

Die Mathematik der Compact Disc

Prof. Dr. Jack H. van Lint (†)

www.win.tue.nl/~jlint



Dieser Artikel ist eine gekürzte Version des Artikels gleichen Titels, welcher in dem Buch Alles Mathematik [1] erschien und welchen wir hier mit freundlicher Genehmigung des Vieweg Verlags abdrucken dürfen. Das Buch Alles Mathematik, welches eine Vielzahl weiterer interessanter populärwissenschaftlicher Artikel über mathematische Anwendungen enthält, erscheint 2008 in der dritten Auflage. Der Autor Jack van Lint ist leider am 28. September 2004 verstorben, s. www.win.tue.nl/~jlint.

Zusammenfassung

Jeder verwendet heute ganz selbstverständlich Compact Discs. Warum ist aber die Musikübertragung auf einer CD reiner als auf einer herkömmlichen Schallplatte? Die Antwort lautet, um einen populären Slogan abzuwandeln: There is mathematics inside! Genauer gesagt, ein Zweig der Diskreten Mathematik, nämlich die Theorie der Fehler korrigierenden Codes. In diesem Artikel soll über die Anwendung solcher Codes auf das Design des Compact-Disc-Audio-Systems berichtet werden, das von Philips Electronics und Sony entwickelt wurde.

Wörter und Codes

Wir werden das folgende leicht verständliche mathematische Konzept verwenden. Betrachten wir zwei n -Tupel $\mathbf{a} = (a_1, a_2, \dots, a_n)$ und $\mathbf{b} = (b_1, b_2, \dots, b_n)$, wobei die a_i und b_i aus einer Menge Q , genannt das *Alphabet*, stammen. Der *Hamming-Abstand* von \mathbf{a} und \mathbf{b} ist definiert durch

$$d(\mathbf{a}, \mathbf{b}) = \text{Anzahl der } i \text{ mit } a_i \neq b_i.$$

Wir nennen \mathbf{a} und \mathbf{b} *Wörter der Länge* n über dem Alphabet Q .

Die Analogie dieses Begriffes „Wörter“ zur gewöhnlichen Sprache ist absichtlich. Nehmen wir an, wir lesen ein Wort (sagen wir, in einem Buch auf Deutsch) und bemerken, dass das Wort zwei Druckfehler enthält. Dann heißt das in unserer Terminologie, dass das gedruckte Wort Hamming-Abstand 2 zum korrekten Wort hat. Der Grund, warum wir die 2 Druckfehler erkennen, liegt darin, dass in der deutschen Sprache nur ein einziges Wort mit so einem kleinen Abstand zum gedruckten (fehlerhaften) Wort existiert. Das ist auch schon das grundlegende Prinzip der Fehler korrigierenden Codes: Entwurf eine Sprache (genannt *Code*) von Wörtern einer festen Länge über einem Alphabet Q , so dass je zwei Codewörter mindestens Abstand $2e + 1$ haben. Diese Größe $2e + 1$ heißt dann der Minimalabstand des Codes. Offensichtlich ist ein Wort, das höchstens e Fehler

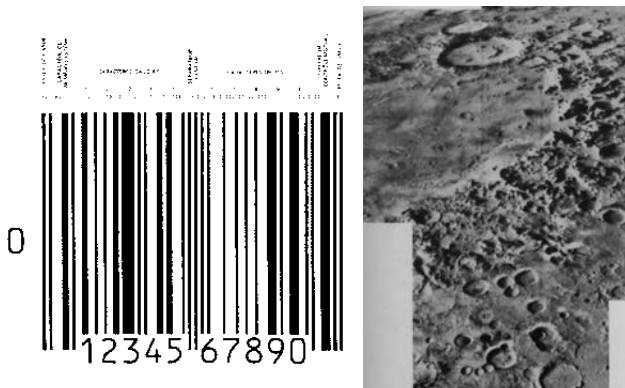
enthält, näher zum korrekten Wort als zu jedem anderen Codewort.

