EDUCETH
Das Bildungsportal der ETH Zürich

Publikation von www.educeth.ch

EAN, ISBN, CD, DVD: Von Prüfziffern zu fehlerkorrigierenden Codes

Eine Unterrichtseinheit von Urs Stammbach

Inhalt und Lernziele:
Bei der Übermittlung von Daten werden oft mathematische Methoden verwendet, um Übertragungsfehler zu vermeiden oder sogar zu korrigieren. Einige derartige Systeme werden beschrieben, bzw. deren prinzipielle Wirkungsweise erklärt.
Es soll gezeigt werden, wie in vielen Einrichtungen und Geräten des täglichen Lebens Mathematik als wesentliches Konstruktionselement verwendet wird.

Unterrichtsmethode:
Vortrag

Fachliches Review:
Urs Kirchgraber, Departement Mathematik, ETH Zürich

Fachdidaktisches Review:
Urs Kirchgraber, Departement Mathematik, ETH Zürich

Publiziert auf EducETH:
4. Mai 2007

Rechtliches:
Die vorliegende Unterrichtseinheit darf ohne Einschränkung heruntergeladen und für Unterrichtszwecke kostenlos verwendet werden. Dabei sind auch Änderungen und Anpassungen erlaubt. Der Hinweis auf die Herkunft der Materialien (ETH Zürich, EducETH) sowie die Angabe der Autorinnen und Autoren darf aber nicht entfernt werden.

Publizieren auf EducETH?
Möchten Sie eine eigene Unterrichtseinheit auf EducETH publizieren? Auf folgender Seite finden Sie alle wichtigen Informationen: http://www.educeth.ch/autoren

Weitere Informationen:
Weitere Informationen zu dieser Unterrichtseinheit und zu EducETH finden Sie im Internet unter http://www.educ.ethz.ch oder unter http://www.educeth.ch.

SCIENCE MEETS SCHOOL
EDUCETH.CH

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

EAN, ISBN, CD, DVD: Von Prüfziffern zu fehlerkorrigierenden Codes[1]

Urs Stammbach, Prof. em. ETH-Zürich
stammb@math.ethz.ch

Einleitung

Sie kennen alle die Diskussionen, in denen es um den Stellenwert der Mathematik im Gymnasium geht. Ich bin sicher, dass dabei von Ihrer Seite das Argument ins Feld geführt wird, die Mathematik spiele in der heutigen Wissenschaft und im heutigen Leben eine zentrale Rolle. Es sei deshalb nur natürlich, dass die Schule ihr einen entsprechend grossen Platz einräume. Ich bin überzeugt, dass dieses Argument bei allen, die hier in diesem Raum anwesend sind, auf Zustimmung stösst. Schwieriger wird es, das Argument in Diskussionen mit Personen zu vertreten, die in der Schule mit der Mathematik traumatische Erfahrungen gesammelt haben. Denn diese antworten darauf – für viele überzeugend – , sie hätten im Laufe ihres Lebens die gymnasiale Mathematik kaum gebraucht und hätten es trotzdem zu etwas gebracht. Vor Jahren gab es in der Presse zu diesem Thema eine Umfrage unter Prominenten: Man hatte keine Mühe, eine ganze Reihe von Personen zu finden, die es in der Tat im Leben zu etwas gebracht hatten und überzeugend darlegen konnten, Mathematik hätte dabei keine Rolle gespielt. Konkret erinnere ich mich an eine derartige Aussage von Christian Gross, dem Fussballtrainer vom FC Basel. In der Tat, die Fähigkeit bis 11 zu zählen, erwirbt man nicht erst im Gymnasium! Es hätte Gross allerdings zu denken geben müssen, dass Ottmar Hitzfeld damals schon ein erfolgreicherer Fussballtrainer war als er selbst – Ottmar Hitzfeld, der ehemalige Mathematiklehrer!

Doch Spass beiseite! Man ist tatsächlich als Mathematiker bei dem erwähnten Argument etwas im Notstand. Der Grund dafür scheint mir der folgende zu sein: Zwar spielt die Mathematik im täglichen Leben eine grosse Rolle, aber sie ist oft unsichtbar, weil sie in zahlreichen Geräten versteckt ist, die wir, ohne viel zu denken, einfach so benützen. Aber wenn man als Gymnasiast oder Gymnasiastin die Grundlagen des heutigen Lebens verstehen will, so sollte man nicht nur wissen, auf welchen Prinzipien ein Elektromotor oder eine Viertaktautomotor funktioniert, weshalb ein Flugzeug fliegen, weshalb ein Schiff aus Stahl schwimmen kann, sondern man sollte auch etwas Bescheid darüber wissen, was im Supermarkt an der Kasse vor sich geht, was beim Abspielen einer CD geschieht, was beim Gebrauch eines Handys alles abläuft, etc. Es wird dabei nicht um die Details der Funktion der Geräte gehen, – das macht

[1] Vortrag gehalten am *17. Schweizerischen Tag über Mathematik und Unterricht*, Kantonsschule Zürcher Unterland Bülach, 20. September 2006

schon das Beispiel mit dem Elektromotor deutlich – sondern um die Prinzipien, um die Grundlagen, auf denen die Geräte basieren.

In diesem Geist möchte ich Ihnen in diesem Vortrag einige konkrete Beispiele vorführen. Die Mathematik ist in den entsprechenden Geräten so gut versteckt, dass man sich ihrer in der Tat nicht bewusst wird; aber ohne die Mathematik wäre die Konstruktion solcher Geräte gar nicht möglich. Das Bewusstmachen dieser Tatsache scheint mir im heutigen Mathematikunterricht wichtig zu sein.

Noch ein Wort zur Darstellung, die ich für den Vortrag wähle. Der erste Teil des Vortrages halte ich mit Absicht mathematisch sehr elementar; ich glaube, man könnte diesen Teil fast Eins zu Eins im Gymnasialunterricht verwenden. In der Tat habe ich dies im Rahmen einer Studienwoche für Gymnasiasten und Gymnasiastinnen an der ETH mit Erfolg einmal ausgetestet. Im zweiten Teil geht es – wie Sie sehen werden – noch mehr als im ersten Teil "nur" um Prinzipien und weniger um handfeste Mathematik; aber wie ich oben angedeutet habe, sind es gerade diese Prinzipien, deren Vermittlung mir wichtig erscheint, viel wichtiger jedenfalls als die mathematischen Details.

Nun also zum ersten Beispiel, das ich Ihnen vorstellen will.

Strichcode

EAN-Etiketten kennt jedermann (siehe Abb. 1). Ältere wissen noch, wie

Abb. 1. EAN-Etikette, Strichcode und zugehörige Ziffernfolge (unten)

früher im Supermarkt an der Kasse für jedes Produkt der Preis eingetippt wurde und die Kasse dann am Ende die eingetippten Beträge addiert hat. Heute ist das anders: Die Person an der Kasse zieht die EAN-Etiketten über ein Lesegerät. Offensichtlich kann dieses Gerät den Strichcode als eine Ziffernfolge interpetieren, nämlich als *die* Ziffernfolge, die unterhalb des Strichcodes angegeben ist. Diese Ziffernfolge bestimmt das Produkt eindeutig und damit auch den Preis. Das Lesegerät

ist zweifellos eine technisches Wunderwerk: es ist offensichtlich unseren Augen weit überlegen, indem es nämlich die Striche *sehr rasch* lesen kann. Der Kunde fragt sich vielleicht von Zeit zu Zeit, ob ihm denn immer das *richtige* Produkt berechnet werde und ob nicht eventuell doch an Stelle seiner Flasche Mineralwasser eine Flasche Champagner auf die Rechnung geschrieben worden sei. Wenn man das nachträglich auf dem Kassenzettel kontrolliert, so wird man feststellen, dass eigentlich *nie* ein Fehler geschieht. Offensichtlich kann das Gerät die Striche nicht nur *sehr schnell* lesen, sondern auch mit *traumhafter Sicherheit*. Müssten wir mit unseren Augen die Striche interpretieren bzw. die entsprechenden Ziffern lesen, so würden uns zweifellos weit mehr Fehler unterlaufen.

