Codierungstheorie und ihre Beziehung zu Geometrie und Zahlentheorie

von *Friedrich Hirzebruch*, Bonn

Ausarbeitung in erweiterter Form von Herrn Nils-Peter Skoruppa. Für Durchsicht und Korrekturen bin ich Herrn Ulrich Everling dankbar.

Die Codierungstheorie versucht, möglichst effiziente Wege der Nachrichtenübermittlung aufzuzeigen. Effizienz bedeutet hierbei: ein möglichst geringer Energieaufwand bei gleichzeitig möglichst großer Redundanz. Die mathematische Normalisierung dieses Problems führt zu bestimmten endlichen Strukturen, den Codes. Überraschenderweise sind nun die für den Codierungstheoretiker interessanten Fragestellungen über Codes auf das Engste verflochten mit teilweise sehr alten Fragestellungen aus der reinen Mathematik, die auf den ersten Blick nichts mit Codierungstheorie zu tun haben und die von Mathematikern völlig unabhängig studiert wurden oder noch studiert werden.

Was sind Codes?

Betrachten wir ein naheliegendes Beispiel. Seit 1969 wird jedes in Westeuropa oder den USA erscheinende Buch mit der Internationalen Standard-Buchnummer (ISBN) versehen. Solch eine ISB-Nummer ist 10-stellig, z. B.

3-531-08370-8

(an der zehnten Stelle taucht gelegentlich statt einer Ziffer das Symbol X auf). Die eigentliche Information, also die Nummer eines Buches, ist hierbei die aus den ersten 9 Ziffern gebildete Zahl. Die letzte Ziffer ist eine sogenannte Kontrollziffer. Sie ist so bestimmt, daß für eine ISB-Nummer $a_1a_2a_3 \ldots a_{10}$ die Zahl $1 \cdot a_1 + 2a_2 + 3a_3 + \ldots + 10a_{10}$ stets durch 11 teilbar ist (wobei gegebenenfalls das Symbol X als Zahl 10 zu interpretieren ist). So ist im obigen Beispiel

$$1 \cdot 3 + 2 \cdot 5 + 3 \cdot 3 + 4 \cdot 1 + 5 \cdot 0 + 6 \cdot 8 + 7 \cdot 3 + 8 \cdot 7 + 9 \cdot 0 = 151.$$

Folglich muß die letzte Ziffer eine 8 sein:

$$151 + 8 \cdot 10 = 231 = 11 \cdot 21.$$

Die Kontrollziffer hat den offensichtlichen Vorteil, in einem gewissen Umfang vor Fehlern zu schützen, die beim Abdruck der ISB-Nummer in einem Katalog, beim Abspeichern in einem Computer oder sonstwo auftreten können. Wird etwa genau eine Ziffer beim Übermitteln einer ISB-Nummer falsch weitergegeben, z. B.

3-511-08370-8

an Stelle der oben gegebenen Nummer, so wird – wie man sich leicht überlegen kann – die empfangene Nummer auf keinen Fall mehr die oben beschriebene, charakteristische Eigenschaft einer ISB-Nummer haben; im Beispiel ist $1\cdot 3+2\cdot 5+3\cdot 1+4\cdot 1+5\cdot 0+6\cdot 8+7\cdot 3+8\cdot 7+9\cdot 0+10\cdot 8=225$, und die Zahl ist nicht durch 11 teilbar. Die ISB-Nummern sind also so beschaffen, daß *ein* Fehler stets entdeckt werden kann. Ist die Stelle des Fehlers bekannt, so kann er sogar korrigiert werden: Im Beispiel ist die dritte Stelle falsch. Es ist eine Zahl a zwischen 0 und 9 zu bestimmen, so daß

$$1\cdot 3+2\cdot 5+3\cdot a+4\cdot 1+5\cdot 0+6\cdot 8+7\cdot 3+8\cdot 7+9\cdot 0+10\cdot 8=222+3\cdot a$$

durch 11 teilbar ist, und diese Aufgabe hat genau eine Lösung, nämlich $a=3$. Der Fehler ist korrigiert. Treten mehr als ein Fehler auf, so kann es allerdings geschehen, daß diese Fehler nicht mehr entdeckt werden; z. B. weicht 3-531-07350-8 an genau zwei Stellen von der anfangs gegebenen ISB-Nummer ab und ist dennoch eine korrekte ISB-Nummer.

Der Codierungstheoretiker würde die eben geschilderte Situation folgendermaßen beschreiben. Gegeben ist ein endliches Alphabet A – hier die Ziffern 0 bis 9 und das Symbol X. Aus den Buchstaben des Alphabets A werden Wörter zu je n Buchstaben gebildet – hier ist $n=10$. Die Menge aller möglichen, n-stelligen Wörter wird mit A^n bezeichnet. In dieser Menge A^n aller n-stelligen Wörter wird nun eine Teilmenge C, ein „Code", als Menge der zulässigen Wörter ausgezeichnet. Die Wörter in C heißen dann Codewörter. Im Beispiel besteht der Code aus den Wörtern $a_1a_2a_3\ldots a_{10}$, für die $1\cdot a_1+\ldots+10\cdot a_{10}$ durch 11 teilbar ist und unter a_1 bis a_9 kein X vorkommt.

In der Praxis ist A natürlich kein willkürlich gewähltes Alphabet. Um mit einem Code zu arbeiten, muß man ihn beschreiben können. Die naheliegende Möglichkeit, einen Code zu beschreiben, indem man die Codewörter auflistet, ist nicht praktikabel (der ISBN-Code enthält 1 000 000 000 Codewörter). Was benötigt wird, ist ein möglichst einfacher Algorithmus, der entscheidet, ob ein vorgelegtes Wort ein Codewort ist oder nicht. Im ISBN-Beispiel besteht dieser Algorithmus aus einigen Additionen, Multiplikationen und einem Test auf Teilbarkeit durch 11. Die offensichtliche Ursache für diese erhebliche Vereinfachung ist die Tatsache, daß das Alphabet beim ISBN-Code aus Ziffern besteht, und mit Ziffern

kann man algorithmisch operieren, genauer: man kann sie addieren und multiplizieren. Es ist daher nicht verwunderlich, daß die in der Praxis verwendeten Alphabete meist so beschaffen sind, daß man mit den Buchstaben „rechnen" kann.

Tatsächlich sind die am häufigsten verwendeten Alphabete „endliche Körper". Auch beim ISBN-Code gehen die etwas tiefer liegenden Eigenschaften (ein Fehler kann entdeckt und – falls die Stelle des Fehlers bekannt ist – sogar korrigiert werden) auf die Tatsache zurück, daß 11 eine Primzahl ist, und daß man die Ziffern $0, \ldots, 9, X$ als Elemente des Körpers $\mathbf{F}_{11}$ auffassen kann. Was ist ein endlicher Körper?

Studiert wurden endliche Körper zuerst von dem französischen Mathematiker Evariste Galois (1811–1832). Die einfachsten Beispiele erhält man folgendermaßen: Zu einer fest gewählten Primzahl p bezeichne $\mathbf{F}_p$ die Menge aller möglichen Reste, die bei Division einer ganzen Zahl durch p auftreten können; $\mathbf{F}_p$ besteht also aus den Zahlen $0, 1, 2, \ldots, p-1$. Man kann mit den Zahlen in $\mathbf{F}_p$ rechnen, indem man als Summe zweier Zahlen a, b aus $\mathbf{F}_p$ diejenige Zahl c aus $\mathbf{F}_p$ vereinbart, für die $a+b \equiv c \bmod p$ gilt. Letzteres ist eine in der Mathematik übliche Schreibweise und bedeutet, daß $a+b-c$ durch p teilbar ist, oder – was gleichbedeutend ist – daß c der Rest von $a+b$ bei Division durch p ist. Analog vereinbart man als Produkt von a und b diejenige Zahl d in $\mathbf{F}_p$, so daß $a \cdot b \equiv d \bmod p$ ist. Mit der so erklärten Addition und Multiplikation in $\mathbf{F}_p$ kann man nun genau so rechnen, wie man etwa mit rationalen Zahlen rechnet. (Die Voraussetzung, daß p eine Primzahl ist, ist notwendig, um sicherzustellen, daß zu jedem von 0 verschiedenen Element a in $\mathbf{F}_p$ ein b gefunden werden kann, sodaß $a \cdot b \equiv 1 \bmod p$ gilt, d. h. daß in $\mathbf{F}_p$ die Division durch a erklärt ist.)

In der Nachrichten- und Computertechnik verwendet man häufig aus naheliegenden Gründen als Alphabet den Körper $\mathbf{F}_2$, d. h. die Buchstaben 0, 1 („Strom fließt, Strom fließt nicht"). Jeden dieser Buchstaben bezeichnet man auch als „Bit". Ein 5-Bit-Wort ist also ein Element von $(\mathbf{F}_2)^5$. Hier ist die Additions- und Multiplikationstabelle für den Körper $\mathbf{F}_2$:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

.

Diese Tabellen sind auch vom „ausschließenden Oder" bzw. „Und" der Aussagenlogik bekannt.