Ein einfaches Beispiel

Ein Beispiel solch codierter Information ist jedem von uns geläufig: Es sind die *Strich-Codes*, mit denen heute die meisten Produkte versehen sind. Zunächst wird jedes Produkt mit einer Folge von 12 Zahlen (aus 0 bis 9) identifiziert. Jede Zahl wird ersetzt durch ein Codewort mit sieben 0'en und 1'en. Auf dem Produkt werden 0 und 1 durch einen dünnen Strich dargestellt: 0 durch einen weißen Strich und 1 durch einen schwarzen Strich. Zum Beispiel wird 5 codiert durch 0110001, so dass auf dem Produkt ein weißer Strich erscheint, eine Einheit breit, gefolgt von einem schwarzen Strich, zwei Einheiten breit, einem weißen Strich, drei Einheiten breit, und einem abschließenden schwarzen Strich. Wird nun das Produkt an der Kasse des Supermarktes gescannt, so kann es passieren, dass ein Bit (d.h. eine 0 oder 1) falsch gelesen wird. Die Codewörter für die Zahlen und für die Produkte sind so gewählt, dass der Scanner den Fehler entdeckt und der Kassierer ein Signal gibt, den Scannvorgang zu wiederholen. Jeder von uns hat dies sicher schon des öfteren erlebt.

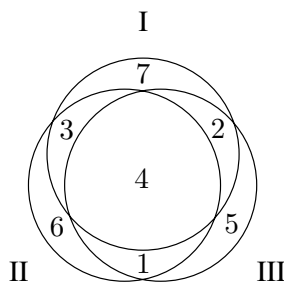
Einer der frühesten Erfolge von Fehler korrigierenden Codes war die Qualität der Bilder von Satelliten,

z.B. vom Mars. Wären diese Bilder ohne die Verwendung von Codes zur Erde übertragen worden, so wäre überhaupt nichts zu erkennen gewesen. Die Kontrollstationen hätten nur einen unverständlichen Bildsalat erhalten (in der Fachsprache: random noise).



Strich-Code und Viking-Aufnahme vom Mars (Jet Propulsion Laboratory of the California Institute of Technology)

Der erste effiziente Fehler korrigierende Code wurde von R.W. Hamming 1948 in den Bell Laboratories entworfen. Eine binäre Folge (d.h. eine Folge von 0 und 1) wurde in Blöcke zu je 4 Bits zerlegt. Hamming's Idee war es, jedem 4-Block drei Korrekturbits anzuhängen, mit Hilfe der folgenden Regel. Betrachten wir das folgende Diagramm:



Die 4 Bits (z.B. 1101) werden in die Teile mit den Nummern 1 bis 4 geschrieben. Die Korrekturbits kommen von den Teilen 5 bis 7. Die Regel ist, dass jeder Kreis eine gerade Anzahl von 1'en enthalten muss. Eine Konfiguration von 7 Bits, welche einen Fehler enthält, ergibt einen oder mehrere Kreise mit einer ungeraden Anzahl von 1'en. Das Bit, welches in all diesen Kreisen mit ungerader Parität enthalten ist, aber nicht in jener mit gerader Parität, muss dann das fehlerhafte Bit sein.

Wir sehen in diesem Beispiel, dass jedes Wort der Länge 7 genau 4 Informationsbits enthält. Daher sagen wir, dass der Hamming-Code ein binärer $[7, 4]$ -Code ist mit Informationsrate $\frac{4}{7}$. Wir bemerken, dass die einfache Wiederholung der 4 Informationsbits einen $[8, 4]$ -Code ergibt, also einen Code mit Informationsrate $\frac{4}{8} = \frac{1}{2}$ (schlechter als im Hamming-Code). Und dieser Code kann zwar einen Fehler entdecken, aber nicht korrigieren.

Von Musik zu Audiobits

Bevor wir uns den Codes zuwenden, wollen wir besprechen, wie Musik in eine Folge sogenannter Audiobits umgewandelt wird. Im CD-System wird das Analogsignal 44.100 Mal pro Sekunde bemustert (in der Fachsprache „sampled“). Diese Rate von 44,1 kHz ist ausreichend, um Frequenzen bis zu 20.000 Hz hören zu können. Die Muster werden uniform in 16 Bits zerlegt, und da wir Stereo-Musik empfangen wollen, so entspricht jedes Muster einer Folge von 32 Bits. So eine Folge von 32 Bits wird aufgefasst als 4 aufeinanderfolgende Bytes (ein Byte ist eine Folge von 8 Bits). Für den Codierungsvorgang werden diese Bytes als Elemente des Körpers \mathbb{F}_{2^8} aufgefasst. Wer nicht weiß, was ein (mathematischer) Körper ist: In einem Körper gelten die üblichen Rechenregeln, d.h. wir können Bytes addieren, multiplizieren und dividieren, wie wir es gewohnt sind.