So "sagt" das Gerät denn auch – wie Sie wissen – mit einem vernehmlichen "Peep", wenn "es" der Auffassung ist, richtig gelesen zu haben. Ertönt kein "Peep", wiederholt die Person an der Kasse den Lesevorgang bekanntlich noch einmal, oder sogar mehrere Male. Woran merkt denn das Gerät, dass es nicht nur *erfolgreich*, sondern auch *richtig* gelesen hat? Hier ist tatsächlich eine ganze Reihe von Sicherungsmassnahmen eingebaut. Sie alle beruhen auf Mathematik. Ich will *eine* dieser Sicherungsmassnahmen herausgreifen, eine die auf der Gynmnasialstufe ohne weiteres zu erklären ist, aber auch eine, die ein grundlegendes, vielfach verwendetes Prinzip offenlegt.

Auf weitere Sicherungsmassnahmen und mathematische Details des EAN-Codes will ich nur am Rande kurz zu sprechen kommen, und die technische Seite der Geräte will ich hier ganz beiseite lassen.

Der EAN-Code

EAN steht als Abkürzung für **E**uropean **A**rticle **N**umbering System. Das System wurde 1977 auf der Grundlage eines kurz vorher in Amerika verwendeten Bezeichnungssystems in Europa eingeführt. Dabei hat man das amerikanische System erweitert, und zwar so, dass die beiden Systeme kompatibel sind.

Die Produktnummer, von der EAN ausgeht, besteht aus 12 Ziffern, $a_1, a_2, \cdots, a_{12}$. Diesen 12 Ziffern wird eine 13. Ziffer a_{13} angefügt:

$$a_1, a_2, \cdots, a_{12}, a_{13} \ .$$

Und zwar so, dass

$$a_1 + 3a_2 + a_3 + 3a_4 + \cdots + 3a_{12} + a_{13}$$

eine Zehnerzahl ist. Es ist also nicht jede Folge von 13 Ziffern eine EAN-Zahl, sondern nur dann, wenn die zusätzliche Bedingung erfüllt ist. Man nennt deshalb a_{13} auch etwa eine *Prüfziffer*. Sie ist das Sicherheitselement, von dem hier die Rede sein soll.

Das folgende Beispiel zeigt, wie diese Bedingung zu erfüllen ist.

9	7	8	0	3	8	7	9	4	8	2	3	?
1	3	1	3	1	3	1	3	1	3	1	3	1
9	21	8	0	3	24	7	27	4	24	2	9	?
9	1	8	0	3	4	7	7	4	4	2	9	?
9	1	8	0	3	4	7	7	4	4	2	9	2

Die erste Zeile besteht aus den 12 ersten Ziffern des Codes, die zweite gibt die Gewichte an, mit denen die einzelnen Ziffern zu multiplizieren sind, in der dritten stehen die entsprechenden Produkte. Da für die Rechnung Vielfache von 10 nicht berücksichtigt werden müssen, kann man sich in der vierten Zeile mit den *Resten modulo 10* begnügen. Die Prüfziffer ergänzt die Summe zur nächsten Zehnerzahl.

Wenn das Lesegerät die dreizehn Ziffern der EAN Etikette – wie es meint – erfolgreich gelesen hat, so untersucht es, ob die obige Bedingung erfüllt ist. Ist sie erfüllt, so betrachtet das Lesegerät die gelesene 13-stellige Zahl als die richtige EAN Nummer, sagt "peep" und gibt sie an den Kassencomputer weiter. Ist die Bedingung aber nicht erfüllt, so ist die gelesene 13-stellige Zahl *keine* EAN Nummer und es muss beim Lesevorgang ein Fehler geschehen sein. Möglicherweise wurde eine oder sogar mehrere Ziffern falsch gelesen, d.h. die entsprechende Strichkombination wurde falsch interpretiert. Der Lesefehler wurde *entdeckt!* In diesem Fall bleibt das *Peep* des Lesegerätes aus, und der Lesevorgang muss wiederholt werden.

Die Frage stellt sich: Was nützt das Hinzufügen der Prüfziffer? Man wird ja nicht einfach ohne Grund eine weitere, eigentlich "nicht notwendige" Ziffer hinzufügen.

Behauptung: Der EAN Code kann einfache Fehler (falsche Ziffern) erkennen.

Beweis: Für ungerade Indizes ist das klar. Deshalb betrachte ich hier nur den Fall von geraden Indizes.

$$a_1 + 3a_2 + a_3 + \cdots + 3a_i + \cdots + a_{13} = x \cdot 10 \ ,$$

$$a_1 + 3a_2 + a_3 + \cdots + 3b_i + \cdots + a_{13} = y \cdot 10 \ ,$$

wo x und y ganze Zahlen bezeichnen. Die Differenz ist

$$3a_i - 3b_i = z \cdot 10 \ ,$$

wo z wiederum eine ganze Zahl ist. Daraus folgt

$$3(a_i - b_i) = z \cdot 10 \ .$$

Wegen $0 \leq |a_i - b_i| \leq 9$ ist dies nur möglich, wenn $z = 0$, also $a_i = b_i$ ist.

Behauptung: EAN entdeckt das Vertauschen von aufeinanderfolgenden Ziffern, es sei denn, ihre Differenz ist 5.

Beim elektronischen Lesegerät wird dieser Fehler wohl kaum auftreten; aber es sind Situationen denkbar, in denen der EAN-Code eingetippt werden muss. Dann sind Sicherheitsmassnahmen gegen das Vertauschen von (aufeinanderfolgenden) Ziffern sinnvoll.

Beweis:

$$a_1 + 3a_2 + \cdots + 3a_i + a_{i+1} + \cdots + a_{13} = x \cdot 10 \ ,$$

$$a_1 + 3a_2 + \cdots + 3a_{i+1} + a_i + \cdots + a_{13} = y \cdot 10 \ ,$$

wo x und y ganze Zahlen bezeichnen. Zu zeigen ist: $a_i = a_{i+1}$ oder $|a_i - a_{i+1}| = 5$. Die Differenz der beiden obenstehenden Gleichungen ist:

$$3a_i + a_{i+1} - 3a_{i+1} - a_i = z \cdot 10 \ ,$$

wo z wiederum eine ganze Zahl ist. Daraus folgt:

$$a_i - a_{i+1} = z \cdot 5 \ .$$

Wegen $0 \leq |a_i - a_{i+1}| \leq 9$ ist dies nur möglich, wenn $a_i = a_{i+1}$ oder wenn $|a_i - a_{i+1}| = 5$.

Nebenbemerkung: Ihre Schüler können natürlich jetzt ausrechnen, welcher Anteil der Fehler entdeckt wird, die auf die Vertauschung von zwei aufeinanderfolgenden Ziffern beruhen.

Analoges wie für die Vertauschung aufeinanderfolgender Ziffern gilt offenbar für die Vertauschung einer Ziffer an einer geraden Stelle mit einer Ziffer an einer ungeraden Stelle.

Im Unterschied dazu kann EAN den Fehler offensichtlich *nicht* erkennen, wenn zwei Stellen mit nur geraden oder nur ungeraden Indizes vertauscht werden.

Man lernt aus dieser einfachen Untersuchung, dass das Hinzufügen der Prüfziffer es erlaubt, einige Lesefehler zu *entdecken*, dass aber andere unentdeckt bleiben. Das einzusehen ist ganz wichtig: Eine derartige Sicherheitsmassnahme kann einen *Teil* der Fehler eliminieren, aber nicht *alle*. Das ist *immer* so. Das System ist dann *gut*, wenn es die Häufigkeit der Fehler insgesamt signifikant senkt. Es ist umso effektiver, je grösser die Reduktion der Gesamtfehlerhäufigkeit ist.