Allgemein gibt es zu einer vorgelegten natürlichen Zahl n genau dann einen Körper mit n Elementen, wenn n eine Primzahlpotenz ist. Dieser Körper ist (genauer: seine Rechenregeln sind) völlig eindeutig durch Angabe von n bestimmt, und er wird mit $\mathbf{F}_n$ bezeichnet.

Auch die für den Nicht-Mathematiker vielleicht etwas fremdartig erscheinenden Körper $\mathbf{F}_n$, wo n nicht gerade eine Primzahl ist, finden in der Praxis Verwendung. So wurde zum Beispiel der Körper $\mathbf{F}_{256}$ ($256 = 2^8$) benutzt, um Informationen von der Raumsonde Giotto, die zur Beobachtung des Kometen Halley eingesetzt war, zur Erde zu übermitteln. Genauer wurde dabei ein sogenannter Reed-Solomon-Code, bestehend aus 255-stelligen Wörtern über dem Alphabet $\mathbf{F}_{256}$, benutzt. Dies klingt weit weniger verblüffend, wenn man weiß, daß man jedes Element von $\mathbf{F}_{256}$ selbst als 8-Bit-Wort auffassen kann. Es gibt ein Element α in $\mathbf{F}_{256}$, so daß sich jedes weitere Element in $\mathbf{F}_{256}$ in der Form $a_0 + a_1 \cdot \alpha + a_2 \cdot \alpha^2 + \ldots + a_7 \cdot \alpha^7$ mit einem eindeutig bestimmten 8-Bit-Wort $a_0 a_1 \ldots a_7$ schreiben läßt („+", „$\cdot$", „α^2", ... stehen hierbei natürlich für die Addition, Multiplikation bzw. Potenz im Körper $\mathbf{F}_{256}$). Also hat man zum Beispiel

8-Bit-Wort	Element von $\mathbf{F}_{256}$
01100010	$\alpha+\alpha^2+\alpha^6$
01000111	$\alpha+\alpha^5+\alpha^6+\alpha^7$.

Nun gibt es genau 240 verschiedene solche α, d. h. fast jedes Element in $\mathbf{F}_{256}$ hat die beschriebene Eigenschaft. Man kann es aber so einrichten, daß etwa

$$\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$$

gilt (es gibt genau 8 verschiedene solche α, und jedes solche α hat noch die bemerkenswerte Eigenschaft, daß $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{254}$ genau die von 0 verschiedenen Elemente des Körpers sind). Damit ist dann aber klar, wie man im Körper $\mathbf{F}_{256}$ rechnet: in der naheliegenden Art und Weise unter Einbeziehung der Rechenregel $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$; also z. B.

$$\begin{aligned}
&(1+\alpha)+(1+\alpha^4) = (1+1)+\alpha+\alpha^4 = \alpha+\alpha^4,\\
&(1+\alpha^3+\alpha^5)\,(1+\alpha^4) = 1+\alpha^3+\alpha^5+\alpha^4+\alpha^7+\alpha^9\\
&= 1+\alpha^3+\alpha^4+\alpha^5+\alpha^7+\alpha(\alpha^4+\alpha^3+\alpha^2+1)\\
&= 1+\alpha+\alpha^7 .
\end{aligned}$$

Man mag einwenden, daß es sich bei dem Reed-Solomon-Code im Grunde doch um einen binären Code, d. h. einen Code über $\mathbf{F}_2$, handelt. Dies mag man zwar so sehen (und man bezeichnet einen Reed-Solomon-Code deshalb auch als „block-code"); allerdings würde man bei einer Einengung auf diese Sichtweise die weiter unten gegebene Erklärung dieses Codes nicht verstehen, und man hätte ihn ohne Kenntnis des Körpers $\mathbf{F}_{256}$ wohl kaum entdeckt. Welchen Sinn hat $(10010100) \cdot (10001000) = (11000001)$, wenn nicht den oben beschriebenen?

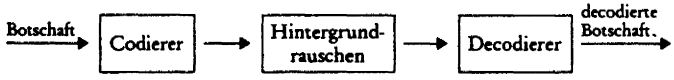
Vor einiger Zeit ist die digitale Informationsverarbeitung in Form des Compact-Disc-Systems in der Unterhaltungselektronik angewandt worden. Insbesondere

wird dabei eine Kombination von zwei Reed-Solomon-Codes (Cross-Interleaved Reed-Solomon-Code) benutzt. In CD-Plattenspielern ist also in bestimmter Art und Weise der Körper $\mathbb{F}_{256}$ implementiert.

Allgemein ist ein Code zunächst lediglich eine Menge C von Codewörtern in der Menge A^n aller n-stelligen Wörter über einem Alphabet A, wobei A meist ein Körper $\mathbb{F}_q$ ist. Um zu sehen, was solch ein Code soll, und welche Forderungen ein Codierungstheoretiker an einen Code stellt, müssen wir etwas zum Thema „Übermitteln von Nachrichten" sagen.

Was sollen Codes leisten?

Sicherlich stark vereinfacht stellen wir uns eine Nachrichtenübermittlung in drei Schritte zerlegt vor:



Eine Botschaft wird in einen Codierer eingegeben; dies können die in bestimmten Zeitabständen gemessenen Daten eines akustischen Signals, die Schwärzung der Punkte eines Rasters zur Erfassung eines Bildes (vielleicht durch die Kamera einer Raumsonde aufgenommen) oder für den Speicher eines Computers bestimmte (eventuell vom Computer selbst berechnete) Daten sein. Diese Botschaft verläßt den Codierer als Folge von Codewörtern eines Codes C in einer Menge A^n von n-stelligen Wörtern; technisch zum Beispiel als Folge von elektrischen Spannungsstößen verschiedener Stärke. Solch ein Codewort durchläuft nun einen „Informationskanal" und ist dabei einem „Hintergrundrauschen" ausgesetzt. „Informationskanal" kann dabei ein elektromagnetisches Feld sein, es kann aber auch für den Prozeß des Abspeicherns und anschließenden Wiederaufrufens eines Binärwortes in einem Computer stehen. Auch das Wort „Hintergrundrauschen" ist nicht wörtlich zu nehmen; es kann elektrische Interferenz, Staub oder Kratzer auf einer CD-Platte oder auch das Bombardement eines Computer-Chips durch α-Teilchen bedeuten. Dieses Hintergrundrauschen bewirkt jedenfalls, daß ein Codewort möglicherweise verfälscht zum Decoder gelangt. Es ist natürlich wünschenswert, solche Verfälschungen, d. h. Fehler, zu entdecken. Nun ist dies in gewissem Maße gerade durch die Unterscheidung zwischen Codewörtern und Nicht-Codewörtern gegeben – denken wir an den ISBN-Code, der einen Fehler entdecken kann. Wie aber soll die Decodierungsvorrichtung auf einen für sie offensichtlichen Fehler reagieren?

Bei den ersten Computern wurde im Fall, daß bei einer Zwischenrechnung kein zulässiges Binärwort – also kein Codewort – herauskam, der gesamte Rechenvorgang angehalten. Der Geschichte nach soll dieses R. W. HAMMING 1947 dazu geführt haben, den ersten praktikablen Fehler-korrigierenden Code zu entwikkeln. Die Idee ist, den Code C so zu wählen, daß die Codewörter sich möglichst stark voneinander unterscheiden. Die Decodierungsvorrichtung sucht dann zu einem empfangenen Wort das diesem Wort ähnlichste Codewort heraus.

Hier das vielleicht einfachste Beispiel, der sogenannte Repetition-Code: Die zu übertragende Information ist „Ja" oder „Nein". „Ja" wird in 11111, „Nein" in 00000 codiert; also $C = \{11111,00000\}$ als Teilmenge von $(\mathbb{F}_2)^5$. Empfängt der Decodierer 01001, so ist es – mangels besserer Einsicht – vernünftig, anzunehmen, daß „Nein" gesendet wurde, denn 01001 unterscheidet sich nur an zwei Stellen von 00000, aber an drei Stellen von 11111. Der Decodierer gibt also „Nein" als decodierte Botschaft aus. Man überlegt sich leicht, daß dieser Code *zwei* Fehler korrigiert, d. h.: Tritt an höchstens zwei Stellen ein Übermittlungsfehler auf, so werden diese in jedem Fall erkannt und korrigiert. Wir bemerken einen wesentlichen Unterschied zum ISBN-Code: Der ISBN-Code kann keinen Fehler korrigieren (es sei denn, die Stelle des Fehlers ist bekannt).

Um dieses Phänomen quantitativ zu erfassen, bezeichnet man für zwei Wörter W und W' gleicher Länge über einem gegebenen Alphabet mit $d(W, W')$ die Anzahl der Stellen, an denen sich W und W' unterscheiden, also z. B. $d(101, 122) = 2$. Die Zahl $d(W, W')$ nennt man auch Hamming-Abstand von W und W'. Mit d bezeichnen wir den Minimalabstand eines gegebenen Codes C, d. h. den kleinsten Abstand $d(W, W')$, der auftritt, wenn W und W' die voneinander verschiedenen Wörter von C durchlaufen. Beim ISBN-Code ist $d = 2$, beim Repetition-Code ist $d = 5$.

