist $\mathscr{F}$ ein $\mathscr{O}_X$-Modul und $\alpha\colon X \to Y$ eine stetige Abbildung zwischen topologischen Räumen, so ist $\alpha_*\mathscr{F}$ ein $\alpha_*\mathscr{O}_X$-Modul. Über einen Garbenmorphismus $\alpha^{\#}\colon \mathscr{O}_Y \to \alpha_*\mathscr{O}_X$ läßt sich $\alpha_*\mathscr{F}$ dann sogar als $\mathscr{O}_Y$-Modul auffassen.

[†] Im wesentlichen sind dies das Lemma 2.4 auf Seite 12 und der Satz 3.16 von Cayley-Bacharach

B.1.2. Twistung

Verschiebt man im Grundring S die Graduierung um $a \in \mathbb{Z}$:

$$S(a) = \bigoplus_{\ell \in \mathbb{Z}} S(a)_\ell, \quad \text{mit } S(a)_\ell := S_{a+\ell},$$

so erhält man einen S-Modul $S(a)$. Analog zur Konstruktion der Strukturgarbe $\mathscr{O}_X$ kann man zu diesem um *a getwisteten* Grundring $S(a)$ eine *getwistete Strukturgarbe* $\mathscr{O}_X(a)$ auf X definieren (siehe Hartshorne, 1977, S. 116).

Mittels $\mathscr{O}_X(a)$ läßt sich eine Twistung für anderer $\mathscr{O}_X$-Moduln definieren:

Definition B.2: *Sei $\mathscr{F}$ ein $\mathscr{O}_X$-Modul. Für $a \in \mathbb{Z}$ bezeichnet $\mathscr{F}(a)$ die* ***getwistete Garbe*** *$\mathscr{F} \otimes_{\mathscr{O}_X} \mathscr{O}_X(a)$. Dabei ist das* ***Tensorprodukt*** *$\mathscr{G} \otimes_{\mathscr{O}_X} \mathscr{H}$ zweier $\mathscr{O}_X$-Moduln $\mathscr{G}, \mathscr{H}$ die zur Prägarbe $U \mapsto \mathscr{G}(U) \otimes_{\mathscr{O}_X(U)} \mathscr{H}(U)$ assoziierte Garbe.*

Im folgenden Satz sind einige Eigenschaften der Twistung zusammengefaßt:

Satz B.1: *Für jedes $\mathfrak{p} \in X$ gilt für den Halm der um $a \in \mathbb{Z}$ getwisteten Strukturgarbe:*

$$\mathscr{O}_X(a)_\mathfrak{p} \cong S(a)_{(\mathfrak{p})}.$$

Außerdem hat man für alle $a, b \in \mathbb{Z}$:

$$\mathscr{O}_X(a) \otimes \mathscr{O}_X(b) \cong \mathscr{O}_X(a+b), \quad \textit{insbesondere: } \mathscr{F}(a) \otimes \mathscr{O}_X(b) \cong \mathscr{F}(a+b).$$

Beweis: Siehe Hartshorne (1977, S. 117, Prop. 5.11(a) und Prop. 5.12(b)). ■

Notiz B.2: Sei $(Y, \mathscr{O}_Y)$ ein abgeschlossenes Unterschema von $(X = \operatorname{Proj} R, \mathscr{O}_X)$ mit Idealgarbe $\mathscr{I}_Y$. Für $a \in \mathbb{N}$ ist

$$0 \to \mathscr{I}_Y(a) \to \mathscr{O}_X(a) \to {}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)} \to 0$$

eine kurze exakte Sequenz aus um a getwisteten Garben; eine Sequenz von Garben

$$\ldots \to \mathscr{F}^i \xrightarrow{\varphi^i} \mathscr{F}^{i+1} \xrightarrow{\varphi^{i+1}} \mathscr{F}^{i+2} \to \ldots$$

ist *exakt*, falls in jeder Stufe $\operatorname{Im} \varphi^i = \operatorname{Ker} \varphi^{i+1}$ gilt. ◊

B.1.3. Assoziierter Modul

Über die Twist-Operation können wir jeder Garbe von Moduln auf $X = \operatorname{Proj} S$ einen graduierten S-Modul zuordnen:

Definition B.3: *Sei $\mathscr{F}$ eine Garbe von $\mathscr{O}_X$-Moduln. Der zu $\mathscr{F}$ **assoziierte graduierte S-Modul** sei als Gruppe gegeben durch:*

$$\Gamma_*(\mathscr{F}) = \bigoplus_{a \in \mathbb{Z}} \Gamma(X, \mathscr{F}(a)).$$

Die Modulstruktur sei folgende: Jedes homogene Element $s \in S_b$ bestimmt einen globalen Schnitt $\sigma \in \Gamma(X, \mathscr{O}_X(b))$, nämlich $\sigma\colon \mathfrak{p} \mapsto \frac{s}{1}$. Daher sei für jedes $\tau \in \Gamma(X, \mathscr{F}(a))$ das Produkt $s \cdot \tau$ das Tensorprodukt $\sigma \otimes \tau$. Wegen $\mathscr{F}(a) \otimes \mathscr{O}_X(b) \cong \mathscr{F}(a+b)$ (☞ Satz B.1) ist dann tatsächlich $s \cdot \tau = \sigma \otimes \tau \in \Gamma(X, \mathscr{F}(a+b))$.

