AUDIO CDS UND REED-SOLOMON CODES

BENJAMIN KLOPSCH

Zusammenfassung. Dieser Aufsatz basiert auf einem Vortrag, den ich im Rahmen des Seminars "Kodierungstheorie" im Wintersemester 2001/02 gehalten habe. Anhand eines ganz konkreten Beispiels, nämlich der handelsüblichen Audio CD, soll der Einsatz der mathematischen Kodierungstheorie im praktischen Alltag aufgezeigt werden. Im ersten Teil wird das grundlegende Prinzip der Datenspeicherung auf einer solchen Audio CD erläutert. Im zweiten Teil werden die dabei zur Verwendung kommenden Reed-Solomon Codes mathematisch durchleuchtet.

1. Einleitung

Vor nunmehr fast zwanzig Jahren kamen die ersten Musik Compact Discs in den Handel. Sehr schnell lösten sie die bis dahin üblichen Langspielplatten als Verbreitungsmedium für Tonaufnahmen ab. Neu war, daß die Musik nun *digital* (d.h. als Folge von Nullen und Einsen) und nicht mehr analog auf dem Datenträger gespeichert wurde. Neu war auch, daß die Musikinformationen *per Laser* und nicht mehr durch direkten mechanischen Kontakt (zum Beispiel über eine Nadel) vom CD Spieler abgetastet wurden. Soviel ist eigentlich jedem bekannt.

Hält man eine CD ins Licht, so kann man die auf ihr gespeicherten Nullen und Einsen in allen Regenbogenfarben schillern sehen. Was man vielleicht nicht unbedingt sieht, ist, daß eine hochwertige CD selbst bei sorgfältiger Behandlung unheimlich viele Fehler aufweisen kann. Bei genauerem Hinsehen erkennt man wohlmöglich Kratzer, Fingerabdrücke oder ähnliches. Trotzdem läßt sich eine solche fehlerbehaftete CD in der Regel ohne merkbare Qualitätseinbußen abspielen—ein kleines Wunder.

Dahinter stehen natürlich eine Vielzahl technischer Klügeleien und ein langer Entwicklungsprozeß. Maßgeblich für die Korrektur von Fehldaten auf einer CD sind insbesondere die sogenannten *Reed-Solomon Codes*, die bei der Datenspeicherung und im späteren Lesevorgang ihre Anwendung finden. Diese Codes wurden von ihren beiden Konstrukteuren bereits im Jahre 1960 (in einer Arbeit mit dem unscheinbaren Titel "Polynomial Codes over Certain Finite Fields") vorgestellt, also zu einer Zeit, als die Kodierungstheorie noch in den Kinderschuhen steckte.

Im ersten Teil dieses Aufsatzes beschreibe ich kurz, auf welche Weise Informationen auf einer Audio CD abgespeichert sind. Ich bin in diesem Bereich wahrlich kein Experte und habe einfach im Internet hin- und hergelesen. Besonders hilfreich fand ich dabei die folgenden Seiten:

- G. Erickson, *Compact Disc Player*, WWW Dokument (http://www.digitalcentury.com/encyclo/update/cdplayer.html),
- K. Kuhn, *Audio Compact Disk - An Introduction*, WWW Dokument (http://www.ee.washington.edu/conselec/CE/kuhn/cdaudio/95x6.htm).

Im zweiten Teil behandle ich dann in Grundzügen die mathematische Struktur der Reed-Solomon Codes. Details finden sich zum Beispiel in dem Buch *Designs and Their Codes* [1]. Interessant ist auch der Aufsatz *Some error-correction codes and their applications* von J.D. Key [2, Kapitel 14], in dem weitere praktische Anwendungen der Kodierungstheorie dargestellt werden.

2. Datenspeicherung auf einer Audio Compact Disc

Schon der Herstellungsprozeß einer CD ist eine komplizierte und durchaus spannende Geschichte. Darauf soll hier aber gar nicht weiter eingegangen werden. Vielmehr geht es darum, den grundsätzlichen Aufbau einer CD und im Zusammenhang damit ihre Funktionsweise kurz zu beschreiben. Eine wichtige Tatsache, die man sich immer wieder vor Augen halten muß, ist, daß digitale Informationen (d.h. eine Kette von Nullen und Einsen) nie direkt und unbehandelt auf eine Audio CD geschrieben, sondern zuvor mehrfach umgewandelt und präpariert werden. In angemessener Kürze soll erklärt werden, wie aus den ursprünglich vorliegenden Informationen die dann tatsächlich abgespeicherte Zeichenkette gewonnen wird.