Man kann sich nun überlegen, daß ein Code mit Minimalabstand d genau t Fehler korrigiert, wobei t durch $d = 2t + 1$ (für ungerades d) bzw. $d = 2(t + 1)$ (für gerades d) erklärt ist.

Um Nachrichten möglichst sicher zu übermitteln, ist man demnach an Codes mit möglichst großem Minimalabstand d interessiert. Der Repetition-Code hat $d = 5$; er ist für den Codierungstheoretiker dennoch nicht ohne Makel. Er ist zu aufwendig: fünf Bit zur Übertragung einer 1-Bit-Information. Eine Raumsonde unterliegt Energie- und Zeitbeschränkungen, bei Computern ist kein Speicherplatz zu vergeuden. Dies führt aber auch schon zu dem grundsätzlichen Problem der Codierungstheorie: Erwünscht sind Codes mit großem Minimalabstand d, d. h. stark unterschiedlichen Codewörtern. Dies zieht aber nach sich, daß man ein großes Alphabet oder Wörter mit vielen Stellen verwenden muß, also jedenfalls einen großen Aufwand. Letzteres ist wiederum unerwünscht.

Um diese Problematik quantitativ zu erfassen, führt man neben dem Minimalabstand d noch die Informationsrate R eines Codes C aus A^n ein:

$$R = \frac{\log_2 |C|}{\log_2 |A^n|}.$$

Hierbei steht $|C|$ bzw. $|A^n|$ für die Anzahl der Codewörter bzw. der überhaupt möglichen Wörter. Die Zahl $\log_2 |C|$ (und ähnlich $\log_2 |A^n|$) ist hierbei als minimale Anzahl von Bit's - etwa Ja-Nein-Entscheidungen - zu sehen, die man benötigt, um jedes beliebige Codewort mit Sicherheit aufzufinden.

Mit diesen Bezeichnungen läßt sich nun das Hauptproblem der Codierungstheorie etwas überspitzt folgendermaßen formulieren: Es sollen Codes gefunden werden, die die beiden inkompatiblen Ziele eines großen Minimalabstands d und einer großen Informationsrate R verwirklichen.

Der Hamming-Code

Der historisch wohl erste der etwas subtileren und effizienteren Codes ist der Hamming-Code: Jede Information, die gesendet werden soll, besteht aus 4-Bit-Wörtern. Tatsächlich gesendet wird ein 7-Bit-Wort, d. h. es wird an jede 4-Bit-Information eine 3-Bit-Kontrollfolge angehängt. Dies geschieht folgendermaßen: Ist $\varepsilon_0\varepsilon_1\varepsilon_2\varepsilon_3$ ein 4-Bit-Wort, also $\varepsilon_i = 0$ oder $= 1$, so setzen wir

$$k_1 = \varepsilon_0 + \varepsilon_2 + \varepsilon_3, \quad k_2 = \varepsilon_0 + \varepsilon_1 + \varepsilon_3, \quad k_3 = \varepsilon_0 + \varepsilon_1 + \varepsilon_2 .$$

Gerechnet wird hierbei in $\mathbb{F}_2$, also $k_1 = 0$ oder 1 je nachdem, ob die Summe der Zahlen ε_0, ε_2, ε_3 gerade ist oder nicht etc. Das 7-Bit-Wort $\varepsilon_0\varepsilon_1\varepsilon_2\varepsilon_3 k_1 k_2 k_3$ ist das Codewort, welches gesendet wird. Eine Übersetzungstabelle und eine andere nette Beschreibung des Hamming-Codes findet man in Abb. 1 und Abb. 2.

Der Hamming-Code ist ein sogenannter linearer Code: Da $\mathbb{F}_2$ ein Körper ist, trägt $(\mathbb{F}_2)^7$ in natürlicher Art und Weise die Struktur eines 7-dimensionalen Vek-

Abb. 1: Die Übersetzung der 4-Bit Information in 7-Bit-Codewörter beim Hamming-Code.

The Hamming code of dimension four

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

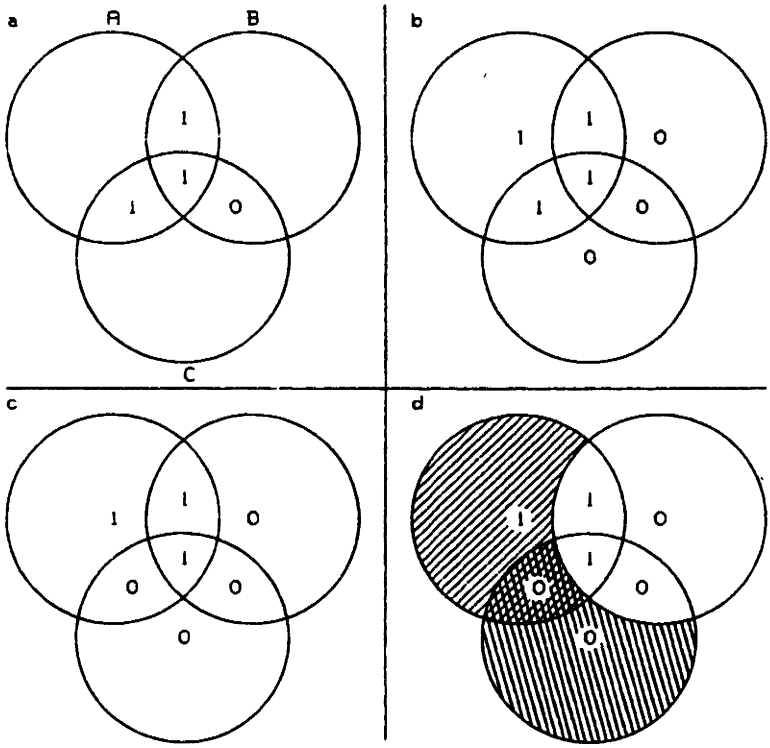


Abb. 2: Hamming Code is the simplest of the error-correcting procedures devised by Richard Hamming at the Bell Telephone Laboratories and employed today to protect data in computer memories. The (7, 4) code requires three so-called parity bits to protect each four bits of data. The construction called a Venn diagram depicts the scheme. Four bits of information are stored in the four central compartments of the diagram (*a*). Then three parity bits are stored (*b*). The rule is that the total number of 1's in each circle must be even. A soft error changes one of the data bits (*c*). The error is detected by reexamining the parity bits, which reveal (*d*) something wrong in circle *A* and circle *C* but not in circle *B*.

torraumes über $\mathbb{F}_2$, genau so, wie die reellen 7-Vektoren $(x_1, x_2, \ldots, x_7)$ einen 7-dimensionalen Vektorraum über den reellen Zahlen bilden. Die Codewörter des Hamming-Codes bilden einen linearen Unterraum von $(\mathbb{F}_2)^7$. Die in der Praxis verwendeten Codes sind meist linear, d. h. das Alphabet ist ein Körper $\mathbb{F}_q$ und die Codewörter bilden einen linearen Unterraum des Vektorraums $(\mathbb{F}_q)^n$ über $\mathbb{F}_q$.

Der Minimalabstand d des Hamming-Codes ist 3. Um dies einzusehen, beachte man, daß $d(W, W') = w(W-W')$ ist, wenn wir für ein Codewort W mit $w(W)$ das sogenannte Hamming-Gewicht von W bezeichnen, d. h. die Anzahl der von 0 verschiedenen Stellen von W. Da der Hamming-Code linear ist, ist demnach der Minimalabstand d auch gleich dem kleinsten $w(W)$, welches auftritt, wenn W alle von 0000000 verschiedenen Codewörter durchläuft. Ein Blick auf Abb. 1 zeigt, daß jedes von 0000000 verschiedene Codewort mindestens an drei Stellen eine 1 hat, d. h. es ist $d = 3$. Der Hamming-Code kann also einen Fehler korrigieren.

Die Informationsrate des Hamming-Codes ist $R = 4/7$. Würde man zur Übermittlung von 4-Bit-Wörtern an Stelle des Hamming-Codes einen Repetition-Code verwenden, so müßte man jedes 4-Bit-Wort dreimal wiederholen, um auf einen Minimalabstand von 3 zu kommen, d. h. um einen Fehler korrigieren zu können. Die Informationsrate dieses Repetition-Codes wäre 4/12. Die Informationsrate des Hamming-Codes ist demnach $12/7 = 1{,}71\ldots$-mal so groß wie die des Repetition-Codes, und dies bedeutet, daß der Hamming-Code in der gleichen Zeit etwa 71% mehr Information übermitteln kann als der Repetition-Code.

Genaugenommen gibt es eine ganze Serie von linearen Codes, die nach HAMMING benannt sind. Der hier beschriebene hat die genauere Bezeichnung „binärer (7,4)-Hamming-Code". Hamming-Codes werden benutzt, um die in Computerspeichern befindlichen Daten (vor natürlichen Phänomenen) zu schützen.