Im allgemeinen stimmt der assoziierte graduierte S-Modul nicht mit S überein (vgl. Hartshorne, 1977, S. 118, Caution 5.13.1). Speziell bei einem Polynomring hat man aber die Gleichheit:

Satz B.3: *Sei $R = K[X_0, \ldots, X_m]$, und sei $(X = \operatorname{Proj} R, \mathscr{O}_X)$ das zugehörige Schema. Dann ist der zu $\mathscr{O}_X$ assoziierte graduierte R-Modul der Polynomring selbst:*

$$\Gamma_*(\mathscr{O}_X) \cong R.$$

Für alle $a \in \mathbb{N}$ gilt also: $\Gamma(X, \mathscr{O}_X(a)) = (\Gamma_*(\mathscr{O}_X))_a \cong R_a$.

Beweis: Siehe Hartshorne (1977, S. 118, Prop. 5.13). ∎

> In diesem Abschnitt sei daher $R = K[X_0, \ldots, X_m]$ ein Polynomring in $m+1$ Unbestimmten über einem algebraisch abgeschlossenen Körper K.

Notiz B.4: Im Beweis des Korollars 5.16 im Buch von Hartshorne (1977, S. 119) ergibt sich, daß der zur Idealgarbe $\mathscr{I}_Y$ assoziierte R-Modul $\Gamma_*(\mathscr{I}_Y)$ gerade das Verschwindungsideal I_Y des Unterschemas Y ist. Daher gilt für alle $a \in \mathbb{N}$:

$$\Gamma(X, \mathscr{I}_Y(a)) = (\Gamma_*(\mathscr{I}_Y))_a \cong (I_Y)_a. \qquad \Diamond$$

Lemma B.5: *Sei $(Y, \mathscr{O}_Y)$ ein abgeschlossenes Unterschema von $(X = \operatorname{Proj} R, \mathscr{O}_X)$ mit Idealgarbe $\mathscr{I}_Y$. Dann gilt für die globalen Schnitte der getwisteten Strukturgarbe $\mathscr{O}_Y(a)$:*

$$\Gamma(Y, \mathscr{O}_Y(a)) \cong \Gamma\Big(X, {}^{\mathscr{O}_X(a)}\!\Big/_{\mathscr{I}_Y(a)}\Big).$$

Beweis: Sei $(i, i^{\#})\colon (Y, \mathscr{O}_Y) \to (X, \mathscr{O}_X)$ die zum Unterschema Y gehörende abgeschlossene Immersion; die Inklusion $i\colon Y \to X$ liefert die direkte Bildgarbe $i_*\mathscr{O}_Y$ von $\mathscr{O}_Y$. Wir zeigen

$$\Gamma\Big(X, {}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)}\Big) \overset{❶}{\cong} \Gamma\Big(X, \Big({}^{\mathscr{O}_X}\!/_{\mathscr{I}_Y}\Big)(a)\Big) \overset{❷}{\cong} \Gamma\big(X, (i_*\mathscr{O}_Y)(a)\big)$$
$$\overset{❸}{\cong} \Gamma\big(X, i_*(\mathscr{O}_Y(a))\big) \overset{❹}{\cong} \Gamma\big(Y, \mathscr{O}_Y(a)\big)$$

in vier Schritten:

❶ Für offenes $U \subset X$ ergibt sich:

$$\begin{aligned}\mathscr{I}_Y(a)(U) &= \mathscr{I}_Y(U) \otimes_{\mathscr{O}_X(U)} \mathscr{O}_X(a)(U)\\ &= \big(\mathscr{I}_Y(U) \cdot \mathscr{O}_X(U)\big) \otimes_{\mathscr{O}_X(U)} \mathscr{O}_X(a)(U)\\ &= \mathscr{O}_X(U) \otimes_{\mathscr{O}_X(U)} \big(\mathscr{I}_Y(U) \cdot \mathscr{O}_X(a)(U)\big) \cong \mathscr{I}_Y(U) \cdot \mathscr{O}_X(a)(U).\end{aligned}$$