Genauso wie bei den Hamming-Codes wird die Folge der Bytes in Gruppen fester Länge zerlegt, an die dann Korrekturbits angehängt werden. Im CD-System wird eine Folge von 24 Bytes in zwei Schritten zu einem Codewort der Länge 32 Bytes verwandelt. Die dabei verwendeten Codes sind sogenannte Reed-Solomon-Codes vom Typ $[28, 24]$ bzw. $[32, 28]$, die im nächsten Abschnitt erklärt werden. Schließlich wird noch ein Extrabyte hinzugefügt, welches die Kontroll- und Anzeigeeinformation enthält. So kann der CD-Player (und der Hörer) erkennen, auf welcher Spur sich die CD gerade befindet. Also: Sechs Muster führen zu 33 Datenbytes, von denen jedes aus 8 Bits besteht.

Eine Sekunde Musik führt zu einer Folge von 4.321.800 Bits auf der Tonspur. Falls der CD-Player ein Bit mit der sehr kleinen Wahrscheinlichkeit von $\frac{1}{10.000}$ falsch interpretieren würde, so würden immer noch hunderte Fehler pro Sekunde passieren!

Es gibt mehrere Gründe für Fehler auf einer CD. Es könnte Schmutz auf der CD sein, Luftblasen im Plastikmaterial, Ungenauigkeiten beim Druck, Fingerabdrücke, Kratzer, Oberflächenfehler. Es sei angemerkt, dass Fehler hauptsächlich hintereinander auftreten (sogenannte „burst errors“). Da wir Codes verwenden, die zufällige Fehler korrigieren, so erfordert dies ein systematisches Austauschen von Bytes, damit Bytes, die in den Codewörtern aufeinanderfolgen, nicht mehr benachbart sind auf der CD.

Reed-Solomon-Codes

Das Codierungssystem, das auf einer Compact Disc verwendet wird, hat den Fachnamen CIRC (Cross-Interleaved Reed-Solomon-Code). Der Inhalt dieses Abschnittes sind die mathematischen Prinzipien, die in der Fehlerkorrektur auf CDs eine Rolle spielen. Wie wir gesehen haben, besteht das Code-Alphabet auf der CD aus $2^8 = 256$ Buchstaben, welche den Körper \mathbb{F}_{2^8} bilden. Um die etwas komplizierten Rechnungen in \mathbb{F}_{2^8} zu vermeiden, illustrieren wir die Arbeitsweise der Reed-Solomon-Codes an einem Beispiel über einem Alphabet mit 31 Elementen, d.h. über dem Körper \mathbb{F}_{31} .

Die Elemente von \mathbb{F}_{31} sind $0, 1, 2, \dots, 30$ und die Rechenoperationen werden wie üblich ausgeführt, wobei das Ergebnis jeweils modulo 31 reduziert wird. Das heißt: Wollen wir z.B. 6 und 9 multiplizieren, so erhalten wir $6 \times 9 = 54$ und dividieren anschließend das Resultat durch 31. Das „Produkt“ 6×9 in \mathbb{F}_{31} ist dann der Rest 23

$$6 \times 9 = 54 = 31 + 23.$$

Wir schreiben kurz: $6 \times 9 = 23$ (modulo 31).

Als ein Beispiel betrachten wir ein Buch mit 200 Seiten, das beschrieben werden soll mit einer Druckgröße, die 3000 Symbole pro Seite erlaubt. Wir identifizieren die Buchstaben a bis z mit den Zahlen 1 bis 26, den Zwischenraum mit 0, und benutzen 27 bis 30 für Punkt, Komma, Strichpunkt und ein weiteres Symbol.