Um letzteres beurteilen zu können, muss man über die Häufigkeit verschiedener Fehlerarten etwas Bescheid wissen. In einer auf der englischen Sprache beruhenden Untersuchung wurde die Fehlerhäufigkeit bei der Übermittlung von Ziffernfolgen (mündlich bzw. durch Eintippen) festgestellt:

Falsche Ziffern 79.1% der Fehler;
Transposition aufeinanderfolgenden Ziffern 10.2% der Fehler;
alle anderen Fehlertypen je unter 1%, darunter der häufigste Fehler
mit 0.8% Vertauschung von *abc* zu *bca*.

Bei der Kommunikation über die Sprachgrenzen hinweg, also zwischen deutsch und englisch oder zwischen deutsch und französisch dürfte der Fehlertypus der Transposition einen wesentlich höheren Anteil haben. Denken Sie etwa an "twentyfive" und "fünfundzwanzig".

Strichcodes werden heute nicht nur zur Produktbezeichnung verwendet, sondern sie werden – modifiziert – auch für viele andere Zwecke eingesetzt. Der Grund dafür ist die weite Verbreitung des ursprünglichen Systems. Dies hatte zur Folge, dass die Lesegeräte in sehr grosser Stückzahl und deshalb entsprechend billig hergestellt werden konnten. Beispiele, in denen Strichcodes verwendet werden, sind die Benutzerkarte der ETH-Bibliothek, die Supercard der Coop, die Cumulus-Card der Migros, die neue AHV-Nummer und viele andere.

Der ISBN-Code

Ein zweites, ähnliches und doch auch wieder etwas verschiedenes System und Sicherungskonzept wird bei den ISBN Nummern verwendet, die der Buchhandel vor Jahren eingeführt hat, zeitlich sogar bevor die EAN-Etiketten auftauchten, nämlich 1968/72. Die ISBN Nummern, welche den Bestellvorgang im Buchhandel erleichtern, werden dabei oft mündlich kommuniziert oder – heute – per Email. Es muss also sichergestellt werden, dass insbesondere bei üblichen Fehlern der mündlichen oder schriftlichen Zahlenübermittlung das System grosse Sicherheit bietet.

ISBN steht als Abkürzung für **I**nternational **S**tandard **B**ook **N**umber. Gegeben sind 9 Ziffern a_1 bis a_9, die das Buch eindeutig bestimmen. (Siehe Abb. 1; die Ziffern der ISBN-Nummer sind oberhalb des Strichcodes zu finden.) Die Ziffer a_{10} ist die *Prüfziffer*. Diese Prüfziffer wird so bestimmt, dass die folgende Bedingung erfüllt ist:

$$10a_1 + 9a_2 + 8a_3 + \cdots + a_{10} \equiv 0 \mod 11 \ .$$

Falls sich daraus $a_{10} = 10$ ergibt, so setzt man $a_{10} = X$. Humanistisch Gebildete erkennen den Grund für diese Wahl!

Ein Beispiel zeigt, wie die Prüfziffer berechnet werden kann.

0	3	8	7	9	4	8	2	3	?
10	9	8	7	6	5	4	3	2	1
0	27	64	49	54	20	32	6	6	?
0	5	9	5	10	9	10	6	6	?
0	5	9	5	10	9	10	6	6	6

Die erste Zeile besteht aus den 9 ersten Ziffern des Codes, die zweite gibt die Gewichte an, mit denen die einzelnen Ziffern zu mutiplizieren sind, in der dritten stehen die entsprechenden Produkte. Da für die Rechnung Vielfache von 11 nicht berücksichtigt werden müssen, kann man sich in der vierten Zeile mit den *Resten modulo 11* begnügen. Die Prüfziffer ergänzt die Summe zur nächsten Elferzahl.

Wie beim EAN zeigt man, dass ISBN einfache Fehler erkennen kann.

Beweis:

$$10a_1 + 9a_2 + \cdots + (11-i)a_i + \cdots + a_{10} = x \cdot 11 \ ,$$

$$10a_1 + 9a_2 + \cdots + (11-i)b_i + \cdots + a_{10} = y \cdot 11 \ ,$$

wo x und y ganze Zahlen sind. Durch Subtraktion erhält man $(a_i - b_i)(11-i) = z \cdot 11$, wo $0 \leq |a_i - b_i| \leq 10$, $1 \leq 11 - i \leq 10$ und z eine ganze Zahl ist.

Da 11 eine Primzahl ist, müsste im Falle $z \neq 0$ die Zahl 11 einen der beiden Faktoren links teilen; dies ist aber offensichtlich nicht möglich. Deshalb folgt $z = 0$ und somit $a_i = b_i$. Damit ist bewiesen, dass ISBN einfache Fehler erkennt.

Im Gegensatz zu EAN erkennt ISBN das Vertauschen von zwei Ziffern in jedem Fall.

Beweis:

$$10a_1 + 9a_2 + \cdots + (11-i)a_i + \cdots + (11-k)a_k + \cdots + a_{10} = x \cdot 11 \ ,$$

$$10a_1 + 9a_2 + \cdots + (11-i)a_k + \cdots + (11-k)a_i + \cdots + a_{10} = y \cdot 11 \ ,$$

wo x und y ganze Zahlen sind. Durch Subtraktion erhält man

$$(a_i - a_k)(k - i) = z \cdot 11 \ ,$$

wo z eine ganze Zahl ist. Daraus folgt für $i \neq k$

$$a_i - a_k = w \cdot 11 \ .$$

wo $0 \leq |a_i - a_k| \leq 10$, und somit $a_i = a_k$ ist.

Etwas mehr Mathematik verlangt der Nachweis der folgenden Eigenschaft. Siehe dazu auch die Bemerkung 2 weiter unten.

Sind 9 der 10 Ziffern bekannt, so kann man bei ISBN die zehnte immer berechnen.

Beweis: Es muss gelten

$$10a_1 + 9a_2 + \cdots + qx + \cdots + a_{10} \equiv 0 \mod 11 \ .$$

Also folgt, da die Division von Resten modulo der Primzahl 11 möglich ist,

$$\frac{1}{q}(10a_1 + 9a_2 + \cdots + (q+1)a_{11-q-1} + (q-1)a_{11-q+1} + \cdots + a_{10}) \equiv -x \mod 11 \ .$$

Somit lässt sich x, $0 \leq x \leq 10$ eindeutig bestimmen.

Bemerkungen: 1. Die zur letzten Behauptung analoge Behauptung für den EAN-Code ist ebenfalls richtig. Weshalb?

2. Noch zwei, drei Richtungen, die sich in diesem Zusammenhang im Gymnasialunterricht öffnen. Zum einen berührt man bei EAN und bei ISBN zaghaft das Rechnen mit Resten modulo 10 bzw. 11. Selbstverständlich lässt sich das ausbauen: wenn einmal der Nutzen einer Idee gezeigt ist, ist wohl das Interesse für Weiteres geweckt. Man kann zeigen, dass man Reste modulo einer vorgegebenen Zahl mit den "alten" Rechenregeln sowohl addieren wie auch multiplizieren kann: besonders attraktiv dürfte für den Unterricht die Rechnung modulo 2 sein. Dass man dabei manchmal "Nullteiler" erhält, aber eben nicht bei Resten modulo einer Primzahl, dürften Schüler und Schülerinnen selber herausfinden können. Und der Schluss, dass die Nullteilerfreiheit dazu führt, dass man modulo einer Primzahl sogar dividieren kann, – dass man also einen Körper (im algebraischen Sinn) vor sich hat, könnte für einige eine regelrechte Erleuchtung sein.

Anschliessen könnte sich an dieser Stelle im Unterricht eine Diskussion der Neunerprobe: Der Beweis, dass sich der Rest modulo 9 einer Zahl leicht via deren Quersumme berechnen lässt, ist einfach. Und vielleicht gelingt Ihren Schülern und Schülerinnen dann, was einem Schüler während der erwähnten Studienwoche gelang: Auf einen leisen Hinweis hin hat er im Anschluss an die Neunerprobe die Elferprobe und ihre Funktionsweise mit der alternierenden Quersumme entdeckt.