Reed-Solomon-Codes

Eine andere Serie von Codes, die wir oben schon erwähnt haben, sind die Reed-Solomon-Codes. Als Beispiel betrachten wir einen (255,223)-Reed-Solomon-Code über dem Körper $\mathbf{F}_{256}$. Die Informationen sind die 223-stelligen Wörter über dem Alphabet $\mathbf{F}_{256}$. Jede solche Information

$$a_0a_1a_2\ldots a_{222}$$

wird in ein 255-stelliges Codewort

$$b_0b_1b_2\ldots b_{254}$$

umgewandelt, wo die b_i ebenfalls Elemente des Körpers $\mathbf{F}_{256}$ sind. Diese Umwandlung geschieht durch die folgende Vorschrift

$$b_0+b_1X+b_2X^2+\ldots+b_{254}X^{254}$$
$$=(a_0+a_1X+a_2X^2+\ldots+a_{222}X^{222})\cdot(X-\alpha)(X-\alpha^2)(X-\alpha^3)\cdot\ldots\cdot(X-\alpha^{32}).$$

Gerechnet wird hierbei natürlich im Körper $\mathbb{F}_{256}$. Das Symbol X ist eine Unbestimmte, d. h. die linke Seite der obigen Gleichung erhält man, indem man die rechte Seite ausmultipliziert und nach Potenzen von X sortiert. Das Symbol α ist hierbei ein fest gewähltes Element von $\mathbb{F}_{256}$ mit der Eigenschaft, daß $1, \alpha, \alpha^2, \alpha^3, \ldots, \alpha^{254}$ gerade die von 0 verschiedenen Elemente des Körpers $\mathbb{F}_{256}$ sind (z. B. kann man das oben beschriebene α nehmen).

Der eben beschriebene Code ist offenbar linear. Durch Anwendung von etwas Algebra ist es möglich zu zeigen, daß jedes Codewort mindestens 33 von 0 verschiedene Stellen hat. Wie oben beim Hamming-Code folgert man hieraus, daß dieser Reed-Solomon-Code den Minimalabstand $d = 33$ hat, und daß er daher 16 Fehler korrigiert.

Man beachte, daß man jedes Element von $\mathbb{F}_{256}$ wie oben beschrieben als 8-Bit-Wort auffassen kann. Der Reed-Solomon-Code korrigiert also 128 Bit, wenn die 128 falsch übermittelten Bit in 16 Blöcken zu je 8 Bit auftreten. Aufgrund dieser Eigenschaft sind Reed-Solomon-Codes dort besonders gut geeignet, wo von vorneherein damit zu rechnen ist, daß Übermittlungsfehler kein einzelnes Bit, sondern sogleich eine ganze Serie aufeinanderfolgender Bits betreffen (z. B. elektrische Interferenz, Staub auf CD-Platten). Schließlich beachte man dabei noch die ziemlich hohe Informationsrate R des beschriebenen Reed-Solomon-Codes:

$$R = \frac{8 \cdot 223}{8 \cdot 255} = 0{,}87\ldots$$

Automorphismengruppe und Gitter zu einem Code

Zwei binäre Codes sind – zumindest theoretisch – gleichberechtigt, falls sie durch Vertauschung (Permutation) der Stellen in den Codewörtern auseinander hervorgehen (vgl. Abb. 3a). Als Automorphismengruppe eines Codes C bezeichnet man diejenigen Permutationen, die den Code als ganzen (nicht notwendig wortweise) invariant lassen. Besteht der Code C aus Wörtern der Länge n (also C Teilmenge von $(\mathbb{F}_2)^n$), so ist die Anzahl der im obigen Sinn zu C gleichberechtigten Codes (äquivalenten Codes) gleich der Anzahl aller möglichen Permutationen der Stellen eines Wortes der Länge n geteilt durch die Ordnung (Anzahl der Elemente) der Automorphismengruppe von C; als Formel: $\frac{n!}{|\mathrm{Aut}(C)|}$.

Betrachten wir den Hamming-Code (Abb. 1), so sehen wir, daß er genau sieben Codewörter vom Gewicht 3 (d. h. mit genau drei Einsen) enthält. Schreibt man diese sieben Codewörter untereinander, so erhält man die Inzidenzmatrix der projektiven Ebene über $\mathbb{F}_2$ (vgl. Abb. 4). Daher kann man die Automorphismengruppe des Hamming-Codes interpretieren als die Gruppe der Kollineationen

C_1	C_1'
000	000
100	001
010	010
110	011

a)

$p_1(abc) = abc$
$p_2(abc) = bac$
$p_3(abc) = cba$
$p_4(abc) = acb$
$p_5(abc) = cab$
$p_6(abc) = bca$

b)

$p_3(p_4(abc)) = p_3(acb) = bca = p_6(abc)$

$p_3 \cdot p_4 = p_6$

c)

Code	000 011 101 110	000 100 010 110	000 111 100 011
Ordnung der Automorphismengruppe	6	2	2
Anzahl der äquivalenten Codes	1	3	3

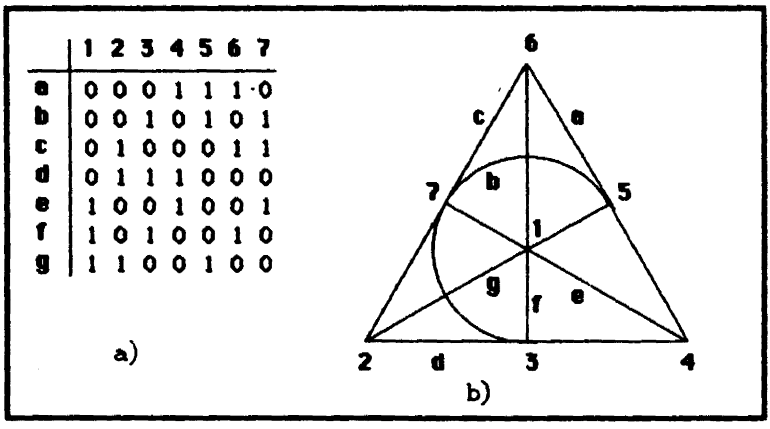
d)

Abb. 3: a) zeigt zwei äquivalente Codes, die durch Vertauschung der 1-ten mit der 3-ten Stelle der Codewörter auseinander hervorgehen. Es gibt genau 6 verschiedene Permutationen der Stellen eines Wortes der Länge 3 (Abb. b)). Das Produkt $p' \cdot p$ zweier Permutationen p' und p ist diejenige Permutation, die man durch Hintereinanderausführen von p und p' erhält (Abb. c)). Es gibt genau sieben binäre lineare 4-Wörter-Codes mit Wortlänge 3. Diese zerfallen in drei Klassen von je 1 bzw. 3 einander äquivalenten Codes (Abb. d)). Der „symmetrischste" ist offenbar der erste (an jedes 2-Bit-Wort wird eine Kontrollziffer 0 oder 1 so angefügt, daß die Anzahl der 1-en gerade wird).

dieser projektiven Ebene (d. h. als die Gruppe derjenigen Permutationen der 7 Punkte dieser projektiven Geometrie, die Geraden in Geraden überführen). Diese Gruppe – sie wird mit $GL_3(\mathbb{F}_2)$ bezeichnet – ist eine berühmte einfache Gruppe der Ordnung 168.

Ein weiteres interessantes Objekt, welches man einem linearen Code zuordnen kann, ist ein Gitter.

Betrachten wir dazu den erweiterten Hamming-Code C in $(\mathbb{F}_2)^8$, den man aus dem Hamming-Code der Abb. 1 dadurch erhält, daß man an jedes Codewort eine weitere Kontrollziffer 0 oder 1 so anfügt, daß die Gesamtzahl der 1-en im neuentstandenen Wort stets gerade ist: aus dem Codewort 1100100 des Hamming-Codes wird also das Codewort 11001001 des erweiterten Hamming-Codes etc. Dieser erweiterte Hamming-Code C hat zwei bemerkenswerte Eigenschaften: In jedem Codewort ist die Anzahl der 1-en durch 4 teilbar (man sagt: „der Code ist doppelt gerade"); ferner sind die Wörter $b_1b_2 \ldots b_8$ in $(\mathbb{F}_2)^8$, die $b_1a_1 + b_2a_2 + \ldots b_8a_8 \equiv 0 \bmod 2$ für alle $a_1a_2 \ldots a_8$ in C erfüllen, genau die Codewörter in C (man sagt: „der Code ist selbstdual").



	1	2	3	4	5	6	7
a	0	0	0	1	1	1	0
b	0	0	1	0	1	0	1
c	0	1	0	0	0	1	1
d	0	1	1	1	0	0	0
e	1	0	0	1	0	0	1
f	1	0	1	0	0	1	0
g	1	1	0	0	1	0	0

Abb. 4: b) zeigt die projektive Ebene über $\mathbb{F}_2$: sieben Punkte $(1, 2, \ldots, 7)$, sieben Geraden $(a, b, \ldots, g)$; jede Gerade enthält genau drei Punkte, jeder Punkt liegt auf genau drei Geraden. a) zeigt die Inzidenzmatrix dieser projektiven Geometrie: der Schnittpunkt der Zeile b und der Reihe 2 ist 0, weil die Gerade b den Punkt 2 nicht enthält; der Schnittpunkt von Zeile f mit Reihe 6 ist 1, weil die Gerade f den Punkt 6 enthält etc. Die Zeilen der Inzidenzmatrix sind genau die sieben Codewörter mit Gewicht 3 im Hamming-Code (vgl. Abb. 1).