2.1. **Die Audio CD – genauer hingeguckt.** Die technischen Vorgaben für das übliche Audio CD System sind in einem gemeinsamen Standard festgeschrieben (Sony, Philips, Polygram 1982). Dort finden sich unter anderem Angaben zur äußeren Erscheinungsform einer CD, technische Abmachungen bezüglich des Lesevorgangs sowie Vorschriften zur Datenverarbeitung.

Festgeschrieben sind zunächst die äußeren Maße einer CD (Durchmesser, Dicke, Durchmesser des Innenloches) sowie die Begrenzungen des bespielbaren Bereichs. Die Informationskette von Nullen und Einsen wird mittels Einbuchtungen auf einer von innen nach außen laufenden Spur auf die CD geschrieben. Dabei sind vorgegeben die Rotationsrichtung, der Spurabstand, die Ausmaße der Einbuchtungen. Das zur Herstellung einer CD verwandte Material muß einen geeigneten Brechungsindex besitzen.

Tabelle 1. Einige technische Vorgaben des Standards

Durchmesser	120 mm
Dicke	1.2 mm
Innenlochdurchmesser	15 mm
Radien des bespielbaren Bereichs	46 – 117 mm
Brechungsindex des Materials	1.55
Spurabstand	1.6 μm
Einbuchtungsbreite	0.5 μm
Einbuchtungstiefe	0.11 μm
Einbuchtungslänge	0.83 – 3.56 μm
Wellenlänge des Laserlichtes	780 nm

Die angegebenen Maße, zum Beispiel für Spur und Einbuchtungen, sind natürlich nicht willkürlich, sondern in Hinblick auf die optischen Vorgänge beim Lesen einer CD geeignet gewählt; siehe unten. Zum Größenvergleich: ein menschliches Haar ist

so zwischen 50 und 100 μm breit. Schließlich sind die technischen Vorgaben so vereinbart, daß sich für eine Audio CD eine maximale Spiellänge von 74 Minuten und 33 Sekunden ergibt, ein akzeptables Ergebnis.

Grundsätzlich besteht eine Audio CD aus zwei lichtdurchlässigen Kunststoffplatten, zwischen denen eine reflektierende Metallschicht liegt. Auf der Metallschicht sind entlang einer Spur die Musikdaten in Form von kleinen Einbuchtungen vermerkt. Gelesen wird eine CD stets von unten, das Label ist oben aufgedruckt. Die obere Kunststoffabdeckung ist dünner als die untere, so daß die empfindliche Metallschicht auch leicht von oben beschädigt werden kann.

Das Lesen einer CD geschieht über einen Infrarotlaser. (Das Infrarotlicht liegt unterhalb des für Menschen sichtbaren Lichtspektrums.) Durch den Eintritt in die untere Plasikhälfte einer CD wird der Laserstrahl gebrochen und dadurch automatisch gebündelt. Er trifft auf die innere Metallschicht, wird reflektiert und über eine Photozelle vom CD Spieler wieder aufgenommen. An einem Übergang in eine Einbuchtung hinein oder aus einer solchen heraus fallen zwei Strahlen zurück: der eine ist bis in die Einbuchtung hinein und heraus gelaufen, der andere nicht. Dadurch sind die Wellenzüge der beiden Strahlen zueinander verschoben, und es kommt zu einer destruktiven Interferenz. Effektiv wird an solchen Übergangsstellen kein Licht reflektiert und damit ein Signal an den CD Spieler übermittelt. Der eben beschriebene Interferenzvorgang ist in Wahrheit natürlich etwas komplizierter. Außerdem werden weitere optische Phänomene (wie zum Beispiel Diffraktion und Polarisation) technisch ausgenutzt.

2.2. **Musik aus Nullen und Einsen.** Die Umwandlung eines analogen Tonsignals, zum Beispiel Beethovens 9. Sinfonie gespielt vom Isländischen Staatsorchester, in eine digitale Informationskette und umgekehrt ist eine Wissenschaft für sich. Grundsätzlich wird die Musik über zwei Kanäle (entsprechend linkem und rechtem Ohr) 44100 mal in der Sekunde abgetastet. Jedem einzelnen Sample wird ein Signalwert zwischen 0 und $2^{16} - 1$ zugeordnet; das entspricht 16 Bits, also einer Folge von 16 Nullen oder Einsen. Für die beiden Kanäle zusammen ergeben sich also 32 Bits an Informationen pro Sample, und somit $44100 \times 32 = 1411200$ Bits pro Sekunde. Die Abtastfrequenz ist so gewählt, daß auch die höchsten vom menschlichen Ohr wahrnehmbaren Frequenzen (ungefähr 20000 Hz) klangecht widergegeben werden können.