3. Ich habe vorhin davon gesprochen, dass Strichcodes im Laufe der Jahre Gebiete erobert haben, für die dieses System eigentlich gar nicht konzipiert worden war. Hier ist ein weiteres Beispiel: Man hat kürzlich entschieden, die (10-stellige) ISBN-Nummer durch eine (13-stellige) EAN-Nummer zu ersetzen und diese dann als Strichcode im Buch zu vermerken. Diese Ablösung scheint bereits für 2007 geplant zu sein.

CD's und DVD's

Schliesslich will ich in diesem Vortrag das Augenmerk auf ein weiteres technisches Gerät richten, das Sie alle kennen und das eine Menge unsichtbarer Mathematik enthält. Es geht um die Speicherung von Daten auf einer CD (**C**ompact **D**isc) oder auf einer DVD (**D**igital **V**ersatile **D**isc, manchmal auch als **D**igital **V**ideo **D**isc bezeichnet). Sie wissen, dass diese Daten alle digital gespeichert sind, nämlich als eine (sehr lange) Folge von Nullen und Einsen. Es ist in der Tat eine sehr lange Folge: Das Audiosignal wird auf beiden Stereokanälen 44'100 mal pro Sekunde abgetastet und jede dieser Messungen wird durch 2 Bytes, also durch 16 Bits dargestellt! Ihre Schüler können ausrechnen, wie lange die 01-Folge für eine einstündige Audio-Aufnahme ist. (Tatsächlich ist sie aus technischen und mathematischen Gründen noch wesentlich länger!) Diese abgespeicherte 01-Folge wird im CD-Player gelesen und wieder in Musik umgesetzt. Der Weg von der Musik zum 01-Datenstrom und wieder zurück zur Musik ist technisch und mathematisch *sehr* kompliziert (siehe Abb. 2). Er kann schon aus Zeitgründen nicht Gegenstand dieses Vortrages sein, dazu wäre ein ganzer Semesterkurs erforderlich.

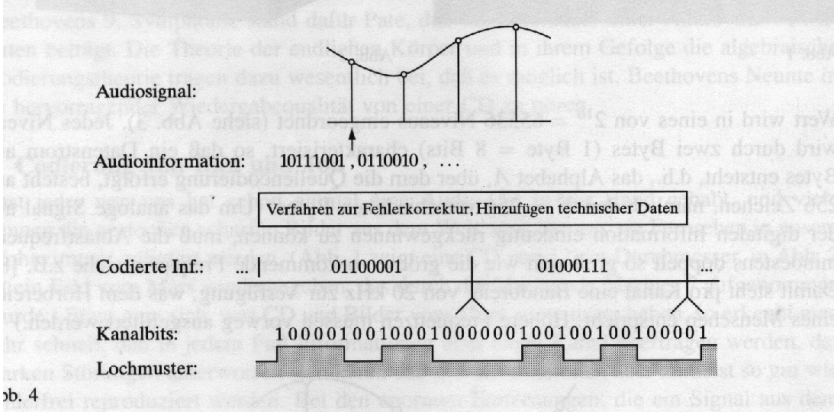

Abb. 2. Schematische Darstellung des Speicher- bzw. Abspielvorganges.

Ich kann hier nur das folgende Detail etwas näher betrachten: Es ist beim Abspielen einer CD absolut notwendig, dass die 01-Folge richtig und vollständig gelesen wird. Jeder Fehler, der hier gemacht wird, hat gravierende Auswirkungen auf den Ton, der nachher daraus erzeugt wird. Gleiches gilt, wenn ein Kratzer oder ein Schmutzpartikel das vollständige Lesen verhindert. Sie kennen solche Effekte wohl noch aus der Zeit der alten Langspielplatten, auf denen die Musik analog gespeichert war. In Anbetracht der Dichte der Information auf der CD sind nun aber solche lokalen Aufzeichnungs- und Ablesefehler gar nicht ganz zu vermeiden. Was also tun? Hier hat man ein Konzept gewählt, welches in der Lage ist, Lesefehler nicht nur

festzustellen – wie das bei der EAN-Etikette und bei der ISBN-Nummer der Fall ist – , sondern ein System, das Fehler selbsttätig *korrigieren* kann. Das tatsächlich verwendete System ist zwar viel zu kompliziert, um in kurzer Zeit besprochen zu werden, aber das *Prinzip* kann man durchaus verstehen. Und mit diesem Prinzip, das wiederum mathematischer Natur ist, will ich mich jetzt in diesem Vortrag noch etwas auseinandersetzen.

Binäre Codes, Hamming Code

Ich will mich dem Problem schrittweise nähern, und zwar in *kleinen* Schritten. Denken Sie daran, dass ich hier auch immer wieder Ihre Schüler und Schülerinnen im Auge habe!

Binäre Codes, also Codes, wo nur die Ziffern 0,1 vorkommen, spielen in der Elektrotechnik eine grosse Rolle. Die beiden Ziffern 1 und 0 erlauben es, zwischen den Zuständen *es fliesst ein Strom* und *es fliesst kein Strom* zu unterscheiden bzw. zwischen den Zuständen *positiv* und *negativ*. Viele Gebiete der Elektrotechnik machen *einzig* von dieser binären Unterscheidung Gebrauch und stellen nicht auf die Stärke des Stroms bzw. der Grösse der Spannung ab. Dies gilt insbesondere für die moderne Kommunikationstechnik, wo man zu diesem Zweck die Nachrichten in 01-Folgen umwandelt und diese übermittelt; so wird bei der CD zum Beispiel die Tonfolge des Musikstücks in eine 01-Folge umgewandelt und erst diese abgespeichert. Die Intensität des Signals spielt dabei nur mehr eine geringe Rolle: das Signal darf prinzipiell beliebig schwach sein, ohne dass der korrekte Empfang der Nachricht verunmöglicht wird. Bei der analogen Kommunikation hingegen hängt die Qualität wesentlich von der Stärke des Signals ab. Diese vorteilhafte Eigenschaft der digitalen Kommunikation ist einer der der Gründe, – nicht der einzige! – weshalb man diese neuerdings ganz allgemein der analogen vorzieht.

Bemerkung: Die Zahlen 0,1 können mathematisch als Elemente von $\mathbb{F}_2$ aufgefasst werden, also als Reste modulo 2. Dies hat den Vorteil, dass man damit leicht rechnen kann.

Sehr oft wird – zum Beispiel intern im Computer – ein sogenannter Paritätscheck verwendet. Dieser besteht darin, dass man einem 01-Wort der Länge k

$$a_1, a_2, \ldots, a_k$$

ein *Prüfbit* a_{k+1} hinzufügt, so dass das Wort

$$a_1, a_2, \ldots, a_k, a_{k+1}$$

immer eine *gerade* Anzahl von Einsen enthält (gerade Parität). (Selbstverständlich gibt es daneben auch einen Code mit ungerader Parität.)

Jeder soche Paritäts-Check kann in jedem Wort einfache Fehler entdecken. Der Empfänger weiss aber nicht, *wo* der Fehler steckt. Das ist ähnlich wie beim EAN-Code oder beim ISBN-Code. – Übrigens: Wenn man im binären Code einen Fehler nicht nur entdecken, sondern zusätzlich auch lokalisieren kann, so kann man ihn auch *korrigieren*. Es kommen ja nur die Möglichkeiten 0 oder 1 vor. Zur Korrektur muss man also an der Fehlerstelle eine 0 in eine 1 und eine 1 in eine 0 abändern.

Bei der CD werden derartige raffinierte Codes eingesetzt: Solche, die es fertigbringen, den Fehler auch noch zu *lokalisieren*. Im Prinzip ist das eigentlich einfach: Man macht es, wie es der Lehrer schon immer gemacht hat: Man sagt dasselbe mehrmals. Will man also 01 vermitteln, sagt man 0011.