Im 8-dimensionalen Raum $\mathbb{R}^8$ hat man das „Rechenkästchen-Gitter" $\frac{1}{\sqrt{2}}\mathbb{Z}^8$, d. h. alle Vektoren $\left(\frac{x_1}{\sqrt{2}}, \frac{x_2}{\sqrt{2}}, \ldots, \frac{x_8}{\sqrt{2}}\right)$, wo die $x_1, x_2, \ldots, x_8$ ganze Zahlen sind ($\sqrt{2}$ ist hier lediglich eine Normierung, um verschiedene Formeln einfacher schreiben zu können, und hat keine weitergehende Bedeutung). Dem erweiterten Hamming-Code C entspricht nun ein interessantes Teilgitter Γ von $\frac{1}{\sqrt{2}}\mathbb{Z}^8$: Das Gitter Γ besteht aus allen Vektoren $\left(\frac{x_1}{\sqrt{2}}, \ldots, \frac{x_8}{\sqrt{2}}\right)$ aus $\frac{1}{\sqrt{2}}\mathbb{Z}^8$, so daß die Reduktion modulo 2 von $(x_1, \ldots, x_8)$ in C liegt (letzteres bedeutet: ist ε_i der Rest von x_i bei Division durch 2, so soll $\varepsilon_1\varepsilon_2\ldots\varepsilon_8$ ein Codewort in C sein).

Die beiden oben erwähnten Eigenschaften des erweiterten Hamming-Codes übertragen sich auf das Gitter Γ: Die Zahl $x_1^2 + x_2^2 + \ldots + x_8^2$ – d. h. das Längenquadrat – eines Vektors $(x_1, \ldots, x_8)$ aus Γ ist stets eine gerade ganze Zahl (man sagt: „Das Gitter Γ ist gerade"). Ferner ist Γ unimodular, d. h. die Vektoren $(y_1, \ldots, y_8)$ aus $\mathbb{R}^8$, für die das Skalarprodukt $x_1y_1 + x_2y_2 + \ldots + x_8y_8$ mit jedem $(x_1, \ldots, x_8)$ aus Γ ganzzahlig ist, sind genau die Vektoren in Γ. Das Gitter Γ ist das einzige 8-dimensionale Gitter mit diesen beiden Eigenschaften, und es wird üblicherweise mit E_8 bezeichnet.

Die Ausdrucksweise „einziges Gitter" ist hierbei natürlich in einem etwas abstrakteren Sinne zu verstehen: zwei Gitter, die durch eine Drehung des 8-dimensionalen euklidischen Raums auseinander hervorgehen, werden als gleich angesehen; der Mathematiker sagt: Sie sind „isomorph". So kann man das Gitter E_8 – genauer: ein zu obigem Γ isomorphes Gitter – auch folgendermaßen erhalten: Wir identifizieren den 8-dimensionalen euklidischen Raum mit den Vektoren $(x_1, x_2, \ldots, x_9)$ im Minkowski-Raum $\mathbb{R}^{8,1}$, die auf dem Vektor $(1, 1, 1, 1, 1, 1, 1, 1, -3)$ (mit Längenquadrat $1^2 + 1^2 + \ldots + 1^2 - (-3)^2 = -1$) senkrecht stehen, d. h. $x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7 + x_8 - 3x_9 = 0$ erfüllen. Das Längenquadrat eines Vektors $(x_1, x_2, \ldots, x_9)$ in diesem Modell des 8-dimensionalen euklidischen Raums ist dabei natürlich durch $x_1^2 + x_2^2 + x_3^2 + \ldots + x_8^2 - x_9^2$ gegeben. Ein weiteres Modell für E_8 erhält man nun in Form aller Vektoren $(x_1, x_2, \ldots, x_9)$, wo die x_i ganze Zahlen sind (und natürlich $x_1 + x_2 + \ldots + x_8 - 3x_9 = 0$ erfüllen).

Das Gitter E_8 hat 240 Vektoren minimaler Länge. Dies liest man am besten am Gitter Γ aus entsprechenden Eigenschaften des erweiterten Hamming-Codes ab. Die kürzeste Länge eines von $(0, \ldots, 0)$ verschiedenen Vektors in Γ ist $\sqrt{2}$: Jeder von $(0, \ldots, 0)$ verschiedene Vektor in Γ hat mindestens 4 von 0 verschiedene Koordinaten oder aber seine Koordinaten sind ganzzahlige Vielfache von $\sqrt{2}$, denn jedes von $0 \ldots 0$ verschiedene Codewort hat mindestens Gewicht 4. Die Anzahl der Vektoren der Länge $\sqrt{2}$ ist

$$\left[\begin{array}{c}\text{14 Wörter im erweiterten Hamming-Code vom Gewicht 4}\end{array}\right] \times (2^4 \text{ Vorzeichen}) +$$

$$+ (1 \text{ Wort } 0 \ldots 0) \times \left[\begin{array}{c}\text{8 Möglichkeiten, eine 2 auf 8 Stellen zu verteilen}\end{array}\right] \times (2 \text{ Vorzeichen}) = 240 .$$

Um der Anschauung bei der Diskussion von Gittern etwas näher zu kommen, betrachten wir eine Serie sehr einfacher Codes: C_n sei der Code in $(\mathbb{F}_2)^n$, der aus allen Wörtern mit einer geraden Anzahl von 1-en besteht. Zum Beispiel

$$C_1 : 0 \qquad C_2 : \begin{matrix} 0\,0 \\ 1\,1 \end{matrix} \qquad C_3 : \begin{matrix} 0\,0\,0 \\ 0\,1\,1 \\ 1\,0\,1 \\ 1\,1\,0 \end{matrix} .$$

Dies sind offenbar lineare Codes. Die zugehörigen Gitter bezeichnen wir mit D_n. Es ist also D_n die Gesamtheit aller Vektoren $\left(\frac{x_1}{\sqrt{2}}, \ldots, \frac{x_n}{\sqrt{2}}\right)$ in $\frac{1}{\sqrt{2}}\,\mathbb{Z}^n$, so daß $x_1 + x_2 + \ldots + x_n$ gerade ist (vgl. Abb. 5).

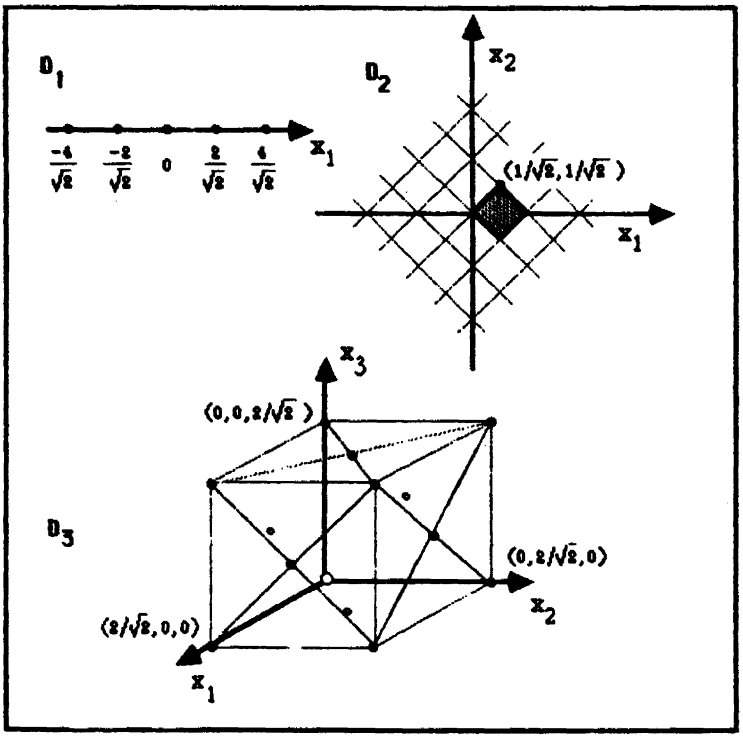


Abb. 5: Die Gitter D_1, D_2 und D_3. Ein Bereich wie der schraffierte im Bild von D_2 heißt Fundamentalmasche. Füllt man den 3-dimensionalen Raum mit Würfeln der Kantenlänge $\sqrt{2}$ aus, beginnend mit dem im Bild dargestellten, so bilden die Eckpunkte und Oberflächenmittelpunkte dieser Würfel gerade das Gitter D_3. Dieses Gitter heißt deshalb auch das „flächenzentrierte kubische Gitter". Die Eckpunkte eines Würfels entsprechen dem Codewort 000, die Flächenmittelpunkte den drei übrigen Codewörtern von C_3.

Das Gitter D_3 besitzt genau 12 Vektoren minimaler Länge 1:
(3 Wörter in C_3 vom Gewicht 2) × (2^2 Vorzeichen) = 12.

Denken wir uns um jeden Gitterpunkt in D_3 eine Kugel vom Radius ½ gelegt, so erhalten wir eine Kugelpackung des 3-dimensionalen euklidischen Raums; dabei wird jede Kugel von genau 12 anderen berührt (vgl. Abb. 6).