Durch Aneinanderreihung der einzelnen Sample-Ergebnisse ergibt sich die ursprüngliche Informationskette aus Nullen und Einsen, die auf einer CD festgehalten werden soll. Diese Kette wird aber *nicht* direkt auf die CD geschrieben, sondern zuvor zahlreichen Umformungen unterzogen. Dadurch wird gewährleistet, daß mögliche Schreib- oder Lesefehler später weitesgehend ausgebügelt werden können.

Jeweils sechs Samples, also insgesamt $6 \times 32 = 192$ Bits, werden in einer Einheit, einem sogenannten *frame*, zusammengefaßt. Tatsächlich werden aber für jeden frame ganze 588 Bits auf die CD geschrieben. Dies erklärt sich wie folgt.

Zunächst wird die ursprüngliche Informationskette kodiert. Dazu benutzt man einen sogenannten *Cross Interleaved Reed-Solomon Code* (CIRC). Das *interleaving*, also die Verschachtelung von Daten, bedeutet nichts anderes als die Neuverteilung von Ziffern (oder Buchstaben) nach einem vorgegeben Prinzip. Dadurch wird verhindert, daß es zu totalen lokalen Datenverlusten kommen kann (zum Beispiel durch

einen Kratzer auf der CD Oberfläche). Am besten läßt sich dieses Verfahren an einem Beispiel erklären.

> Angenommen, ich möchte Paola auf einem Stück Papier die Botschaft "WARMER APFELKUCHEN" zukommen lassen (weil ich mir warmen Apfelkuchen zum Geburtstag wünsche).
>
> Schreibe ich "WARMER APFELKUCHEN" direkt auf einen kleinen Zettel und zerläuft in der Mitte die Tinte, so erhält Paola nur die Information "WARMER .....KUCHEN". Das könnte alles mögliche bedeuten, zum Beispiel "WARMER PFANNKUCHEN". Treffen Paola und ich aber die Abmachung, die Buchstaben immer um fünf versetzt zu schreiben, so gebe ich ihr die verschachtelte Nachricht "WPHEKA FERURENACML". Wieder geht der mittlere Teil verloren. Paola erhält nur noch "WPHEKA .....ENACML" und liest dies als "WA.ME. AP.ELK.CH.N". Der Informationsverlust tritt nun nicht mehr konzentriert an einer Stelle, sondern weitgestreut auf, und die Nachricht läßt sich viel einfacher rekonstruieren.
>
> Genau dieses Prinzip wird beim Speichern von Daten auf einer CD benutzt. Der CD Spieler liest also immer schon Werte im voraus ein und gibt die zugehörigen Musiktöne erst nach Entschachtelung, also mit einer gewissen Zeitverzögerung aus.

Ein weiterer wichtiger Schritt in der Bearbeitung der Informationskette ist die eigentliche Kodierung. Dazu werden zwei verkürzte *Reed-Solomon Codes* über dem Körper $\mathbb{F}_{2^8}$ mit 2^8 Elementen verwendet. Diese Codes werden in Abschnitt 3.5 näher beschrieben. Entscheiden ist, daß der ursprünglichen Informationskette zusätzliche Prüfziffern angefügt werden. Die zunächst $192 = 24 \times 8$ Bits eines frames lassen sich als Folge von 24 Elementen aus $\mathbb{F}_{2^8}$ deuten. Ihnen werden 8 weitere Elemente des Körpers, entsprechend $8 \times 8 = 64$ Bits, angefügt.

Verschachtelung und Kodierung werden wiederholt hintereinander durchgeführt. Anschließend wird jedem frame ein sogenannter *subcode* vorangestellt, der zum Beispiel über die Länge der einzelnen Stücke auf einer CD Auskunft gibt. Dann werden alle Daten einer *Eight to Fourteen Modulation* (EFM) unterzogen: Je acht Bits an Informationen werden auf vierzehn Bits ausgewalzt, um die Anzahl der Übergänge von Null zu Eins oder umgekehrt zu beschränken. Dadurch soll das Auftreten kleiner Einbuchtungen auf der CD vermieden werden. Schließlich wird jedem frame ein 24-Bit langes *synchronization word* vorangestellt, und je zwei aufeinanderfolgende Gruppen von nun 14 Bits werden durch drei weiter Bits miteinander verbunden.