Allerdings genügt eine zweifache Repetition nicht! Wenn ein Bit falsch ankommt, so kann man zwar feststellen, dass ein Fehler geschehen ist, man kann ihn aber nicht korrigieren, weil man nicht weiss, welches der beiden fraglichen Bits falsch und welches richtig ist.

Wenn man jedes Bit dreimal setzt, so ist die Situation besser: Jede Ziffer wird statt einmal *dreimal* hintereinander geschrieben; so wird die Nachricht 010 als 000111000 codiert. Bei einer Störung, z.B. zu 000101000, wird der Empfänger die mittlere Ziffer aus Wahrscheinlichkeitsgründen trotz des Fehlers als 1 interpretieren. Man sagt, der dreifache Repititionscode könne *einfache Fehler* korrigieren. Dafür zahlt man mit diesem Code allerdings einen hohen Preis, indem man die Nachricht dreimal länger gemacht hat.

Wiederum begegnet man hier der Tatsache, dass ein solches System *gewisse Fehler* erkennen bzw. korrigieren kann, dass es aber Fälle gibt, in denen es versagt. Sind etwa zufälligerweise die zwei äusseren Bits der mittleren Gruppe verfälscht worden, so liefert die Korrektur das falsche Resultat. Man geht also bei der Fehlerkorrektur davon aus, dass *zwei gleichzeitig und nahe beieinander auftretende* Fehler weit weniger wahrscheinlich sind als ein einzelner Fehler.

Abb. 3. Richard Hamming, 1915 – 1998.

Der Hammingcode

Hier ist eine andere, eine bessere(!) Möglichkeit! Sie stammt von Richard Hamming (1915–1998) (siehe Abb. 3). Man zerlegt die binäre Nachricht in Wörter der Länge 4 und fügt jedem Wort nicht nur ein Prüfbit sondern gleich *drei* Prüfbits hinzu. Die Vorschrift ist wie folgt:

Nachrichten	Codewörter
1000 →	1110000
0100 →	1001100
0010 →	0101010
0001 →	1101001

Die übrigen 4-stelligen 01 Nachrichtenwörter ergeben sich durch die Addition (modulo 2) der 4 Grundnachrichten. Auf diese Weise lassen sich 15 verschiedene (nicht-triviale) Nachrichtenwörter codieren.

Nachrichten		Codewörter
1111	→	1111111
1110	→	0010110
1101	→	1010101
1100	→	0111100
1011	→	0110011
1010	→	1011010
1001	→	0011001
1000	→	1110000
0111	→	0001111
0110	→	1100110
0101	→	0100101
0100	→	1001100
0011	→	1000011
0010	→	0101010
0001	→	1101001

Die ursprünglichen Nachrichtenwörter sind an den Stellen 3,5,6,7 erkennbar.

Wichtig ist hier bei diesem Code, dass sich zwei verschiedene Codewörter immer an *mindestens drei Stellen* unterscheiden. Die Anzahl Stellen, in denen sich zwei Wörter unterscheiden, nennt man den *Hamming-Abstand*. Tritt bei der Übermittlung eines Codewortes ein Fehler auf, so nimmt der Empfänger an, dass eigentlich dasjenige Wort "gemeint" ist, das dem "empfangenen Wort" (im Sinne des Hamming-Abstandes) am nächsten liegt.

Beispiel: Wird das Wort 0001001 empfangen, so gibt es nur eines unter den Codewörtern, das sich von diesem nur an einer Stelle unterscheidet, nämlich 0011001. Es ist das einzige Wort des Codes, das vom empfangenen Wort den Hamming-Abstand 1 besitzt. Die Nachricht, die gesendet werden sollte, hiess also 1001.

Man stellt fest: Der Hamming-Code ersetzt jedes vierstellige Nachrichtenwort durch ein siebenstelliges, dies bedeutet nicht einmal eine *Verdoppelung* der Stellenanzahl. Trotzdem erlaubt dieser Code, einfache Fehler zu korrigieren. Bei der ersten Idee mit dem dreifachen Repetitionscode hätte man für diese selbe Fähigkeit eine *Ver-*

dreifachung der Stellenanzahl in Kauf nehmen müssen.

In Wirklichkeit werden die Verfahren der Codierung und der Decodierung bzw. der Korrektur natürlich alle auf mathematischer Grundlage durchgeführt und nicht einfach durch Probieren, wie ich das hier vorgeführt habe. Das wäre viel zu ineffizient und würde zu lange dauern. Die mathematischen Verfahren, die bei der Codierung und Decodierung zum Zuge kommen, verlangen viel Mathematik; ich muss mich hier in der kurzen Zeit auch beim einfachen Hamming-Code auf einige Bemerkungen beschränken. Die Verfahren basieren selbstverständlich auf der mathematischen Struktur, die dem Hamming-Code zugrunde liegt und zu der ich unten noch einige Worte anfüge. Auf Grund dieser Struktur kann man z.B. auch *beweisen*, dass der Hamming-Abstand zweier Wörter jeweils mindestens drei ist.

Man kann den Vorgang des Codierens durch eine Matrizenmultiplikation beschreiben, nämlich als Multiplikation des Nachrichtenwortes mit der sogenannten erzeugenden Matrix G. In der Tat wurde der Hamming-Code oben eigentlich mit Hilfe einer linearen Abbildung definiert. Zu jedem Vektor der Standardbasis eines vierdimensionalen Vektorraumes (über $\mathbb{F}_2$) wurde sein Bild in einem siebendimensionalen Vektorraum (über $\mathbb{F}_2$) festgelegt; die durch diese Festlegung definierte lineare Abbildung g beschreibt den Hamming-Code. Die zugehörige Matrix bezüglich der Standardbasen ist G.

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

Auf der Empfängerseite wird man testen, ob das empfangene Wort w ein Codewort ist. Mathematisch muss man also nachprüfen, ob w im Bild der zu G gehörige Abbildung g liegt. Am einfachsten geschieht dies dadurch, dass man eine Abbildung h von unserem siebendimensionalen Vektorraum in einen dreidimensionalen Vektorraum betrachtet, deren Kern gerade aus den Codewörtern besteht, d.h. aus dem Bild der Abbildung g. Eine derartige Abbildung h hat Hamming durch die Matrix H beschrieben – wie sich unten herausstellen wird, ist Hammings Wahl äusserst raffiniert:

$$H = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Man verifiziert ohne Schwierigkeiten, dass der Kern der Abbildung h gerade das Bild der Abbildung g ist.[2] Diese Matrix H, die Hamming *Checkmatrix* genannt hat, kann man auch zur Fehlerkorrektur heranziehen.

Es werde das Wort w empfangen. Es soll nur eine einzige Fehlerstelle enthalten. Das Wort w unterscheidet sich also an genau einer Stelle von einem "richtigen" Codewort. Wenn man herausfinden kann, an welcher Stelle des Wortes sich der Fehler befindet, so kann man ihn sofort korrigieren: Da nur 0 oder 1 in Betracht kommen, muss an der Fehlerstelle eine allfällige 0 in eine 1 und eine allfällige 1 in eine 0 abändert werden! Wie findet man die Fehlerstelle?

Da sich das Wort w nur an einer Stelle von einem Codewort unterscheidet, lässt es sich in der Form $c+e$ schreiben, wo c ein Codewort und e ein sogenanntes Fehlerwort ist: es ist das Wort, das nur an der Fehlerstelle eine Eins hat und sonst überall Nullen. (Man beachte, dass man modulo 2 rechnet!) Laut Definition der Matrix H ergibt jedes "richtige" Codewort c bei der Rechnung $H \cdot c$ den Nullvektor. Es ergibt sich dann:

$$H \cdot w = H \cdot c + H \cdot e = H \cdot e.$$

Aber $H \cdot e$ ist nichts anderes, als diejenige Spalte von H, die an der Stelle steht, in der in e die Eins vorkommt, also an der Fehlerstelle von w.