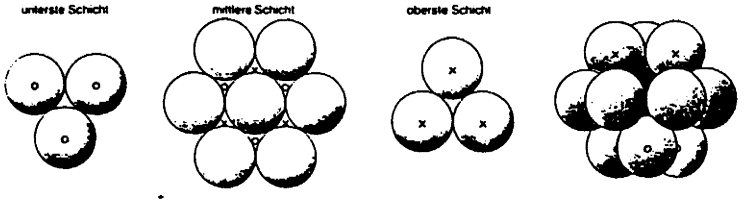


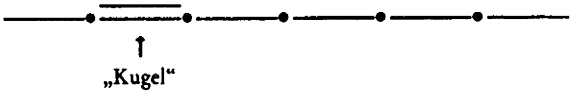
Abb. 6: Bei der zu D_3 gehörenden Kugelpackung wird jede Kugel von genau zwölf anderen berührt.

Kußzahl und Dichte

Bemerkenswert ist hier, daß 12 überhaupt die maximale Anzahl von Kugeln gleicher Größe ist, die eine weitere Kugel gleicher Größe berühren können. Dieses „Kontaktzahl-" oder „Kußzahl-Problem" ist sehr alt und führte zu einem Disput zwischen ISAAC NEWTON („12 ist die maximale Zahl") und dem Astronomen DAVID GREGORY (er bezweifelte es) im Jahre 1694. Daß NEWTON recht hatte, wurde von R. HOPPE (1874), G. BENDER (1874) und S. GÜNTHER (1875) bewiesen.

Es ist ein ungelöstes Problem, die maximale Kontaktzahl τ_n in n Dimensionen zu bestimmen, d. h. die maximale Anzahl τ_n von Kugeln gleicher Größe im n-dimensionalen Raum $\mathbb{R}^n$, die an eine weitere Kugel gleicher Größe angelegt werden können. (Die „Kugel" in $\mathbb{R}^n$ im Mittelpunkt $(a_1, a_2, \ldots, a_n)$ und Radius r ist die Gesamtheit aller $(x_1, \ldots, x_n)$, so daß $(x_1 - a_1)^2 + (x_2 - a_2)^2 + \ldots + (x_n - a_n)^2 \leqq r^2$ gilt.)

Es ist offensichtlich $\tau_1 = 2$:



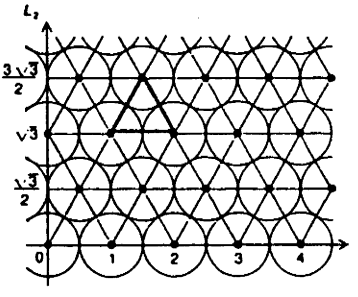
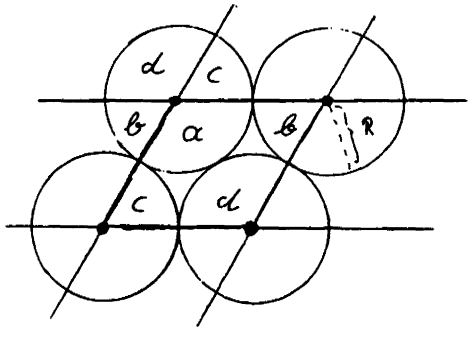


Abb. 7: Das Gitter A_2, auch das „hexagonale Gitter" genannt.

Etwas weniger offensichtlich, aber durch etwas Nachdenken leicht einzusehen, ist $\tau_2 = 6$. Diese Kußzahl wird wieder realisiert bei einer Kugelpackung, die von einem Gitter herrührt, dem Gitter A_2 (vgl. Abb. 7). Wie eben erwähnt, weiß man $\tau_3 = 12$. Außerdem weiß man noch $\tau_8 = 240$ und $\tau_{24} = 196\,560$ (A. M. Odlyzko, N. J. A. Sloane 1979 und V. I. Levenshtein 1979). Auch diese beiden Kußzahlen können durch Gitter realisiert werden: Im Fall der Dimension $n = 8$ durch das oben beschriebene, aus dem erweiterten Hamming-Code gewonnene Gitter E_8: wie wir gesehen haben, gibt es 240 Vektoren minimaler Länge $\sqrt{2}$ im Gitter E_8; legt man um jeden Gitterpunkt eine Kugel vom Radius $\frac{\sqrt{2}}{2}$, so erhält man eine Kugelpackung, wo jede Kugel von genau 240 anderen berührt wird. Im Fall der Dimension $n = 24$ wird die maximale Kußzahl beim Leech-Gitter erreicht, auf das wir später noch eingehen werden. Für $n \neq 1, 2, 3, 8, 24$ ist τ_n bis heute noch unbekannt.

Verwandt mit dem Kontaktzahlproblem ist das Problem der dichtesten Kugelpackung: Der n-dimensionale Raum $\mathbb{R}^n$ ist möglichst dicht mit Kugeln gleicher Größe aufzufüllen. Eine vernünftige Restriktion ist, zunächst nur Gitterpackungen zu betrachten: Als Kugelmittelpunkte wählen wir die Punkte eines Gitters, als Radius der Kugeln die Zahl $R = \frac{1}{2} \times$ (Länge des kleinsten von $(0, \ldots, 0)$ verschiedenen Gittervektors). Die Dichte einer Gitterpackung erfaßt man quantitativ durch den Anteil der Fundamentalmasche eines Gitters, der von Kugelteilen überdeckt wird (vgl. Abb. 8).

Abb. 8: Die Dichte δ einer Gitterpackung kann durch folgende Formel berechnet werden:
$$\delta = \frac{\text{Volumen einer Kugel vom Radius R}}{\text{Volumen einer Fundamentalmasche}}$$



n	Name des Gitters	Dichte der Gitterpackung	Anzahl der Vektoren kürzester Länge
1	D_1	$2 \cdot \frac{1}{2} = 1.0000$	2
2	A_2	$\pi \cdot \frac{1}{2\sqrt{3}} = 0.9068$	6
3	D_3	$\frac{4\pi}{3} \cdot \frac{1}{4\sqrt{2}} = 0.7404$	12
4	D_4	$\frac{\pi^2}{2} \cdot \frac{1}{8} = 0.6168$	24
5	D_5	$\frac{8\pi^2}{15} \cdot \frac{1}{8\sqrt{2}} = 0.4652$	40
6	E_6	$\frac{\pi^3}{6} \cdot \frac{1}{8\sqrt{3}} = 0.3729$	72
7	E_7	$\frac{16\pi^3}{105} \cdot \frac{1}{16} = 0.2952$	126
8	E_8	$\frac{\pi^4}{24} \cdot \frac{1}{16} = 0.2536$	240

Abb. 9: In den Dimensionen n = 1 bis n = 8 sind die dichtesten Gitterpackungen bekannt.

Im Fall der Dimension n = 1 führt offenbar jedes Gitter zu einer optimalen Gitterpackung mit Dichte 1. Das Gitter D_2 hat die Dichte $\pi \left(\frac{1}{2}\right)^2 = 0{,}78\ldots$ (vgl. Abb. 5). Eine dichtere Packung hat man beim Gitter A_2 (vgl. Abb. 7); die Dichte ist hier $\frac{\pi \left(\frac{1}{2}\right)^2}{\sqrt{3/4}} = 0{,}90\ldots$ Es ist nicht sehr schwer einzusehen, daß dies die dichteste Gitterpackung in zwei Dimensionen ist. In Dimension 3 ist D_3 die dichteste Gitterpackung (C. F. Gauss 1831); in Dimension 4, 5 sind es D_4, D_5 (A. Korkine, G. Zolotareff 1872 und 1877); in Dimension 6, 7, 8 sind es E_6, E_7, E_8 (H. F. Blichfeldt 1934). Die Gitter E_6, E_7 sind gewisse „Schnitte" im Gitter E_8. In den höheren Dimensionen ist das Problem, die dichteste Gitterpackung zu bestimmen, bis heute noch ungelöst.

Codes, Thetareihen und Modulformen

Gitter stehen in engem Zusammenhang mit Fragen der Zahlentheorie. Denken wir uns ein Gitter Γ im n-dimensionalen Raum gegeben, von dem wir annehmen, daß die Längenquadrate der Gittervektoren ganzzahlige Vielfache einer reellen Zahl R sind, wie es bei allen bisher betrachteten Gittern der Fall ist. Als Länge

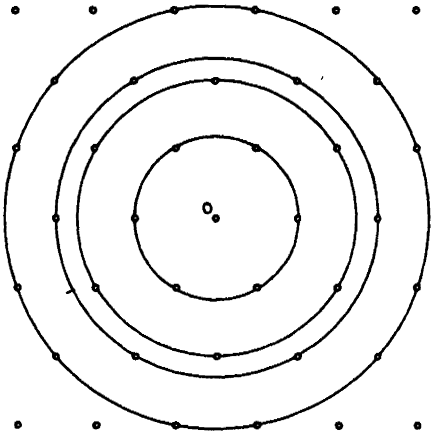


Abb. 10: Beim Gitter A_2 enthalten die ersten fünf Kugeln (Kreise), auf denen Gitterpunkte zu finden sind, jeweils 1, 6, 6, 6 bzw. 12 Punkte.

eines Gittervektors kommen also die Zahlen 0, $\sqrt{R}$, $\sqrt{2R}$, $\sqrt{3R}$, ... in Frage; etwas anschaulicher ausgedrückt: Die Gittervektoren sind auf den Kugeln vom Radius 0, $\sqrt{R}$, $\sqrt{2R}$, $\sqrt{3R}$, ... zu finden.