Da für einen A-Modul M und ein Ideal $\mathfrak{a} \in A$ gilt: $A/\mathfrak{a} \otimes_A M = M/\mathfrak{a}M$, folgt:

$$\begin{aligned}\Big({}^{\mathscr{O}_X}\!/_{\mathscr{I}_Y}\Big)(a)(U) &\cong \Big({}^{\mathscr{O}_X(U)}\!/_{\mathscr{I}_Y(U)}\Big) \otimes_{\mathscr{O}_X(U)} \mathscr{O}_X(a)(U)\\ &\cong {}^{\mathscr{O}_X(a)(U)}\!/_{\big(\mathscr{I}_Y(U) \cdot \mathscr{O}_X(a)(U)\big)}\\ &\cong {}^{\mathscr{O}_X(a)(U)}\!/_{\mathscr{I}_Y(a)(U)} \cong \Big({}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)}\Big)(U).\end{aligned}$$

Das gibt: $\mathscr{O}_X(a)/\mathscr{I}_Y(a) \cong (\mathscr{O}_X/\mathscr{I}_Y)(a)$.

❷ Weil $i^{\#}\colon \mathscr{O}_X \to i_*\mathscr{O}_Y$ nach Voraussetzung surjektiv ist und weil definitionsgemäß $\operatorname{Ker} i^{\#} = \mathscr{I}_Y$ ist, hat man:

$$i_*\mathscr{O}_Y \cong {}^{\mathscr{O}_X}\!/_{\mathscr{I}_Y} \qquad \Longrightarrow\ (i_*\mathscr{O}_Y) \otimes \mathscr{O}_X(a) \cong \Big({}^{\mathscr{O}_X}\!/_{\mathscr{I}_Y}\Big) \otimes \mathscr{O}_X(a).$$

Offenbar gilt: $(i_*\mathscr{O}_Y)(a) \cong (\mathscr{O}_X/\mathscr{I}_Y)(a)$.

❸ Das ist ein Spezialfall von Prop. 5.12(c) im Buch von Hartshorne (1977, S. 117).

❹ Klar nach Definition 3.9 auf Seite 30, denn $i^{-1}(X) = Y$. ∎

Ähnlich wie im nichtgetwisteten Fall (☞ Satz 3.13) können wir die globalen Schnitte $\mathscr{O}_Y(a)(Y)$ eines nulldimensionalen reduziertn projektiven Unterschemas bestimmen. Es gilt

Satz B.6: *Sei $Y = \operatorname{Proj} R/I_Y$ ein nulldimensionales reduziertes projektives Unterschema von $X = \operatorname{Proj} R$. Dann bilden die globalen Schnitte $\mathscr{O}_Y(a)(Y)$ für jedes $a \in \mathbb{N}$ einen endlichdimensionalen K-Vektorraum, und für dessen Dimension gilt:*

$$\dim_K \mathscr{O}_Y(a)(Y) = {}^{\#}Y =: n, \qquad \text{also: } \Gamma(Y, \mathscr{O}_Y(a)) \cong K^n.$$

Beweis (analog zum nichtgetwisteten Fall aus Satz 3.13):
Wie oben sei $Y = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_n\} \mathrel{\widehat{=}} \{p_1, \ldots, p_n\} = \Gamma \subset \mathbb{P}^m$. Für jeden der Punkte $p_k = (p_{k_0} : \ldots : p_{k_m})$ ist eine Koordinate $p_{k_\ell} \neq 0$. Wir setzen $S := R/I_\Gamma$ (hier gilt $I_\Gamma = I_Y$, denn Y ist reduziert). Da die einzelnen Primideale $\mathfrak{p}_k$ auch offene Mengen sind (diskrete Toplologie), können wir betrachten:

$$\mathscr{O}_Y(a)(\{\mathfrak{p}\}) = \{\sigma\colon \{\mathfrak{p}\} \to S(a)_{(\mathfrak{p})}\} \cong S(a)_{(\mathfrak{p})} \cong \mathscr{O}_Y(a)_{\mathfrak{p}}.$$

Das Garbenaxiom (G2) (☞ Definition 3.5 auf Seite 28) liefert nun für offenes $U \subset Y$:

$$\mathscr{O}_Y(a)(U) \cong \prod_{\mathfrak{p}\in U} S(a)_{(\mathfrak{p})} \cong \prod_{\mathfrak{p}\in U} \mathscr{O}_Y(a)_{\mathfrak{p}}.$$

Insbesondere ist $\mathscr{O}_Y(a)(Y) \cong \prod_{j=1}^n S(a)_{(\mathfrak{p}_j)} \cong \prod_{j=1}^n \mathscr{O}_Y(a)_{\mathfrak{p}_j}$; wir sind also fertig, falls für $k \in \{1, \ldots, n\}$ stets gilt:

$$\dim_K S(a)_{(\mathfrak{p}_k)} = 1 \quad \text{oder äquivalent:} \quad \forall\, \frac{g}{h} \in S(a)_{(\mathfrak{p}_k)} \colon \exists\, \lambda \in K \colon \frac{g}{h} = \lambda \cdot \frac{(X_{k_\ell})^a}{1}.$$

Sei daher $\frac{g}{h} \in S(a)_{(\mathfrak{p}_k)}$ gegeben, das heißt, $g \in S$, $h \in S \setminus \mathfrak{p}_k$ und g, h homogen, $\operatorname{grad} g = a + \operatorname{grad} h$. Wegen $\mathfrak{p}_k = \{f \in S \mid f \text{ homogen}, f(p_k) = 0\}$ ist $h(p_k) \neq 0$.