Das System ist jetzt (dank Richard Hamming!) so geschickt aufgebaut, dass die Spalten von H, aufgefasst als Dualzahl, gerade die Nummer der entsprechenden Spalte ergeben. Damit ist die Fehlerstelle gefunden und der Fehler kann ohne weiteres korrigiert werden.

Am obigen Beispiel lässt sich der Vorgang illustrieren. Es werde das Wort $w = 0001001$ empfangen. Die Multiplikation mit H liefert

$$H \cdot w = 011\ .$$

[2] Die Matrizenmultiplikationen, die hier herangezogen wurde, lässt sich natürlich umgehen. Dies ist für die Codierung, also für die Multiplikation mit der Matrix G oben bereits angedeutet worden. Die Matrizenmultiplikation mit H besteht darin, dass die drei Skalarprodukte mit den Zeilen der Matrix H gebildet werden. Diese Sichtweise dürfte den Schülern und Schülerinnen näher liegen. – Anzumerken bleibt noch, dass Hamming bei der Konstruktion seines Codes von der Matrix H ausgegangen ist. Die ursprüngliche Konstruktion des Codes verlief also gerade in der umgekehrten Reihenfolge zu der hier gegebenen Beschreibung.

Damit ist festgestellt, dass das empfangene Wort *kein* Codewort ist und dass (unter der Annahme, dass ein *einziger* Fehler geschehen ist) der Fehler an der dritten Stelle zu suchen ist. Das korrigierte Wort lautet also $c = 0011001$.

Seit der Entdeckung durch Richard Hamming hat man natürlich längere und auch raffiniertere fehlerkorrigierende Codes konstruieren können. Was die CD betrifft, so kann man das Folgende erwähnen:

Bei der CD werden zwei verschiedene derartige Codes hintereinander verwendet (und zwar über dem Alphabet, dessen Buchstaben Elemente des endlichen Körpers GF(256) sind):

Der eine Code fügt einem Nachrichtenwort der Länge 24 vier Prüfstellen hinzu; er ist so konstruiert, dass in jedem Wort zweifache Fehler korrigiert werden können. Der minimale Hamming-Abstand ist 5! Der zweite Code fügt einem Nachrichtenwort der Länge 28 noch einmal vier Prüfstellen hinzu; auch dieser Code kann ebenfalls zweifache Fehler korrigieren. Der minimale Hamming-Abstand ist auch hier 5!

Bei der DVD, die ungefähr 10 Jahre nach der CD eingeführt wurde, wurde von den inzwischen erreichten technischen Fortschritten Gebrauch gemacht. So konnte man dank neuer Verfahren auf der DVD eine viel grössere Informationsdichte erreichen; man vergleiche dazu die Abbildung 4, in der links die Spuren einer CD und rechts diejenigen einer DVD bei gleicher Vergrösserung zu sehen sind. Ferner konnte man

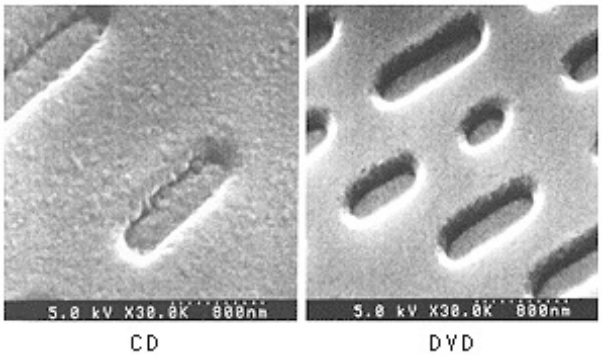

Abb. 4. Vergleich der Spuren bei CD und DVD

im Gerät nun kostengünstig grössere Rechenleistungen einbauen; sie erlaubten es, noch leistungsfähigere fehlerkorrigierende Codes einzusetzen. Insgesamt konnte mit all diesen Verbesserungen bei gleichen Abmessungen der DVD wie bei der CD die Kapazität von rund 0.7 GB auf 4.7 GB erhöht werden.

Wie bei der CD werden bei der DVD zwei fehlerkorrigierende Codes kombiniert verwendet. Der eine fügt einem Nachrichtenwort der Länge 172 zehn Prüfstellen

hinzu, der zweite einem Wort der Länge 192 sechzehn Prüfstellen. Der erste Code kann 5 der zweite 8 Fehler korrigieren.

Das Dekodieren und vor allem die Fehlerkorrektur verlangen bei derart langen Codes effiziente und deshalb komplizierte mathematische Verfahren und viel Rechenleistung. Ein Probieren, wie ich das zu Demonstrationszwecken beim Hamming-Code verwendet habe, kann hier nicht mehr in Betracht kommen. Es ist auch klar, dass mit der Länge der verwendeten Codes die Verfahren des Dekodierens und der Fehlerkorrektur rasch aufwändiger werden. Ein Abspielgerät für CD's oder DVD's ist also immer auch ein ziemlich leistungsfähiger Computer.

Ich bin hier auf die technischen Einzelheiten in allen diesen Beispielen nicht eingegangen: wie wird aufgezeichnet, wie wird abgelesen, wie wird die Geschwindigkeit gesteuert, wie wird die Musik digitalisiert, wie entstehen umgekehrt aus den digitalen Daten wieder Töne, etc. In jedem dieser einzelnen Schritte spielt wiederum die Mathematik eine zentrale Rolle. Es ist in der Tat so: Ein CD-Player enthält im Grunde genommen die Mathematik mehrerer dicker Bücher.

Ich komme ans Ende. Ich habe hier einige ausgewählte Beispiele von fehlererkennenden bzw. fehlerkorrigierenden Codes vorgestellt und über die Rolle gesprochen, die solche Codes bei der CD und DVD spielen; ich hätte statt CD und DVD auch MP3 nehmen können. Tatsächlich kommen derartige Codes heute überall vor: Werden irgendwo im Computer Daten verschoben oder abgespeichert, so geschieht das in aller Regel unter Vermittlung eines fehlererkennenden oder fehlerkorrigierenden Codes. Werden irgendwo numerische Bezeichnungen verwendet, so wird mindestens eine Prüfziffer eingebaut: solches geschieht etwa bei der IBAN-Nummer und bei der Nummerierung von Banknoten und Reisechecks usw. In diesem Umfeld bilden die Prüfziffern natürlich auch ein Merkmal, das Fälschungen erschwert. Die Übermittlung beim Handy geschieht – wie Sie wissen – ebenfalls digital – es werden 01 Folgen übermittelt – , und es wird am Schluss meines Vortrages niemanden mehr in Erstaunen setzen, zu vernehmen, dass auch in *diesem* Bereich fehlerkorrigierende Codes verwendet werden. Man benützt also Mathematik, und zwar schwierige anspruchsvolle Mathematik in fast allen täglichen Beschäftigungen! Mathematik ist – in der Tat – überall!

Anhang A. Bemerkungen zu einigen technischen Details des Strichcodes.

Es seien hier noch zwei, drei Dinge angefügt, welche die Darstellung der einzelnen Ziffern im Strichcode betreffen. Die gegebene Beschreibung ist dabei mit Absicht unvollständig: für Schüler und Schülerinnen dürfte es eine interessante Aufgabe sein, die hier fehlenden Informationen im Internet beizubringen.