Tabelle 2. Gesamtanzahl der geschriebenen Bits für einen frame

Datenbits (nach EFM)	$24 \times 14 = 336$
Kodierungsbits (nach EFM)	$8 \times 14 = 112$
Subcode-Bits (nach EFM)	14
Synchronisationsbits	24
Verbindungsbits	$34 \times 3 = 102$
Summe	588

Jeder frame, der zunächst aus nur 192 Informationsbits besteht, veranschlagt, wie die Rechnung zeigt, nach allen beschriebenen Manipulationen sage und schreibe 588 Bits.

3. Die Mathematik hinter den Reed-Solomon Codes

Nicht nur für die Audio CD, sondern auch in vielen anderen technischen Anwendungen spielen lineare Codes eine wichtige Rolle. Grundlegend für das Verständnis dieser mathematischen Objekte sind die Begriffe und Sätze der Linearen Algebra, mit denen üblicherweise auch ein Mathematikstudium an der Universität beginnt. Die Konstruktionsverfahren für kompliziertere Codes beruhen vielfach auf tieferliegenden Resultaten aus der Zahlentheorie, Kombinatorik oder auch algebraischen Geometrie. Einen klitzkleinen Eindruck hiervon kann man auch schon durch das Studium der Reed-Solomon Codes gewinnen, obschon dieses gar kein Spezialwissen erfordert.

Für die folgende Diskussion setze ich stillschweigend die Bekanntschaft mit Begriffen wie Untervektorraum, Kern einer linearen Abbildung oder Hauptidealring voraus. Falls nötig, können diese ohne Schwierigkeiten in jedem Lehrbuch der Algebra nachgeschlagen werden.

3.1. **Lineare Codes.** Sei K ein endlicher Körper, und sei $n \in \mathbb{N}$. Bezeichne mit $V = K^n$ den n-dimensionalen Standardvektorraum über K. Das *Hamming Gewicht* eines Vektors $\mathbf{a} = (a_1, \ldots, a_n) \in V$ ist die Anzahl seiner von Null verschiedenen Komponenenten, also $w(\mathbf{a}) := \#\{i \mid a_i \neq 0\}$. Die *Hamming Metrik* auf V ist gegeben durch die Abstandsfunktion

$$d : V \times V \to \{0, 1, \ldots, n\}, \quad d(\mathbf{a}, \mathbf{b}) := w(\mathbf{a} - \mathbf{b});$$

man prüft leicht nach, daß (V, d) dann tatsächlich ein metrischer Raum ist. Der Abstand zweier Vektoren entspricht gerade der Anzahl der Komponenten, in denen sie sich unterscheiden.

Ein *linearer Code der Länge n über K* ist ein nicht-trivialer Untervektorraum von V. Die *Minimaldistanz* eines linearen Codes C ist

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

Ein $[n, k, d]$-*Code über K* ist ein linearer Code C der Länge n mit $\dim_K(C) = k$ und $d(C) = d$. Zum Beispiel werden bei der Audio CD zur Kodierung von Musikdaten lineare $[28, 24, 5]$- und $[32, 28, 5]$-Codes über dem Körper $\mathbb{F}_{2^8}$ verwendet.

> Was steckt nun prinzipiell hinter all diesen Definitionen und Abmachungen? Beim Abspielen einer CD wird eine Nachricht (eine Folge von Nullen und Einsen) von der CD an den CD Spieler übermittelt. Durch Kratzer auf der CD Oberfläche oder ähnliches wird diese Datenübertragung gestört, der CD Spieler muß also die eigentliche Informationskette immer erst aus den empfangenen Signalen rekonstruieren.
>
> Der Körper K dient sozusagen als Alphabet; im Falle des CD Spielers ist $K = \mathbb{F}_{2^8}$ ein Alphabet mit 256 Buchstaben. Vektoren aus V entsprechen Buchstabenketten der Länge n; für die Audio CD werden

Codes der Länge 28 und 32 benutzt. Die Elemente eines verabredeten Codes C sind die "grammatikalisch korrekt" gebildeten Wörter. Eine Botschaft ist eine Folge von Wörtern, also eine Kette $(\mathbf{w}_1, \ldots, \mathbf{w}_r)$ von, sagen wir, r Vektoren aus C. Durch Störungen bei der Übertragung werden einzelne Buchstaben, sprich Vektorkomponenten, fehlerhaft übermittelt. Der Empfänger erhält eine Folge $(\mathbf{w}'_1, \ldots, \mathbf{w}'_r)$ von r Buchstabenketten der Länge n. Die Hammingdistanz zwischen einem ursprünglichen Nachrichtenwort $\mathbf{w}_i$ und der empfangenen Buchstabenkette $\mathbf{w}'_i$ mißt gerade die Anzahl der falsch weitergegebenen Buchstaben innerhalb dieses einen Wortes. Ist die Minimaldistanz von C verhältnismäßig groß und treten nicht allzu viele Fehler auf, so kann das Wort $\mathbf{w}_i$ leicht aus $\mathbf{w}'_i$ rekonstruiert werden.