Setze $\lambda := \frac{g(p_k)}{h(p_k)\cdot p_{k_\ell}^a} \in K$. Wähle $t = 1$, falls $n = 1$, andernfalls $t \in \bigcap_{i\neq k} \mathfrak{p}_i, t \notin \mathfrak{p}_k$ (ein solches t existiert, da zwei Primideale wegen $\dim Y = 0$ nicht echt ineinander enthalten sein können). Dann ist $t(p_k) \neq 0$ und $t(p_i) = 0$ für alle $i \neq k$, also:

$$\begin{aligned} \forall\, j\colon t\big(g - \lambda h (X_{k_\ell})^a\big)(p_j) = 0 \quad &\overset{Y \text{ reduziert}}{\iff} \quad t(g - \lambda h (X_{k_\ell})^a) \equiv 0 \text{ in } S = {}^{R}\!/_{I_\Gamma} \\ &\implies \quad \frac{g}{h} = \lambda \cdot \frac{(X_{k_\ell})^a}{1}. \end{aligned}$$

Offenbar ist $S(a)_{(\mathfrak{p})} \cong \mathscr{O}_Y(a)_{\mathfrak{p}}$ für jedes $\mathfrak{p} \in Y$ eindimensional, so daß die Behauptung $\dim_K \mathscr{O}_Y(a)(Y) = {}^{\#}Y$ folgt. ∎

B.2. Homologische Algebra: Garbencohomologie

Wir geben hier die benötigten Aussagen der Cohomologietheorie von Garben an. Dabei richten wir uns nach den Büchern von Hartshorne (1977, Kapitel III.1 und III.2) und Iversen (1986, Kapitel II.3); eine kategorielle Betrachtung findet man bei Kato (2006, Kapitel 3.4).

Im folgenden sei X ein topologischer Raum.

Definition B.4: *Der **Cohomologiefunktor** $H^i(X, \cdot)$ ist der rechts derivierte Funktor des globalen Schnittfunktors $\Gamma(X, \cdot)$. Die für eine Garbe $\mathscr{F}$ gebildeten Gruppen $H^i(X, \mathscr{F})$ heißen **Cohomologiegruppen** von $\mathscr{F}$.*

Insbesondere entspricht die nullte Cohomologiegruppe nach Definition des derivierten Funktors (siehe z. B. Kato, 2006, S. 46) gerade den globalen Schnitten:

$$H^0(X, \mathscr{F}) = \Gamma(X, \mathscr{F}) = \mathscr{F}(X). \qquad (*)$$

Was genau die anderen Cohomologiegruppen beschreiben, ist für das Verständnis dieser Arbeit nicht weiter wichtig, da wir die Gruppen an entsprechender Stelle mit Vektorräumen identifizieren werden.

Für uns interessant ist folgende lange exakte Cohomologiesequenz:

Satz B.7: *Sei $0 \to \mathscr{F} \to \mathscr{G} \to \mathscr{H} \to 0$ eine kurze exakte Sequenz von Garben auf X. Dann gibt es Verbindungshomomorphismen $\delta^i \colon H^i(X, \mathscr{H}) \to H^{i+1}(X, \mathscr{F})$, so daß folgende lange Sequenz von Cohomologiegruppen exakt ist:*

$$0 \to H^0(X, \mathscr{F}) \to H^0(X, \mathscr{G}) \to H^0(X, \mathscr{H}) \xrightarrow{\delta^0} H^1(X, \mathscr{F}) \to \dots$$

$$\dots \to H^i(X, \mathscr{F}) \to H^i(X, \mathscr{G}) \to H^i(X, \mathscr{H}) \xrightarrow{\delta^i} H^{i+1}(X, \mathscr{F}) \to \dots$$

Beweis: Siehe Hartshorne (1977, S. 207) oder Kato (2006, S. 98f). ∎

Im Falle eines noetherschen topologischen Raumes endlicher Dimension bricht jede lange Cohomologiesequenz ab. Dies liefert der Verschwindungssatz von Grothendieck:

Satz B.8: *Sei X ein noetherscher topologischer Raum der Dimension m. Für alle $i > m$ und alle Garben $\mathscr{G}$ von abelschen Gruppen auf X gilt: $H^i(X, \mathscr{G}) = 0$.*

Beweis: Siehe Hartshorne (1977, S. 208, Theorem 2.7). ∎

Wir betrachten noch den Anfang der langen Cohomologiesequenz; gemäß Gleichung $(*)$ stehen hier globale Schnitte:

$$0 \to \mathscr{F}(X) \to \mathscr{G}(X) \to \mathscr{H}(X) \xrightarrow{\delta^0} H^1(X, \mathscr{F}) \to H^1(X, \mathscr{G}) \to \dots$$

Falls $H^1(X, \mathscr{G}) = 0$ gilt, ist δ^0 surjektiv.