Abb. 5. EAN-Etikette

Der Strichcode (siehe Abb. 5) zerfällt schon rein optisch in einen linken und einen rechten Teil. Ganz links, in der Mitte und ganz rechts sind je zwei schmale, alleinstehende schwarze Striche zu sehen, die gewöhnlich etwas länger sind als die übrigen Striche. Die erste Ziffer ganz links spielt eine Sonderrolle – ich nenne sie deshalb im Folgenden die *Sonderziffer* –, es ist die Ziffer, die von den Europäern eingeführt worden ist. In Amerika steht an dieser Stelle immer die Ziffer 0, die dann gewöhnlich gar nicht gedruckt wird. Diese Sonderziffer wird auf andere Art in den Strichcode umgesetzt als die übrigen zwölf. Jede dieser zwölf Ziffern wird durch ein Muster von sieben schwarzen bzw. weissen Strichen gleicher Breite dargestellt, die ohne Zwischenraum aufgedruckt werden. Auf der rechten Seite des Strichcodes wird jede Ziffer gemäss dem folgenden Schema (siehe Abb. 6) dargestellt, wobei 0 einen weissen und 1 einen schwarzen Strich bezeichnet.

Liest man von rechts, so beginnt die Strichcodierung jeder Ziffer der rechten Gruppe mit einem weissen Strich und endet mit einem schwarzen Strich. Die Ziffern selbst werden somit eigentlich (mathematisch!) nur durch *fünf* weisse bzw. schwarze Striche dargestellt. Die Codierung auf der rechten Seite ist so gewählt, dass in der Darstellung jeder Ziffer eine *gerade* Anzahl schwarzer Striche auftritt (gerade Parität). Man kann im abgebildeten Strichcode nun ohne weiteres auf der rechten Seite einzelne Ziffern identifizieren.

Right-Hand Characters
Even Parity (2 or 4 dark modules)

Module Location:	1	2	3	4	5	6	7
	Binary Pattern (0 or 1 Encodation)						
Right-Hand Character of Code:	↓	↓	↓	↓	↓	↓	↓
0 →	1	1	1	0	0	1	0
1 →	1	1	0	0	1	1	0
2 →	1	1	0	1	1	0	0
3 →	1	0	0	0	0	1	0
4 →	1	0	1	1	1	0	0
5 →	1	0	0	1	1	1	0
6 →	1	0	1	0	0	0	0
7 →	1	0	0	0	1	0	0
8 →	1	0	0	1	0	0	0
9 →	1	1	1	0	1	0	0

Abb. 6. Strichcodierung rechts.

Noch ein Wort zu der Gruppe von Ziffern auf der linken Seite. Liest man von links, so beginnt hier die Strichcodierung jeder Ziffer mit einem weissen Strich und endet mit einem schwarzen. Die Darstellung der einzelnen Ziffer durch die restlichen fünf weissen und schwarzen Striche ist aber – anders als dies auf der rechten Seite der Fall ist – i.a. abhängig von der Sonderziffer und von der Stelle, an der die Ziffer steht. Unabhängig von der Sonderziffer ist nur die Codierung der ersten Ziffer der linken Gruppe. Deren Strichcodierung ist diejenige, die sich durch Vertauschen von weiss und schwarz in der Codierung auf der rechten Seite ergibt. Insbesondere ist die Anzahl schwarzer Striche immer *ungerade* (ungerade Parität).

Aus dieser Tatsache ergibt sich, dass die äussersten, durch Striche codierten Ziffern, die linke bzw. rechte Seite des Strichcodes charakterisieren: Die Codierung der ersten Ziffer links enthält eine ungerade Anzahl schwarzer Striche, die Codierung der letzten Ziffer rechts enthält eine gerade Anzahl schwarzer Striche. Dies hat den erwünschten Effekt, dass das Lesegerät die linke und die rechte Seite erkennen kann: die EAN Etikette darf in einer beliebigen Richtung eingelesen werden.

Es ist im übrigen gerade die gerade bzw. ungerade Parität, die für die Codierung der Sonderziffer verwendet wird: Zu jeder Sonderziffer gehört ein (fünfstelliges) Paritätsmuster, das die Strichcodierungen der Ziffern der linken Gruppe festlegt.[3]

Anhang B. Richard Wesley Hamming.

Richard Hamming wurde 1915 in Chicago geboren. Er studierte an der *University of Chicago*, der *University of Nebraska* und an der *University of Illinois at Urbana-Champaign*, wo er im Jahr 1942 doktorierte. Anschliessend wurde er Professor an der *University of Louisville*. Von 1945 bis 1946 arbeitete er im Rahmen des Manhattan Projects, das die Entwicklung der Atombombe zum Ziel hatte; er entwickelte dort Algorithmen und Programme zur numerischen Lösung der auftretenden komplizierten Differentialgleichungen mit Hilfe des damals erstmals zur Verfügung stehenden digitalen Computers.

Von 1946 bis 1976 arbeitete Hamming bei den *Bell Telephone Laboratories*, der Forschungsabteilung dieser grossen amerikanischen Telefon-Gesellschaft. In diese Zeit fallen seine wichtigen Beiträge zur Theorie der digitalen Kommunikation, zur Codierungstheorie und zum weiten Feld der Computer Science.

Im Jahre 1976 wechselte Hamming sein Betätigungsfeld und wurde Professor an der *Naval Postgraduate School* in *Monterey*, Kalifornien.

Er starb kurz nach seiner Emeritierung im Jahre 1998.

Hamming hat viele bedeutende wissenschaftliche Arbeiten und Bücher veröffentlicht; in der einen oder anderen Weise behandeln sie alle das Thema Mathematik, Kommunikation und Computer: numerische Methoden, Programmierung, Computer-Algorithmen, mathematische Methoden der Informations- und Kommunikationstheorie, etc. Eine faszinierende und äusserst anregende Lektüre (nicht nur für Studierende sondern auch für Lehrer und Lehrerinnen) ist sein für ein allgemeineres Publikum geschriebenes Buch *The Art of Doing Science and Engineering: Learning to Learn*, Gordon and Breach, 1997. Er beschreibt dort u.a. ziemlich detailliert, wie er aus Anlass eines für ihn ärgerlichen Problems in seinem Laboratorium seinen fehlerkorrigierenden Hamming-Code entdeckt hat. Die aus diesem Werk stammenden Zitate *Machines should work, people should think* und *The purpose of computing is insight, not numbers* sind wohl auch im Unterricht beherzigenswert.

Anhang C. Einige technische Daten zur CD.

Die **Compact Disk** CD wurde 1982 in Europa und 1983 in den USA eingeführt.

[3]Die hier fehlende Information lässt sich unschwer im Internet auffinden, z.B. auf der Adresse http://www.export911.com/e911/coding/eanParity.htm

DVD, Minidisks sind Abkömmlinge davon, die sich technisch nicht prinzipiell von den CD unterscheiden; die verwendeten Ideen und Techniken sind die gleichen. Das technische Prinzip der CD wurde von der Firma Philips entwickelt und weltweit als Standard angenommen. Wesentlich ist dabei die Verwendung eines fehlerkorrigierenden Codes, denn die Dichte der Datenspeicherung verlangt nach der Möglichkeit, Lesefehler und andere Störungen selbsttätig zu *korrigieren* (Verunreinigungen, Fingerabdrücke, Kratzer, etc.)

Die Technik in ihrer Gesamtheit ist sehr kompliziert und vereinigt viele verschiedenartige Aspekte. Überblichsmässig stellt sich der Aufzeichnungs- bzw. Abspielvorgang wie folgt dar.

Das Audiosignal wird 44'100 Mal/sec (pro Audiokanal) abgetastet und der Wert wird in eines der $2^{16} = 65'536$ Niveaus eingeteilt. Jedes Niveau wird durch 2 Bytes (1 Byte = 8 Bits) charakterisiert. Das Alphabet der *Quellencodierung* besteht aus den $2^8 = 256$ verschiedenen Bytes.

Auf diesen Datenstrom werden die *Codierungsverfahren* angewendet, von denen im Vortrag kurz die Rede war.

Die Codierungsverfahren auf dem Datenstrom der Quellencodierung lassen sich überblicksmässig so darstellen: Als Alphabet betrachtet man die Elemente des endlichen Körper GF(256). Die verwendeten Codes machen aus Nachrichtenwörtern der Länge k Codewörter der Länge n. Man spricht in solchen Fällen von einem (n, k)-Code, und man sagt, ein derartiger Code weise $n - k$ Prüfstellen auf.