Ein zentrales Problem der Kodierungstheorie ist daher die Konstruktion von $[n, k, d]$-Codes mit kleiner Codimension $n - k$ und großer Minimaldistanz d.

3.2. **Erzeugenden- und Checkmatrix.** Sei K ein endlicher Körper, und sei C ein $[n, k, d]$-Code über K. Als Untervektorraum von K^n läßt sich C auf verschiedene Weisen konkret angeben.

Ist $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ eine Basis von C und $\mathbf{b}_i = (b_{i,1}, \ldots, b_{i,n})$, so wird

$$E := \begin{pmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \\ \vdots \\ \mathbf{b}_k \end{pmatrix} = \begin{pmatrix} b_{1,1} & b_{1,2} & \cdots & b_{1,n} \\ b_{2,1} & b_{2,2} & \cdots & b_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{k,1} & b_{k,2} & \cdots & b_{k,n} \end{pmatrix} \in \mathrm{Mat}_{k,n}(K)$$

eine *Erzeugendenmatrix* von C genannt[1]. Offenbar bestimmt E den Code eindeutig.

Genausogut läßt sich C als Kern einer linearen Abbildung $K^n \to K^{n-k}$ beschreiben. Eine zugehörige Matrix

$$H = \begin{pmatrix} \mathbf{h}_1^t & \mathbf{h}_2^t & \cdots & \mathbf{h}_{n-k}^t \end{pmatrix} = \begin{pmatrix} h_{1,1} & h_{1,2} & \cdots & h_{1,n-k} \\ h_{2,1} & h_{2,2} & \cdots & h_{2,n-k} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n,1} & h_{n,2} & \cdots & h_{n,n-k} \end{pmatrix} \in \mathrm{Mat}_{n,n-k}(K)$$

heißt *Checkmatrix* für C. Auch sie bestimmt C eindeutig. Die Vektoren

$$\mathbf{h}_1 = (h_{1,1}, \ldots, h_{n,1}), \quad \ldots, \mathbf{h}_{n-k} = (h_{1,n-k}, \ldots, h_{n,n-k})$$

bilden eine Basis für das orthogonale Komplement $C^\perp$ von C in K^n. Anhand einer Checkmatrix H läßt sich zudem die Minimaldistanz des zugehörigen Codes C ablesen. Ist $1 \leq d \leq n$, so gilt $d(C) \geq d$ genau dann, wenn je $d - 1$ paarweise verschiedene Zeilen von H linear unabhängig sind. Vor allem für die Dekodierung sind Checkmatrizen auch von praktischem Interesse.

3.3. **Maximum Distance Separable Codes.** Sei K ein endlicher Körper. Wie schon erwähnt, können bei vorgegebener Länge n die Dimension und Minimaldistanz eines Codes nicht gleichzeitig nahe ihres Maximalwertes n liegen. Eine der einfachsten Einschränkungen wird durch den folgenden Satz ausgesprochen.

[1]Ich schreibe Vektoren gerne als Zeilen; lineare Abbildungen operieren dann natürlicherweise von rechts.

Satz 3.1 (Singleton Schranke)**.** *Sei C ein $[n,k,d]$-Code über K. Dann gilt*

$$n \geq k + d - 1.$$

Beweis. Bezeichne mit $\pi : K^n \to K^{n-d+1}$, $(a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_{n-d+1})$ die Projektion auf die ersten $n-d+1$ Koordinaten. Da C die Minimaldistanz d besitzt, ist die Einschränkung von π auf C injektiv. Also gilt

$$n - d + 1 \geq \dim_K(\pi(C)) = \dim_K(C) = k,$$

und damit $n \geq k + d - 1$. □

Ein $[n,k,d]$-Code heißt *Maximum Distance Separable*, oder kurz MDS, falls $n = k+d-1$. In gewisser Hinsicht sind MDS Codes also optimal, aber nur in gewisser Hinsicht. In Abschnitt 3.5 wird sich zeigen, daß die uns interessierenden Reed-Solomon Codes MDS Codes sind.