Das tritt beispielsweise ein, wenn $\mathscr{G}$ die um a getwistete Strukturgarbe $\mathscr{O}_X(a)$ des projektiven Schemas $X = \operatorname{Proj} K[X_0, \dots, X_m]$ ist:

Satz B.9: *Sei $X = \operatorname{Proj} K[X_0, \dots, X_m]$ mit $m > 0$. Dann gilt für $0 < i < m$ und alle $a \in \mathbb{Z}$:*

$$H^i\big(X, \mathscr{O}_X(a)\big) = 0.$$

Beweis: Siehe Hartshorne (1977, S. 225, Theorem 5.1(b)). ∎

B.3. Umformulierung in die Sprache der Cohomologietheorie

Wir wollen hier das Lemma 2.4 und den Satz 3.16 von Cayley-Bacharach wie im Artikel von Gold, Little und Schenck in die Sprechweise der Cohomologietheorie übertragen. Abschließend beweisen wir das Hauptresultat so, wie es die genannten Autoren in ihrer Arbeit tun.

Sei $\Gamma = \{p_1, \ldots, p_n\}$ eine Menge $\mathbb{F}_q$-rationaler Punkte im $\mathbb{P}^m_{\mathbb{F}}$. Die zu Γ gehörende Auswerteabbildung $e_a(\Gamma)$, $a \in \mathbb{N}$, führt auf folgende exakte Sequenz von $\mathbb{F}_q$-Vektorräumen:

$$0 \to (I_\Gamma)_a = \operatorname{Ker} e_a(\Gamma) \to R_a \xrightarrow{e_a(\Gamma)} \mathbb{F}_q^n \to \operatorname{Coker} e_a(\Gamma) \to 0.$$

Dabei ist $R = \mathbb{F}_q[X_0, \ldots, X_m]$. Verwenden wir nun statt des Grundkörpers $\mathbb{F}_q$ dessen algebraischen Abschluß $\mathbb{F}$ und schreiben $\mathcal{R} = \mathbb{F}[X_0, \ldots, X_m]$, so ist auch

$$0 \to (\mathcal{I}_\Gamma)_a = \operatorname{Ker} e_a(\Gamma) \to \mathcal{R}_a \xrightarrow{e_a(\Gamma)} \mathbb{F}^n \to \operatorname{Coker} e_a(\Gamma) \to 0 \qquad (*)$$

exakt. Diese $\mathbb{F}$-Vektorräume haben dieselbe Vektorraumdimension wie obige über $\mathbb{F}_q$ gebildeten Vektorräume, da wir Polynome für $\mathbb{F}_q$-rationale Punkte auswerten.[†]

Wie wir in Beispiel 3.4 auf Seite 33 gesehen haben, bestimmt Γ ein reduziertes, abgeschlossenes Unterschema $(Y, \mathscr{O}_Y)$ von $(X = \operatorname{Proj} \mathcal{R}, \mathscr{O}_X)$. Die $\mathbb{F}$-Vektorräume der exakten Sequenz $(*)$ lassen sich als globale Schnitte realisieren. Nach Notiz B.4 auf Seite 53 und Satz B.3 auf Seite 53 gilt nämlich:

$$\Gamma(X, \mathscr{I}_Y(a)) \cong (\mathcal{I}_\Gamma)_a, \qquad \Gamma(X, \mathscr{O}_X(a)) \cong \mathcal{R}_a.$$

Da Y reduziert ist, liefern Lemma B.5 und Satz B.6 auf Seite 55 außerdem:

$$\Gamma\Big(X, {}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)}\Big) \cong \Gamma(Y, \mathscr{O}_Y(a)) \cong \mathbb{F}^n.$$

Die hier auftretenden um a getwisteten Garben bilden die kurze exakte Garbensequenz aus Notiz B.2 auf Seite 52:

$$0 \to \mathscr{I}_Y(a) \to \mathscr{O}_X(a) \to {}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)} \to 0.$$

Jetzt kommt die Cohomologietheorie ins Spiel. Nach Satz B.7 existiert zu der kurzen Garbensequenz eine lange exakte Sequenz von Cohomologiegruppen (dabei benutzen wir den Verschwindungssatz B.9: $H^1(\mathscr{O}_X(a)) = 0$):

$$0 \to H^0(\mathscr{I}_Y(a)) \to H^0(\mathscr{O}_X(a)) \to H^0\Big({}^{\mathscr{O}_X(a)}\!/_{\mathscr{I}_Y(a)}\Big) \xrightarrow{\delta^0} H^1(\mathscr{I}_Y(a)) \to 0;$$