Die einzelnen Schritte sind die folgenden:

1. Von den beiden Audiokanälen werden abwechslungsweise je zwei Bytes genommen. Daraus werden sogenannte Frames der Bytelänge 24 gebildet; dies ist die Länge der Nachrichtenwörter über dem Alphabet GF(256).

2. Anwendung eines (28,24)-Codes C_1 über GF(256). Es werden also jedem Nachrichtenwort 4 (Prüf-)Bytes hinzugefügt. Der Code kann 2-Byte-Fehler korrigieren und 4-Byte-Fehler erkennen. Auf Bit-Ebene sind somit zwischen 9 und 16 Bits korrigierbar. Sowohl der Code C_1 wie auch der Code C_2 (siehe unter Ziffer 4) sind sogenannte *verkürzte Reed-Solomon-Codes.*

3. Interleaving: Von je 28 aufeinanderfolgenden Codewörtern wird jeweils die erste Stelle, dann der zweite, etc. genommen. Dieses Verfahren verbessert die Korrekturmöglichkeit des Codes gegenüber sogenannten Bursts. Unter Bursts versteht man Fehler, die eine grössere Anzahl von unmittelbar aufeinanderfolgenden Zeichen betreffen. Das Inteleaving bewirkt, dass ein darartiger Burst-Fehler zwar mehrere Wörter betrifft, aber jedes nur an wenigen Stellen.

4. Anwendung eines (32,28)-Codes C_2 über GF(256). Auch dieser Code kann 2-Byte-Fehler korrigieren und 4-Byte-Fehler erkennen.

5. Ergänzung des Datenstromes durch Hinzufügen von einem Byte zu jedem Wort der Länge 32. Damit entstehen Wörter der Länge 33.

Unmittelbar vor der Aufzeichnung auf die CD steht die *Kanalcodierung*, auch *EF-Modulation* genannt. Dabei wird jedes Byte auf 14 Bits plus 3 Verbindungsbits, also auf 17 Bits erweitert. Man vermeidet durch diese Erweiterung u.a., dass nie zwei Einsen unmittelbar nacheinander vorkommen, denn dieses Muster ist bei der gewählten Aufzeichnungsart (siehe weiter unten) gar nicht möglich. Ausserdem erreicht man dadurch eine Anzahl von Erleichterungen technischer Art. Ein Wort, das vor der EF-Modulation die Länge von 33 Bytes besitzt, wird also nun durch $33 \cdot 17$ Bits dargestellt. Schliesslich werden 27 Synchronisationsbits (Uhr!) hinzugefügt. Somit hat ein Frame von anfänglich 24 Bytes (=192 Bits) bei der Aufzeichnung eine binäre Länge von 588 Bits.

Beim Abspielen werden die aufgezeichneten Zeichen mit 4.3 Megabits/sec abgetastet. Es werden als erstes die Synchronisationsdaten herausgelesen, was die Steuerung der Umlaufgeschwindigkeit möglich macht. Dann wird die EF-Modulation rückgängig gemacht. Die Abspielinformation (Track, Zeit, etc) wird dem Display zugänglich gemacht. Der restliche Datenstrom enthält die codierte Audioinformation; sie wird zur Weiterbehandlung in einen Buffer geleitet; die Verarbeitung geht zeitlich mit der Genauigkeit einer Quarzuhr vor sich. In diesem Buffer folgt die Decodierung des Codes C_2, die Umkehrung des Interleavings und die Decodierung des Codes C_1. Fehler werden bei jedem Schritt korrigiert. Sollte das nicht möglich sein, so wird – in gewissen Grenzen – auch interpoliert. Die resultierende digitale Information wird wieder in Ton umgesetzt.

Eine CD hat einen Durchmesser von 12 cm. Sie enthält eine spiralförmige Spur, die von innen nach aussen läuft. Die Schicht, welche die eingebrannte Information trägt, ist durch eine durchsichtige Schutzschicht abgedeckt. Die Spur besteht aus eingebrannten Vertiefungen (mindestens $9 \cdot 10^{-4}$ mm lang). Der Abstand zwischen zwei Spuren beträgt $1.6 \cdot 10^{-3}$ mm. Die Abtastung erfolgt durch einen Laserstrahl. Auf den Erhebungen wird der Strahl voll reflektiert, in den Vertiefungen (ca. 1/4 der Wellenlänge des Lichtes) dagegen kaum. Jeder Wechsel(!) der Reflexionsstärke wird als eine Eins interpretiert, sonst als (jeweils mehrere aufeinanderfolgende) Nullen. Man ersieht daraus, dass das Zeitmass im Gerät mit äusserster Genauigkeit verfügbar sein muss, sonst könnte die *Anzahl* der Nullen gar nicht festgestellt werden.

Anhang D. Quellen, Literaturangaben.

Die Information zur mathematischen Seite des EAN-Codes holt man sich am besten aus dem Internet:

http://www.barcodeisland.com/ean13.phtml

Die folgenden Adressen fassen das wesentliche zusammen:

http://www.export911.com/e911/coding/eanParity.htm
http://www.export911.com/e911/coding/eanChar.htm

Die Abb. 6 stammt von dieser Adresse.

Die Vorgaben zur neuen AHV-Nummer findet man auf der Adresse:

http://www.ahv.ch/Home-D/allgemeines/
nnahv/NNSSInformationenVersichertennummerd.pdf

Angaben zu Varianten und Erweiterungen des Strichcodes, die hier nicht behandelt wurden, findet man unter:

http://www.barcodeisland.com/symbolgy.phtml

Zur ISBN-Nummer gibt es detaillierte Angaben unter:

http://www.isbn-international.org/index.html

Das folgende Buch behandelt das allgemeine Thema Prüfziffern auf lesbarem Niveau ziemlich eingehend:

Joseph Kirtland: *Identification Numbers and Check Digit Schemes.* The Mathematical Association of America, 2001.

Daneben gibt es eine Anzahl von Artikeln zum Thema Prüfziffer, die in allgemeinen mathematischen Zeitschriften erschienen sind und die zum Teil auf weitere Beispiele eingehen, z.B.:

Joseph A. Gallian: *Assigning Driver's License Numbers.* Math. Magazine 64 (1991), 13-22.

Joseph A. Gallian, St. Winters: *Modular Arithmetic in the Marketplace.* Amer. Math. Monthly 95 (1988), 548-551.

Ralph-Hardo Schulz: *Prüfziffern und Teilbarkeit.* MU 5 (1990), 5-18.

Man vergleiche dazu auch die von Ralph-Hardo Schulz zusammengestellte Literaturliste:

http://page.mi.fu-berlin.de/∼schulz/checkdigit_literatur.pdf

Auf die Angabe von eigentlicher Fachliteratur zu fehlererkennende und fehlerkorrigierende

Codes wird hier verzichtet; entsprechende Titel – die Literatur füllt inzwischen ganze Bibliotheken – , lassen sich unschwer im Internet finden.

Die folgenden beiden Artikel behandeln das Thema der fehlererkennenden und fehlerkorrigierenden Codes in sehr lesbarer Weise, aber etwas detaillierter als das hier geschehen ist. Sie führen es auch noch etwas weiter, insbesondere in mathematischer Richtung.

François Sigrist: *Codes correcteurs d'erreurs.* Elem. Math. 48 (1993), 157-169.

Dietmar Doringer: *Algebraische Codierungstheorie und Compact Discs.* Elem. Math. 51 (1996), 89-101.

Die oben eingefügte Abb. 2 stammt aus dem Artikel von Dietmar Doringer.

Zu den technischen Details von DVD vergleiche man die ausführliche Dokumentation unter:

http://pioneer.jp/crdl/tech/index-e.html

Aus dieser Dokumentation stammt Abb. 4.

Prof. em. Urs Stammbach
Mathematik
ETH-Zürich
8092 Zürich

stammb@math.ethz.ch