Wie viele Gitterpunkte liegen auf der Kugel vom Radius $\sqrt{R \cdot m}$ für eine beliebig vorgegebene natürliche Zahl m?

Seiner Natur nach ist dies ein Problem der Zahlentheorie, genauer: ein diophantisches Problem. Wollte man dies Problem etwa für die Gitter D_2 oder A_2 formelmäßig formulieren, so würde man zu der folgenden Frage geführt: Wie viele Paare (x, y) ganzer Zahlen gibt es, so daß $x^2 + y^2 = m$ (für D_2) bzw. $x^2 + xy + y^2 = m$ (für A_2) gilt?

Es bezeichne N_m die Anzahl der Gitterpunkte von Γ, die auf der Kugel von Radius $\sqrt{m \cdot R}$ liegen. Der methodisch erfolgreichste Weg in der Mathematik, um Aussagen über die Zahlen N_m zu erhalten, ist, alle diese Zahlen zu einem einzigen Objekt zusammenzufassen, der „Thetareihe zum Gitter Γ":

$$\theta_\Gamma = 1 + N_1 q + N_2 q^2 + \ldots = \sum_{m=0}^{\infty} N_m q^m .$$

Man kann sich hier zunächst q als eine Unbestimmte und θ_Γ als ein unendliches Polynom vorstellen.

Bedeutungsvoll wird diese Schreibweise, wenn man $q = e^{2\pi i z}$ setzt. Dann wird $\theta_\Gamma = \theta_\Gamma(z)$ eine Funktion in der Variablen z, wobei für z jede komplexe Zahl mit positivem Imaginärteil eingesetzt werden darf.

Die Thetafunktion gehört nun einer sehr distinguierten Klasse von Funktionen an, den sogenannten „Modulformen". Im einfachsten Fall ist eine Modulform eine Funktion der Gestalt $f(z) = a_0 + a_1q + a_2q^2 + \ldots$, die unendlich vielen Funktionalgleichungen genügt: $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$, wobei die a, b, c, d beliebige ganze Zahlen mit $ad - bc = 1$ sein dürfen, und wobei k eine fest vorgegebene natürliche Zahl ist; genauer heißen die eben beschriebenen Funktionen „Modulformen auf der vollen Modulgruppe mit Gewicht k". Allgemeinere Modulformen erhält man, indem man die Zahlen a, b, c, d noch gewissen weiteren Restriktionen unterwirft und für k beliebige Zahlen zuläßt. Identifiziert man je zwei komplexe Zahlen (mit positivem Imaginärteil), falls sie durch eine Substitution $z \to \frac{az+b}{cz+d}$ (a, b, c, d ganze Zahlen, $ad - bc = 1$ und eventuell weitere Restriktionen) auseinander hervorgehen, so erhält man ein geometrisches Objekt, eine „Modulkurve". Im einfachsten Fall ist dieses geometrische Objekt die komplexe projektive Gerade oder Riemannsche Zahlenkugel, aus der man einen Punkt herausgenommen hat. Das Studium der Modulkurven führt zu Aussagen über Modulformen. (Wieder) im einfachsten Fall erhält man zum Beispiel die Aussage, daß jede Modulform auf der vollen Modulgruppe mit Gewicht k für durch 4 teilbares k von der Gestalt $c_0E_4^{k/4} + c_1E_4^{k/4-3}\Delta + c_2E_4^{k/4-6}\Delta^2 + \ldots = \sum c_iE_4^{k/4-3i}\Delta^i$ sein muß. Hierbei sind die $c_0, c_1, c_2, \ldots$ beliebige komplexe Zahlen; die Summe ist über die endlich vielen natürlichen Zahlen zu erstrecken, für die $k/4-3i$ nicht-negativ ist. Die Symbole E_4, Δ bezeichnen zwei sehr grundlegende Modulformen:

$$E_4 = 1+240(q+9q^2+28q^3+\ldots) = 1+240\sum_{m=1}^{\infty}\sigma_3(m)q^m$$

($\sigma_3(m)$ = Summe der dritten Potenzen der Teiler von m) und

$$\Delta = q(1-q)^{24}(1-q^2)^{24}\cdot\ldots = q\prod_{m=1}^{\infty}(1-q^m)^{24}$$

$$= q-24q^2+252q^3-1472q^4\pm\ldots$$

Um nun zu den Thetareihen zurückzukehren, nehmen wir an, daß Γ gerade und unimodular ist (vgl. den vorletzten Abschnitt). Dann ist $\theta_\Gamma(z)$ eine Modulform auf der vollen Modulgruppe mit Gewicht $\frac{n}{2}$ (man weiß, daß unimodulare, gerade Gitter nur für durch 8 teilbare Dimensionen n existieren). Ist etwa $\Gamma = E_8$, so muß also nach dem eben über Modulformen gesagten die Thetafunktion θ_Γ mit E_4 identisch sein. Also gilt für das Gitter $\Gamma = E_8$ die Formel $N_m = 240\sigma_3(m)$. Analoge Argumentationen kann man auch für beliebige Gitter durchführen, um die Zahlen N_m zu bestimmen (vgl. Abb. 11).

THE HEXAGONAL LATTICE A_2 IN R^2

m	$\frac{1}{6}N_m$	m	$\frac{1}{6}N_m$	m	$\frac{1}{6}N_m$
0	1/6	64	1	147	3
1	1	67	2	148	2
3	1	73	2	151	2
4	1	75	1	156	2
7	2	76	2	157	2
9	1	79	2	163	2
12	1	81	1	169	3
13	2	84	2	171	2
16	1	91	4	172	2
19	2	93	2	175	2
21	2	97	2	181	2
25	1	100	1	183	2
27	1	103	2	189	2
28	2	108	1	192	1
31	2	109	2	193	2
36	1	111	2	196	3
37	2	112	2	199	2
39	2	117	2	201	2
43	2	121	1	208	2
48	1	124	2	211	2
49	3	127	2	217	4
52	2	129	2	219	2
57	2	133	4	223	2
61	2	139	2	225	1
63	2	144	1	228	2

THE FACE-CENTERED CUBIC LATTICE D_3 IN R^3 (THE TABLE GIVES $\frac{1}{6}N_m$ FOR $m = 10r + s$)

r/s	0	1	2	3	4	5	6	7	8	9
0	1/6	2	1	4	2	4	4/3	8	1	6
1	4	4	4	12	8	8	2	8	5	12
2	4	8	4	8	4/3	14	4	16	8	4
3	0	16	1	16	8	8	6	20	4	8
4	4	8	8	20	4	20	0	16	4	18
5	5	8	12	12	16/3	24	0	16	12	12
6	8	20	0	24	2	8	8	28	8	16
7	8	8	5	32	4	20	12	16	0	16
8	4	18	16	20	8	24	4	24	4	16
9	12	24	8	24	0	8	4/3	40	9	20

THE LATTICE D_4 IN R^4

m	$(24)^{-1}N_m$	m	$(24)^{-1}N_m$
1	1	26	14
2	1	27	40
3	4	28	8
4	1	29	30
5	6	30	24
6	4	31	32
7	8	32	1
8	1	33	48
9	13	34	18
10	6	35	48
11	12	36	13
12	4	37	38
13	14	38	20
14	8	39	56
15	24	40	6
16	1	41	42
17	18	42	32
18	13	43	44
19	30	44	12
20	6	45	78
21	32	46	24
22	12	47	48
23	24	48	4
24	4	49	57
25	31	50	31

The lattice D_5 in R^5

m	N_m	m	N_m
1	40	26	3760
2	90	27	6720
3	240	28	4000
4	200	29	7920
5	560	30	4800
6	400	31	6720
7	800	32	5850
8	730	33	8960
9	1240	34	4320
10	752	35	10720
11	1840	36	6200
12	1200	37	9840
13	2000	38	7600
14	1600	39	11040
15	2720	40	5872
16	1680	41	12960
17	3680	42	7520
18	2250	43	12400
19	3280	44	9200
20	2800	45	14000
21	4320	46	8000
22	2800	47	16960
23	5920	48	8880
24	2960	49	13480
25	5240	50	10890

THE LATTICES E_6, E_7, AND E_8 IN R^6, R^7, AND R^8

m	$N_m(E_6)$	$N_m(E_7)$	$(240)^{-1}N_m(E_8)$
1	72	126	1
2	270	756	9
3	720	3024	28
4	936	4158	73
5	2160	7560	126
6	3214	11592	252
7	5040	16704	344
8	6570	24948	585
9	9552	31878	757
10	13104	39816	1134
11	18000	55944	1332
12	9360	66584	2044
13	12240	76104	2198
14	13500	99792	3096
15	17712	116928	3528
16	14760	133182	4681
17	25920	160272	4914
18	19710	177660	6813
19	26064	205128	6860
20	28080	249480	9198
21	36000	265104	9632
22	25920	281736	11988
23	47520	350784	12168
24	37638	382536	16380
25	43272	399726	15751

Abb. 11: Die ersten Zahlen N_m für die optimalen Gitter A_2, D_3, D_4, D_5, E_6, E_7 und E_8. Die Teilbarkeitseigenschaften der Zahlen N_m kommen dadurch zustande, daß die Gitter jeweils bei bestimmten Drehungen des jeweiligen euklidischen Raums in sich überführt werden. So ist zum Beispiel A_2 invariant unter den 6 Drehungen um 60°, 120°, 180°, 240°, 300°, 360° (vgl. Abb. 7). Demnach muß die Anzahl der Gitterpunkte auf jeder Kugel durch 6 teilbar sein.