3.4. **Zyklische Codes.** Eine spezielle Klasse von linearen Codes sind die sogenannten zyklischen Codes. Sei K wieder ein endlicher Körper, und sei $n \in \mathbb{N}$. Ein linearer Code $C \leq K^n$ heißt *zyklisch*, falls C invariant ist unter zyklischer Vertauschung der Koordinaten, d.h. $(a_1, \ldots, a_n) \in C$ impliziert $(a_n, a_1, \ldots, a_{n-1}) \in C$.

Algebraisch läßt sich diese Eigenschaft wie folgt deuten. Der Restklassenring $R := K[X]/(X^n-1)$ ist ein n-dimensionaler K-Vektorraum mit Basis $(1, \overline{X}, \overline{X}^2, \ldots, \overline{X}^{n-1})$. Bezeichne mit Φ den linearen Isomorphismus $K^n \to R$, $(a_1, \ldots, a_n) \mapsto \sum_{i=1}^n a_i \overline{X}^{i-1}$. Dann gilt: Ein linearer Code $C \leq K^n$ ist zyklisch genau dann, wenn $\Phi(C)$ ein Ideal von R ist. Dies liegt einfach daran, daß der zyklischen Vertauschung der Komponenten von $\mathbf{a} \in C$ gerade die Multiplikation von $\Phi(\mathbf{a})$ mit $\overline{X}$ entspricht.

Da $K[X]$ ein Hauptidealring ist, hat jedes Ideal von R die Form $(\overline{f})$, wobei $f \in K[X]$ ein Teiler von X^n-1 ist. Die Primfaktorzerlegung des n-ten Kreisteilungspolynoms $X^n - 1$ über dem endlichen Körper K führt also, zumindest theoretisch, zu einer Klassifizierung aller zyklischen Codes der Länge n über K.

3.5. **Konstruktion und Eigenschaften von Reed-Solomon Codes.** Die zu behandelnden Reed-Solomon Codes können eigentlich als Spezialfälle der sogenannten BCH Codes angesehen werden; siehe [1]. Die allgemeinere Theorie dieser von Bose, Ray-Chaudhuri und Hocquenghem entwickelten Codes kann hier aber leider nicht dargestellt werden. Stattdessen gebe ich eine direkte und ein wenig vereinfachte Konstruktionsmethode für Reed-Solomon Codes an.

Sei K ein endlicher Körper mit q Elementen. Wähle $n, d \in \mathbb{N}$ mit $n \mid (q-1)$ und $2 \leq d \leq n$. Die multiplikative Gruppe $K^\times$ ist zyklisch der Ordnung $q-1$. Also finden wir eine primitive n-te Einheitswurzel $\alpha \in K$. Das Polynom

$$g := (X - \alpha)(X - \alpha^2) \cdots (X - \alpha^{d-1}) \in K[X] \tag{3.1}$$

hat $d-1$ verschiedene Nullstellen $\alpha, \ldots, \alpha^{d-1} \in K$. Jedes dieser Elemente ist auch Nullstelle des Polynoms $X^n - 1$, also gilt $g \mid (X^n - 1)$.

Wie im vorhergehenden Paragraphen bezeichne $\Phi : K^n \to K[X]/(X^n-1)$ den naheliegenden linearen Isomorphismus. Der zu dem Ideal $(\overline{g})$ gehörige zyklische Code $C := \Phi^{-1}(\overline{g}) \leq K^n$ heißt *Reed-Solomon Code*. Ist $n = q - 1$, so spricht man von einem *primitiven* Reed-Solomon Code. Die wichtigsten Eigenschaften von C werden durch den folgenden Satz vollständig geklärt.

Satz 3.2. *Der oben konstruierte Reed-Solomon Code C hat Minimaldistanz $d(C) = d$ und Dimension $\dim_K(C) = n - d + 1$. Insbesondere ist C ein MDS Code.*

Beweis. Sei

$$H := \begin{pmatrix} 1 & 1 & 1 & \cdots & 1 \\ \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{d-1} \\ \alpha^2 & \alpha^4 & \alpha^6 & \cdots & \alpha^{(d-1)2} \\ \vdots & \vdots & \vdots & & \vdots \\ \alpha^{n-1} & \alpha^{2(n-1)} & \alpha^{3(n-1)} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix} \in \mathrm{Mat}_{n,d-1}(K), \tag{3.2}$$

und bezeichne mit $\eta : K^n \to K^{d-1}$ die dazugehörige lineare Abbildung bezüglich der Standardbasen. Wir zeigen zunächst, daß $C = \mathrm{kern}(\eta)$ ist.