[†] Die (normierten) Monome vom Grad a bilden eine Basis der homogenen Polynome vom Grad a. Bezüglich dieser Basis hat die (lineare) Auswerteabbildung $e_a(\Gamma)$ offensichtlich in beiden Fällen dieselbe Darstellung als Matrix, da ja nur Punkte mit Koordinaten in $\mathbb{F}_q$ eingesetzt werden.

abkürzend schreiben wir hier $H^i(\mathscr{F}) = H^i(X, \mathscr{F})$.

Weil die nullten Cohomologiegruppen $H^0(\cdot)$, wie in Kapitel B.2 bemerkt, gerade die globalen Schnitte sind, erhalten wir folgendes kommutative Diagramm:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & \mathscr{I}_Y(a)(X) & \longrightarrow & \mathscr{O}_X(a)(X) & \longrightarrow & \left(\mathscr{O}_X(a)/\mathscr{I}_Y(a)\right)(X) & \xrightarrow{\delta^0} & H^1(\mathscr{I}_Y(a)) \longrightarrow 0 \\
 & & \wr\downarrow & & \wr\downarrow & & \wr\downarrow & & \psi\downarrow \\
0 & \longrightarrow & (\mathcal{I}_\Gamma)_a & \longrightarrow & \mathcal{R}_a & \longrightarrow & \mathbb{F}^n & \longrightarrow & \operatorname{Coker} e_a(\Gamma) \longrightarrow 0.
\end{array}$$

Per „Diagrammjagd“ weist man leicht nach, daß auch ψ ein Isomorphismus ist. Die hier betrachteten Cohomologiegruppen $H^i(\mathscr{F})$ sind also endlichdimensionale $\mathbb{F}$-Vektorräume, deren Vektorraumdimension wir mit $h^i(\mathscr{F})$ bezeichnen. Wie auf der vorherigen Seite beschrieben, stimmen die $h^i(\mathscr{F})$ mit den Dimensionen der jeweiligen $\mathbb{F}_q$-Vektorräume in der exakten Sequenz überein:

$$0 \to (I_\Gamma)_a \to R_a \to \mathbb{F}_q^n \to \operatorname{Coker} e_a(\Gamma) \to 0.$$

Bei einer exakten Sequenz verschwindet stets die alternierende Summe der Dimensionen; wegen $H_\Gamma(a) = \dim R_a - \dim(I_\Gamma)_a$ und $\dim \mathbb{F}_q^n = n = {}^\#\Gamma$ ist also:

$$\begin{aligned}
0 = \dim R_a - \dim(I_\Gamma)_a + \dim \operatorname{Coker} e_a(\Gamma) - \dim \mathbb{F}_q^n \\
\Longrightarrow\ H_\Gamma(a) = {}^\#\Gamma - h^1(\mathscr{I}_Y(a)).
\end{aligned}$$

Damit läßt sich das Lemma 2.4 nun folgendermaßen formulieren:

Lemma B.10: *Ist Γ eine endliche Punktmenge im $\mathbb{P}^m$, so gilt für $a \geq {}^\#\Gamma - 1$:*

$$h^1(\mathscr{I}_Y(a)) = 0.$$

Der Satz von Cayley-Bacharach (☞ Satz 3.16) lautet mit diesen Bezeichnungen:

Satz B.11 (Cayley-Bacharach)**:** *Seien $H_1, \ldots, H_m$ Hyperflächen vom Grad $d_1, \ldots, d_m$ im $\mathbb{P}^m$ mit nulldimensionalem vollständigem Durchschnitt $\Gamma = H_1 \cap \ldots \cap H_m$. Ferner seien Γ' und Γ'' Unterschemata von Γ, die zueinander jeweils Restschemata in Γ sind. Setze $s = \sum d_i - m - 1$. Dann gilt für $a \in \{0, \ldots, s\}$:*

$$\begin{aligned}
h^0(\mathscr{I}_{\Gamma'}(a)) - h^0(\mathscr{I}_\Gamma(a)) &= \dim\left((I_{\Gamma'})_a/(I_\Gamma)_a\right) \\
&= \dim \operatorname{Coker} e_{s-a}(\Gamma'') = h^1(\mathscr{I}_{\Gamma''}(s-a)).
\end{aligned}$$

Wir können unser Hauptresultat über die Abschätzung des Minimalabstands von Auswerte-Codes nun erneut zeigen. Sei dazu Γ wie im Satz B.11 gegeben und zusätzlich reduziert. $C(\Gamma)_a$ sei der in Kapitel 2.2 definierte Auswerte-Code zu Γ. Sein Minimalabstand unterliegt dann folgender Schranke:

Satz B.12: *$C(\Gamma)_a$ hat Minimalabstand $d \geq s - a + 2$, falls $1 \leq a \leq s$.*

Beweis: Wie oben ist $\ell := {}^{\#}\Gamma - (s - a + 1) \geq 0$. Zu einem beliebigem $\Gamma' \subset \Gamma$ mit $\ell = {}^{\#}\Gamma'$ sei Γ'' das Restschema. Dann gilt:

$$ {}^{\#}\Gamma'' = {}^{\#}\Gamma - {}^{\#}\Gamma' = s - a + 1.$$

Offenbar ist also $s - a = {}^{\#}\Gamma'' - 1$, weshalb mit Lemma B.10 und dem Satz von Cayley-Bacharach (☞ Satz B.11) folgt:

$$\begin{aligned} h^1(\mathscr{I}_{\Gamma''}(s-a)) = 0 \quad &\Longrightarrow \quad h^0(\mathscr{I}_{\Gamma}(a)) = h^0(\mathscr{I}_{\Gamma'}(a)) \\ &\Longleftrightarrow \quad \dim(I_\Gamma)_a = \dim(I_{\Gamma'})_a \\ &\Longleftrightarrow \quad H_\Gamma(a) = H_{\Gamma'}(a). \end{aligned}$$

Satz 2.10 liefert nun die Behauptung: $d \geq n - \ell + 1 = {}^{\#}\Gamma - {}^{\#}\Gamma' + 1 = s - a + 2$. ■

Literatur

ASSMUS, E. F., Jr.; KEY, J. D.:
Cambridge Tracts in Mathematics. Bd. 103: *Designs and Their Codes*.
Cambridge: Cambridge University Press, 1992.

BEUTELSPACHER, Albrecht; ROSENBAUM, Ute:
Projektive Geometrie. Von den Grundlagen zu den Anwendungen.
2., durchges. und erw. Aufl.
Wiesbaden: Vieweg, 2004.

CHASLES, Michel:
Traité des sections coniques.
Paris: Gauthier-Villars, 1865.
`http://name.umdl.umich.edu/ABN6567.0001.001`.

DELSARTE, P.; GOETHALS, J. M.; MAC WILLIAMS, F. J.:
„On Generalized Reed-Muller Codes and Their Relatives“.
In: *Information and Control* 16 (1970), Juli, Nr. 5, S. 403 – 442.
DOI 10.1016/S0019-9958(70)90214-7.

DEMTRÖDER, Wolfgang:
Experimentalphysik. Bd. 1: *Mechanik und Wärme*.
3. Aufl.
Berlin; Heidelberg; New York: Springer, 2003.

EISENBUD, David:
Graduate Texts in Mathematics. Bd. 150: *Commutative Algebra: with a View Toward Algebraic Geometry*.
New York; Berlin; Heidelberg: Springer, 1995.

EISENBUD, David; HARRIS, Joe:
Graduate Texts in Mathematics. Bd. 197: *The Geometry of Schemes*.
Corrected 2nd printing.
New York; Berlin; Heidelberg: Springer, 2001.

EISENBUD, David; GREEN, Mark; HARRIS, Joe:
„Cayley-Bacharach Theorems and Conjectures“.
In: *Bulletin (New Series) of the American Mathematical Society* 35 (1996), Juli, Nr. 3, S. 295 – 324.
DOI 10.1090/S0273-0979-96-00666-0.

FULTON, William:
Mathematics Lecture Note Series. Bd. 30: *Algebraic Curves: An Introduction to Algebraic Geometry*.
Menlo Park, California: The Benjamin/Cummings Publishing Company, 1969.
`http://www.math.lsa.umich.edu/~wfulton/`.
Vergriffen, erhältlich auf der Internetseite des Autors.

GOLD, Leah; LITTLE, John; SCHENCK, Hal:
„Cayley–Bacharach and Evaluation Codes on Complete Intersections“.
In: *Journal of Pure and Applied Algebra* 196 (2005), März, Nr. 1, S. 91 – 99.
DOI 10.1016/j.jpaa.2004.08.015.

GOPPA, Valerii Denisovich:
„Codes on Algebraic Curves“.
In: *Soviet Mathematics - Doklady* 24 (1981), März, Nr. 1, S. 170 – 172.

HAMMING, Richard W.:
„Error Detection and Error Correction Codes“.
In: *The Bell System Technical Journal* XXIX (1950), April, Nr. 2, S. 147 – 160.
`http://guest.engelschall.com/~sb/hamming/`.

HANSEN, Johan P.:
„Points in Uniform Position and Maximum Distance Separable Codes“.
In: ORECCHIA, Feruccio (Hrsg.); CHIANTINI, Luca (Hrsg.): *Zero-Dimensional Schemes: Proceedings of the International Conference held in Ravello, June 8–13, 1992*.
Berlin; New York: de Gruyter, 1994, S. 205 – 211.