Wir werden vom Drucker informiert, dass die Technik, die er benutzt, nicht allzu gut ist. Tatsächlich ist sie so schlecht, dass jedes Symbol auf einer Seite mit Wahrscheinlichkeit 0,1% inkorrekt ist. Das bedeutet, dass im Durchschnitt 3 Druckfehler pro Seite passieren, was eindeutig zu viel ist. Man bedenke nur, wie lästig schon ein gelegentliches Klopfen auf der Schallplatte ist. Um die Situation zu verbessern, verwenden wir Ideen aus der Codierungstheorie.

In einem ersten Ansatz zerlegen wir die Folge der Symbole in Gruppen zu je 4. Vor jeder Gruppe von 4 Symbolen werden zwei 2 Korrektursymbole eingefügt. Wir bezeichnen das resultierende Codewort mit $a = (a_0, a_1, \dots, a_5)$, wobei a_0 und a_1 die Korrektursymbole und a_2, a_3, a_4, a_5 die 4 Informationssymbole sind (alles in \mathbb{F}_{31}).

Betrachten wir das Wort CODE. Dieses Wort korrespondiert zu $(a_2, a_3, a_4, a_5) = (3, 15, 4, 5)$. Die Codierungsregeln, um a_0 und a_1 zu berechnen, sind nun:

$$(i) \quad a_0 + a_1 + a_2 + a_3 + a_4 + a_5 = 0 \text{ (modulo 31)}$$

$$(ii) \quad a_1 + 2a_2 + 3a_3 + 4a_4 + 5a_5 = 0 \text{ (modulo 31)}.$$

Daraus erhalten wir $a_0 = 3$ und $a_1 = 1$, so dass CODE als CACODE codiert wird.

Gehen wir zum anderen Ende und nehmen wir an, wir erhalten EPGOOF. Wenn wir die Korrektursymbole auslassen, so würde GOOF als gesendetes Wort resultieren. Aber wir sehen sofort, dass ein Fehler passiert sein muß, denn EPGOOF korrespondiert zu $(a_0, a_1, \dots, a_5) = (5, 16, 7, 15, 15, 6)$ und die Summe der a_i ist

$$5 + 16 + \dots + 6 = 64 = 2 \text{ (modulo 31)},$$

was unserer Codierungsregel widerspricht. Wir vermuten, dass wahrscheinlich eines der Symbole a_i durch $a_i + 2$ ersetzt wurde. Der Wert des Fehler in a_i ist 2, das heißt wir werden $2i$ als Fehlerwert erhalten, wenn wir a_0, \dots, a_5 in Gleichung (ii) einsetzen. Einsetzen ergibt (modulo 31)

$$\begin{aligned} a_1 + 2a_2 + \dots + 5a_5 &= 16 + 14 + 45 + 60 + 30 \\ &= 165 = 10, \end{aligned}$$

also ist $i = \frac{10}{2} = 5$, das heißt der Fehler passierte in der fünften Position. Anstelle von 6 sollte 4 stehen — und wir decodieren EPGOOF in GOOD! Wie schon gesagt, die arithmetischen Operationen in \mathbb{F}_{28} sind ein wenig komplizierter, aber alle Reed-Solomon-Codes verwenden Codierungs- und Decodierungsregeln wie die Gleichungen (i) und (ii).

Wenn wir nun auch wissen, dass dieser Code einen Fehler in einer 6-Gruppe korrigieren kann, so müssen wir ehrlicherweise auf ein Problem eingehen, das auch auf der CD auftritt. Der Code hat eine Informationsrate von $\frac{4}{6} = \frac{2}{3}$. Da wir dieselbe Anzahl von Seiten derselben Größe benutzen wollen, so müssen wir also $1\frac{1}{2}$ -mal so viele Symbole pro Seite unterbringen. Zu unserer Ernüchterung teilt uns aber der Drucker mit, dass die Druckfehlerwahrscheinlichkeit der $1\frac{1}{2}$ -mal kleineren Druckgröße *doppelt so hoch* ist! Mit anderen Worten: Mit dem kleineren Font müssen wir im Durchschnitt 9 Fehler pro Seite *vor der Fehlerkorrektur* in Kauf nehmen. Und nach der Korrektur? Ein Wort mit 6 Symbolen wird korrekt decodiert, falls es höchstens einen Fehler enthält. Die Wahrscheinlichkeit, dass mehr als ein Fehler passiert ist

$$\sum_{i=2}^6 \binom{6}{i} (0,002)^i (0,998)^{6-i} \approx 0,00006.$$

Im Buch wird es einige Wörter geben, die zwei oder mehr Druckfehler enthalten, aber es werden im Schnitt nicht mehr als 10 Wörter im gesamten Buch sein — eine bemerkenswerte Verbesserung!