Sei also $\mathbf{a} = (a_1, \ldots, a_n) \in K^n$. Dann sind aufgrund der Definition von C, g und H die folgenden Aussagen paarweise äquivalent. Der Vektor $\mathbf{a}$ liegt in C. Das Bild $\sum_{i=1}^n a_i \overline{X}^{i-1}$ von $\mathbf{a}$ unter Φ liegt in dem Ideal $(\overline{g})$. Das Polynom $\sum_{i=1}^n X^{i-1}$ hat Nullstellen $\alpha, \ldots, \alpha^{d-1}$. Der Vektor $\mathbf{a}$ liegt in $\mathrm{kern}(\eta)$.

Somit gilt $C = \mathrm{kern}(\eta)$, wie behauptet. Offenbar ist H eine sogenannte Vandermonde Matrix, und $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ sind paarweise verschieden. Daher hat H den Rang $d - 1$, und darüber hinaus sind je $d - 1$ Zeilen von H linear unabhängig. Es folgt, daß die Minimaldistanz von C genau d ist und daß der Kern von η, also C, die Dimension $n - d + 1$ hat. □

Der eben geführte Beweis liefert mit (3.2) automatisch eine Checkmatrix für den Code C. Auch eine Erzeugendenmatrix läßt sich leicht finden. Dazu multipliziert man das Produkt auf der rechten Seite von (3.1) explizit aus:

$$g = g_0 + g_1 X + \ldots + g_{d-1} X^{d-1} \qquad \text{mit Koeffizienten } g_i \in K.$$

Dann läßt sich leicht feststellen, daß

$$G := \begin{pmatrix} g_0 & g_1 & \cdots & g_{d-1} & 1 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{d-1} & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{d-1} & 1 \end{pmatrix} \in \mathrm{Mat}_{n-d+1,n}(K)$$

eine Erzeugendenmatrix für den Code C liefert.

Aus G kann man übrigens auch eine Checkmatrix herleiten. Dazu bringt man durch elementare Zeilenumformungen die Matrix G zunächst auf die Gestalt

$$G' = \begin{pmatrix} I_{n-d+1} & A \end{pmatrix} \in \mathrm{Mat}_{n-d+1,n}(K)$$

wobei I_{n-d+1} die Einheitsmatrix und A eine geeignete $(n - d + 1) \times (d - 1)$ Matrix bezeichnen. In dieser Darstellung sind die $n - d + 1$ Informationseinträge sozusagen deutlich von den $d - 1$ Prüfeinträgen getrennt. Nun liefert

$$H' := \begin{pmatrix} -A \\ I_{d-1} \end{pmatrix} \in \mathrm{Mat}_{n,d-1}(K)$$

die gewünschte Checkmatrix, denn offensichtlich gilt die Matrizengleichung

$$G'H' = -A + A = 0.$$

3.6. **Ein explizites Beispiel.** Bevor ich erkläre, welche Art von Reed-Solomon Codes nun tatsächlich für die Audio CD verwendet werden, möchte ich die vorstehende Diskussion noch mit einem konkreten Beispiel abrunden.

Sei dazu K ein Primkörper mit $q = 11$ Elementen, $n = 5$ und $d = 3$. Dann teilt n natürlich $q - 1 = 10$, und wir suchen eine primitive 5-te Einheitswurzel in K. Dazu rechnen wir nach:

$$2^1 \equiv_{11} 2, \qquad 2^2 \equiv_{11} 4, \qquad 2^3 \equiv_{11} 8, \qquad 2^4 \equiv_{11} 5, \qquad 2^5 \equiv_{11} 10 \equiv_{11} -1.$$

Also ist 2 ein primitives Element von K, und $\alpha := 4$ ist eine primitive 5-te Einheitswurzel.