HANSEN, Johan P.:
„Linkage and Codes on Complete Intersections“.
In: *Applicable Algebra in Engineering, Communication and Computing* 14 (2003), Oktober, Nr. 3, S. 175 – 185.
DOI 10.1007/s00200-003-0119-3.

HARTSHORNE, Robin:
Graduate Texts in Mathematics. Bd. 52: *Algebraic Geometry*.
14th ed.
Springer, 1977.

HØHOLDT, Tom; LINT, Jacobus Hendricus van; PELLIKAAN, Ruud:
„Algebraic Geometry Codes“.
`www.win.tue.nl/~ruudp/paper/31.pdf`.
In: PLESS, V. S. (Hrsg.); HUFFMAN, W. C. (Hrsg.): *Handbook of Coding Theory* Bd. 1.
Amsterdam: Elsevier, 1998, Kapitel 10, S. 871 – 961.
Kapitel auf der Internetseite von R. Pellikaan erhältlich.

HOLZER, S.; LABS, O.:
surfex.
`www.surfex.AlgebraicSurface.net`.
Version: 0.90, 2008.
Programm zur Visualisierung algebraischer Flächen.

IVERSEN, Birger:
Cohomology of Sheaves.
Berlin; Heidelberg; New York: Springer, 1986 (Universitext).

KATO, Goro:
The Heart of Cohomology.
Dordrecht: Springer, 2006.

KUNZ, Ernst:
Einführung in die algebraische Geometrie.
Braunschweig; Wiesbaden: Vieweg, 1997.

LANG, Serge:
Graduate Texts in Mathematics. Bd. 211: *Algebra*.
Rev. 3rd ed.
New York; Berlin; Heidelberg: Springer, 2002.

LINT, Jacobus Hendricus van:
Graduate Texts in Mathematics. Bd. 86: *Introduction to Coding Theory*.
3rd rev. and expanded ed.
Berlin; Heidelberg: Springer, 1999.

LINT, Jacobus Hendricus van; GEER, Gerard van der:
DMV Seminar. Bd. 12: *Introduction to Coding Theory and Algebraic Geometry*.
Birkhäuser, 1988.

LITTLE, John; SAINTS, Keith; HEEGARD, Chris:
„On the Structure of Hermitian Codes".
In: *Journal of Pure and Applied Algebra* 121 (1997), Oktober, Nr. 3, S. 293 – 314.
DOI 10.1016/S0022-4049(96)00067-9.

LIU, Qing:
Oxford Graduate Texts in Mathematics. Bd. 6: *Algebraic Geometry and Arithmetic Curves*.
Transl. from the French by Reinie Erné.
Oxford: Oxford University Press, 2002.

LÜKE, Hans Dieter:
„The Origins of the Sampling Theorem".
In: *IEEE Communications Magazine* 37 (1999), April, Nr. 4, S. 106 – 108.
DOI 10.1109/35.755459.

LÜTKEBOHMERT, Werner:
Codierungstheorie.
1. Aufl.
Braunschweig; Wiesbaden: Vieweg, 2003.

MATSUMURA, Hideyuki:
Mathematics Lecture Note Series. Bd. 56: *Commutative Algebra*.
2nd ed.
London: The Benjamin/Cummings Publishing Company, 1980.

RENTERÍA, C.; TAPIA-RECILLAS, H.:
„Reed-Muller Codes: an Ideal Theory Approach".
In: *Communications in Algebra* 25 (1997), Nr. 2, S. 401 – 413.
DOI 10.1080/00927879708825862.

SHANNON, Claude Elwood:
„A Mathematical Theory of Communication".
In: *The Bell System Technical Journal* XXVII (1948), Juli, Oktober, Nr. 3, S. 379 – 423, 623 – 656.

SILVERMANN, Joseph H.; TATE, John:
Rational Points on Elliptic Curves.
New York; Berlin; Heidelberg: Springer, 1992 (Undergraduate Texts in Mathematics).

STICHTENOTH, Henning:
„A Note on Hermitian Codes over GF(q^2)“.
In: *IEEE Transactions on Information Theory* 34 (1988), September, Nr. 5, S. 1345 – 1348.
DOI 10.1109/18.21267.

STICHTENOTH, Henning:
Algebraic Function Fields and Codes.
Berlin; Heidelberg; New York: Springer, 1993 (Universitext).

STRUIK, Dirk Jan:
A Source Book in Mathematics, 1200-1800.
Princeton, New Jersey: Princeton University Press, 1986.

TSFASMAN, M. A.; VLĂDUŢ, S. G.:
Mathematics and Its Applications. Soviet Series. Bd. 58: *Algebraic-Geometric Codes*.
Dordrecht: Kluwer, 1991.