Mit einer geringfügigen Veränderung wird die Situation dramatisch besser. Dazu verwenden wir einen etwas komplizierteren Reed-Solomon-Code. Wir zerlegen die Symbole in Gruppen von 8, die wir mit $(a_4, a_5, \dots, a_{11})$ bezeichnen. Davor fügen wir 4 Korrekturzeichen hinzu nach den folgenden Regeln:

$$(i) \quad a_0 + a_1 + a_2 + a_3 + \dots + a_{11} = 0 \text{ (modulo 31)}$$

$$(ii) \quad a_1 + 2^k a_2 + 3^k a_3 + \dots + 11^k a_{11} = 0 \text{ (modulo 31) } (k = 1, 2, 3).$$

Die Codierung besteht also aus der Lösung von 4 Gleichungen mit den 4 Unbekannten a_0, a_1, a_2, a_3 . Der Leser kann sich sofort wie oben überlegen, wie ein Fehler korrigiert wird. Nehmen wir an, es passierten zwei Fehler mit den Abweichungen e_1 und e_2 in Positionen i und j . Einsetzen in die Gleichungen (i) und (ii) ergibt sofort

$$e_1 + e_2 \text{ (modulo 31) und}$$

$$i^k e_1 + j^k e_2 \text{ (modulo 31) } (k = 1, 2, 3).$$

Daraus können wir e_1 und e_2 eliminieren und erhalten eine quadratische Gleichung mit i und j als Lösungen. Danach können wir e_1 und e_2 ermitteln und die beiden Fehler korrigieren. Der neue Code ist also ein 2-Fehler korrigierender Code.

Glücklicherweise ergibt das kein neues Problem beim Drucken. Dieser neue Reed-Solomon-Code hat wiederum Informationsrate $\frac{2}{3}$ ($= \frac{8}{12}$) wie der vorige, so dass die Druckfehlerwahrscheinlichkeit wieder $= 0,2\%$ pro Symbol ist. Die Decodierung wird nur versagen, wenn ein gedrucktes Wort von 12 Symbolen mehr als zwei Fehler enthält. Die Wahrscheinlichkeit, dass dies passiert, ist

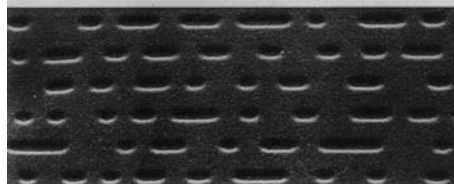
$$\sum_{i=3}^{12} \binom{12}{i} (0,002)^i (0,998)^{12-i} < 0,000002.$$

Das gesamte Buch hat 600.000 Symbole, also 75.000 Wörter der Länge 8. Da $75.000 \times 0,000002 = 0,15$ ist, so ist es unwahrscheinlich, dass überhaupt ein Druckfehler auftritt! Das ist nun tatsächlich eine eindrucksvolle Verbesserung!

Auf einer CD ist die Informationsrate, wie im letzten Abschnitt erwähnt, $\frac{24}{32} = \frac{3}{4}$. Wie eben erläutert (am Beispiel des kleineren Fonts) wird die Fehlerwahrscheinlichkeit für ein Bit dadurch erhöht im Vergleich zur Situation, wenn keine Korrektur durchgeführt wird. Wie wir schon erwähnt haben, kann eine CD ohne weiteres 500.000 Bitfehler enthalten. Allerdings passieren diese Fehler nicht zufällig (wie in unserem Beispiel des Buches), sondern meistens in „bursts“ (hintereinander). Es kann vorkommen, dass einige 1000 aufeinanderfolgende Symbole (z.B. durch einen Kratzer) fehlerhaft sind. Dem wird entgegengewirkt, indem benachbarte Informationssymbole in *verschiedenen* Codewörtern erscheinen (genannt „Interleaving“). Eines muss man sich außerdem beim Design eines CD-Systems vor Augen halten: Der Speicher, der für die Bits zur Verfügung steht, kann nicht zu groß sein. Das impliziert natürlich Beschränkungen bei der Länge der Codewörter und beim Interleaving. Alle Berechnungen, die zur Fehlerkorrektur benötigt werden, passieren im Bruchteil einer Sekunde, und das ist der Grund, warum wir Musik hören, praktisch unmittelbar, nachdem der CD-Player eingeschaltet wird. In dem Buch-Beispiel sahen wir, dass ein längerer Code zwar bessere Korrekturleistung bringt, aber auch mehr Berechnungen benötigt.