Als nächstes bilden wir das Polynom

$$g = (X - 4)(X - 4^2) = (X - 4)(X - 5) = 9 + 2X + X^2 \in K[X].$$

Der zugehörige Reed-Solomon Code C hat also die Erzeugendenmatrix

$$G = \begin{pmatrix} 9 & 2 & 1 & 0 & 0 \\ 0 & 9 & 2 & 1 & 0 \\ 0 & 0 & 9 & 2 & 1 \end{pmatrix}.$$

Eine Checkmatrix für C können wir auf zweierlei Weisen berechnen. Durch Einsetzen in (3.2) erhalten wir

$$H_1 := \begin{pmatrix} 1 & 1 \\ 4 & 4^2 \\ 4^2 & 4^4 \\ 4^3 & 4^6 \\ 4^4 & 4^8 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 4 & 5 \\ 5 & 3 \\ 9 & 4 \\ 3 & 9 \end{pmatrix}.$$

Andererseits können wir G durch elementare Zeilenumformungen auf Standardform bringen. Wegen $5 \cdot 9 \equiv_{11} 1$ erhalten wir

$$G \sim \begin{pmatrix} 1 & -1 & 5 & 0 & 0 \\ 0 & 1 & -1 & 5 & 0 \\ 0 & 0 & 1 & -1 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & -1 & 0 & 5 & 8 \\ 0 & 1 & 0 & 4 & 5 \\ 0 & 0 & 1 & -1 & 5 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 9 & 2 \\ 0 & 1 & 0 & 4 & 5 \\ 0 & 0 & 1 & -1 & 5 \end{pmatrix},$$

und nun ergibt sich die Checkmatrix

$$H_2 := \begin{pmatrix} -9 & -2 \\ -4 & -5 \\ 1 & -5 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 9 \\ 7 & 6 \\ 1 & 6 \\ 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Es ist nicht schwer nachzuprüfen, daß die zu H_1 und H_2 gehörigen linearen Abbildungen denselben Kern haben, nämlich C.

3.7. **Verkürzte Reed-Solomon Codes für die Audio CD.** Das Kürzen eines linearen Codes geschieht durch das folgende allgemeine Konstruktionsverfahren. Sei C ein $[n, k, d]$-Code, und sei $G = \begin{pmatrix} I_k & A \end{pmatrix}$ eine Erzeugendenmatrix für C in Standardform. Gegeben sei $1 \leq r < k$. Dann erhält man durch Wegstreichen der ersten r Zeilen und Spalten von G eine neue Matrix $G^* = \begin{pmatrix} I_{k-r} & A^* \end{pmatrix}$. Diese Matrix wird

nun als Erzeugendenmatrix für den *verkürzten* Code C^* interpretiert. Offensichtlich hat C^* die Länge $n-r$ und die Dimension $k-r$. Wie aber ändert sich die Minimaldistanz?

Beachte dazu, daß $H = \begin{pmatrix} -A \\ I_{n-k} \end{pmatrix}$ eine Checkmatrix für C darstellt. Durch Wegstreichen der ersten r Zeilen ergibt sich eine Checkmatrix $H^* = \begin{pmatrix} -A^* \\ I_{n-k} \end{pmatrix}$ für C^*. Da C die Minimaldistanz d hat, sind je $d-1$ Zeilen von H linear unabhängig. Also sind auch je $d-1$ Zeilen von H^* linear unabhängig, und die Minimaldistanz von C^* ist wenigstens d. Ist insbesondere C ein MDS Code, so gilt $n-r = (k-r)+d-1$, und die Abschätzung in Satz 3.1 zeigt, daß die Minimaldistanz von C^* gleich d ist. In diesem Falle ist also C^* ein $[n-r, k-r, d]$-Code.

Beim Audio CD System werden auf diese Weise *verkürzte* Reed-Solomon Codes verwendet. Zunächst konstruiert man über dem Körper $\mathbb{F}_{2^8}$ einen primitiven Reed-Solomon Code C der Länge $n = 2^8-1 = 255$ und Minimaldistanz $d = 5$. Die Dimension von C ist dann $k = n-d+1 = 251$. Dieser Code wird nun durch Steichen von 227 bzw. 218 Zeilen und Spalten zu einem $[28, 24, 5]$-Code C_1^* bzw. $[32, 28, 5]$-Code C_2^* verkürzt. Zusammen mit den in Abschnitt 2.2 erklärten Verschachtelungstechniken ergibt sich der vielbeschworene *Interleaved Reed-Solomon Code* der Audio CD.

Literatur

[1] E.F. Assmus und J.D. Key, *Designs and Their Codes* (Cambridge University Press, Cambridge, 1992).

[2] D.R. Shier und K.T. Wallenius, *Applied Mathematical Modeling: A Multidisciplinary Approach* (Chapman & Hall, London, 2000).

Mathematisches Institut,
Heinrich-Heine-Universität,
40225 Düsseldorf, Germany.

E-mail address: klopsch@math.uni-duesseldorf.de