Die Compact Disc

Die Musik wird auf einer Compact Disc in Digitalform als eine 5 km lange spiralförmige Spur aufgezeichnet, welche aus einer Folge von sogenannten *Pits* besteht. Die Teile zwischen aufeinanderfolgenden *Pits* heißen *Lands*. Die Steigung der Spur ist $1,6\mu\text{m}$, die Breite ist $0,6\mu\text{m}$ und die Tiefe der *Pits* ist $0,12\mu\text{m}$. Die Abbildung zeigt eine Vergrößerung mehrerer paralleler Spuren.



Vergrößerung mehrerer paralleler Spuren einer CD

Die Spur wird optisch von einem Laserstrahl gescannt. Jeder Land/Pit oder Pit/Land Übergang wird als 1 interpretiert, und alle anderen Bits als 0. So wird z.B. ein Pit der Länge $1,8\mu\text{m}$ gefolgt von einem Land der Länge $0,9\mu\text{m}$ übersetzt in die Folge 100000100. Der Durchmesser des Lichtstrahls ist ungefähr $1\mu\text{m}$. Wenn er auf ein Land fällt, so wird er fast völlig reflektiert. Da die Tiefe eines Pits ungefähr $\frac{1}{4}$ der Wellenlänge des Lichtes im Material der Disc ist, so bewirkt Interferenz, dass weniger Licht von den Pits in die Öffnung des Objektivs reflektiert wird.

Es gibt mehrere Anforderungen an die Folge der Bits, die in der CD beachtet werden müssen. Jedes Pit oder Land muss mindestens 3 Bits lang sein. Das wird gefordert, um zu vermeiden, dass der Lichtstrahl zwei aufeinanderfolgende Übergänge zwischen Pits und Lands gleichzeitig registriert, was eine sogenannte Intersymbol-Interferenz bewirken würde. Jedemal wenn ein Übergang auftritt, wird die „Bit-Uhr“ im CD-Player synchronisiert. Da dies so rechtzeitig erfolgen muss, um einen Verlust an Synchronisation zu vermeiden, darf kein Pit oder Land länger als $3,3\mu\text{m}$ sein, d.h. zwei 1'en in der Sequenz sind durch höchstens 10 0'en getrennt. Die Einschränkung an die maximale Landlänge ist außerdem notwendig für den Mechanismus, der den Laser auf der Spur hält. Eine letzte Anforderung ist, dass der Niedrig-Frequenz Anteil des Signals auf ein Minimum beschränkt ist. Dies bedingt, dass die Gesamtlänge der Pits und Lands von Beginn der Spur an ungefähr gleich ist. Diese Bedingung wird für den Mechanismus benötigt, der entscheidet, ob etwas „hell“ oder „dunkel“ ist. (Das vermindert auch den negativen Effekt eines Fingerabdruckes auf der CD.)

Jedes Byte in einem Codewort wird in 17 sogenannte Kanalbits auf der CD umgewandelt. Wenn die CD gelesen wird, so werden diese Bits zurück verwandelt in Bytes. Dann folgt De-Interleaving, Fehlerkorrektur, Digital-zu-Analog Konversion und schließlich hören wir Musik, mit Dank an Mozart und andere — und an die *Mathematik*.

Literaturverzeichnis

- [1] M. Aigner und E. Behrends, *Alles Mathematik*, Vieweg, Braunschweig, Wiesbaden, 3. Auflage, 2008.