Um schließlich wieder zu den Codes zurückzukommen, erinnern wir uns, daß jedem (binären linearen) Code ein Gitter und – wie wir eben sahen – einem Gitter eine Thetafunktion, d. h. eine Modulform, entspricht. Noch unmittelbarer wird dieser Zusammenhang, führt man das sogenannte Gewichtszählerpolynom eines Codes ein.

Sei dazu C ein linearer Code in $(\mathbb{F}_2)^n$. Mit A_i bezeichnen wir die Anzahl der Codewörter mit genau i Einsen. Die Zahlen $A_0, A_1, \ldots, A_n$ fassen wir zum Gewichtszählerpolynom in zwei Unbestimmten X, Y zusammen:

$$W_C(X, Y) = A_0X^n + A_1X^{n-1}Y + \ldots + A_{n-1}XY^{n-1} + A_nY^n = \sum_{i=0}^{n} A_iX^{n-1}Y^i .$$

Für den erweiterten Hamming-Code – wir bezeichnen ihn mit $\tilde{H}$ – ist zum Beispiel (vgl. auch Abb. 1):

$$W_{\tilde{H}}(X, Y) = X^8 + 14X^4Y^4 + Y^8 .$$

Unten werden wir einen weiteren doppelt-geraden, selbstdualen Code kennen lernen, den erweiterten Golay-Code $\tilde{G}$; sein Gewichtszählerpolynom ist

$$W_{\tilde{G}}(X, Y) = X^{24} + 759X^{16}Y^8 + 2576X^{12}Y^{12} + 759X^8Y^{16} + Y^{24} .$$

Dem Code C entspricht ein Gitter Γ, diesem die Thetareihe θ_Γ, und dieser Zusammenhang drückt sich in der folgenden Formel aus:

$$W_C(\theta_0, \theta_1) = \theta_\Gamma .$$

Hierbei sind θ_0 und θ_1 zwei universelle Thetareihen:

$$\theta_0 = 1 + 2(q + q^4 + q^9 + \ldots) = 1 + 2\sum_{m=1}^{\infty} q^{m^2} \quad \text{und}$$

$$\theta_1 = 2(q^{1/4} + q^{9/4} + q^{25/4} + \ldots) = 2\sum_{m=0}^{\infty} q^{(2m+1)^2/4} .$$

Vermöge dieser Formel kann man Aussagen über Modulformen in Aussagen über Codes übersetzen. Ist zum Beispiel C doppelt-gerade, selbstdual, so ist Γ gerade und unimodular, und dann ist θ_Γ eine Modulform auf der vollen Modulgruppe vom Gewicht n/2 (und n/2 ist durch 4 teilbar). Die oben gegebene Beschreibung dieser Modulformen übersetzt sich dann in die Aussage, daß sich das Gewichtszählerpolynom eines doppelt-geraden, selbstdualen Codes stets in der folgenden Gestalt schreiben läßt:

$$W_C(X, Y) = C_0W_{\tilde{H}}^{n/8} + C_1W_{\tilde{H}}^{n/8-3}W_{\tilde{G}} + C_2W_{\tilde{H}}^{n/8-6}W_{\tilde{G}}^2 + \ldots = \sum C_iW_{\tilde{H}}^{n/8-3i}W_{\tilde{G}}^i$$

mit geeigneten Zahlen $C_0, C_1, C_2, \ldots$, und die Summe ist über alle i zu erstrecken, so daß $n/8 - 3i$ nicht-negativ ist.

Solche Aussagen sind für den Codierungstheoretiker natürlich interessant. Zum Beispiel kann man mittels der eben formulierten Aussage einsehen, daß der Minimalabstand eines doppelt-geraden selbstdualen Codes der Länge n höch-

stens $4\left[\frac{n}{24}\right]+4$ sein kann ($\left[\frac{n}{24}\right]$ = größte natürliche Zahl, die nicht größer als $\frac{n}{24}$ ist), und daß es überdies nur endlich viele doppelt-gerade, selbstduale Codes gibt, die diese oberen Schranken jeweils annehmen; diese heißen „extremale doppelt-gerade, selbstduale Codes". Die ersten dieser extremalen Codes erhält man für die Wortlängen $n = 8$ (erweiterter Hamming-Code, Minimalabstand 4), $n = 16$ (je zwei Codewörter des erweiterten Hamming-Codes nebeneinander geschrieben, Minimalabstand 4), $n = 24$ (erweiterter Golay-Code (vgl. unten), Minimalabstand 8).

Die hier skizzierte Theorie läßt sich auch für lineare Codes über beliebigen endlichen Körpern ansetzen. Bei ternären Codes (Codes über $\mathbb{F}_3$) bleibt man dabei noch im Bereich der oben beschriebenen Modulformen. Für beliebige Primzahlen gelangt man in natürlicher Weise von Codes über $\mathbb{F}_p$ zu Gittern über bestimmten algebraischen Zahlkörpern, und von diesen zu Thetareihen in mehreren Variablen, die sogenannte Hilbertsche Modulformen sind. Das Studium Hilbertscher Modulformen ist auf das Engste verknüpft mit dem Studium Hilbertscher Modulvarietäten. Die Hilbertschen Modulflächen sind in den letzten eineinhalb Jahrzehnten sehr intensiv studiert worden. Im Fall $p = 5$ gelangt man zu einer bestimmten Hilbertschen Modulfläche, die in „F. Hirzebruch: The ring of Hilbert modular forms for real quadratic fields of small discriminant, in Modular Functions of One Variable VI, Springer, Berlin 1977" studiert wurde. Aus den dort erzielten Ergebnissen kann man die von Gleason, Pierce und Sloane erzielte Beschreibung der Gewichtszählerpolynome selbstdualer Codes über $\mathbb{F}_5$ ableiten (G. van der Geer, F. Hirzebruch: siehe Kommentar in: F. Hirzebruch, Gesammelte Abhandlungen, Bd. II, S. 796–798, Springer-Verlag 1987).

Golay-Code und einfache Gruppen

Bei dem erweiterten Golay-Code handelt es sich um einen linearen, 12-dimensionalen Code in $(\mathbb{F}_2)^{24}$. Demnach kann man sich bei der Beschreibung des Golay-Codes darauf beschränken, 12 Basisvektoren anzugeben: Jede Summe beliebig vieler dieser 12 Basisvektoren ergibt ein Codewort, und jedes Codewort wird so erhalten. In Abb. 12 sind zwölf Basisvektoren aufgelistet.

$\tilde{G}$ ist ein doppelt-gerader, selbstdualer extremaler Code mit Minimalabstand $d = 8$; insbesondere kann er 3 Fehler korrigieren. Streicht man irgendeine Spalte in Abb. 12 (zum Beispiel die erste), so erhält man 12 Basisvektoren für den eigentlichen (binären) Golay-Code; bei diesem handelt es sich also um einen 12-dimensionalen Code in $(\mathbb{F}_2)^{23}$ mit Minimalabstand $d = 7$. Dieser äußerst effektive Code

1	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1	0
1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	0	0	1
1	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	0	0	0
1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	0	0
1	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1	0
1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	0	1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	0	1	0	0	0	0	1	1	0	0	0	1	0	1	1	0	1	1
1	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	0	0	1	0	1	1	0	1
1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	0	0	1	0	1	1	0
1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	0	0	1	0	1	1
1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1
0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1

Abb. 12: Zwölf Basisvektoren für den erweiterten Golay-Code untereinander geschrieben.

wurde von M. J. E. Golay 1949 bei der Suche nach sogenannten „perfekten Codes" entwickelt.

Der erweiterte Golay-Code enthält genau 759 Wörter mit Hamming-Gewicht 8, d. h. mit genau 8 Einsen. Wir nennen diese Wörter Oktaden. Damit folgt für $\tilde{G}$ eine bemerkenswerte Eigenschaft: Zu je fünf beliebig ausgewählten Stellen gibt es genau eine Oktade, welche an diesen Stellen eine 1 hat. Einerseits kann es nämlich keine zwei verschiedenen Oktaden W und W' geben, die an den gleichen 5 Stellen Einsen haben, denn sonst hätte das von 0 verschiedene Codewort W + W' weniger als 7 Einsen, wogegen ja $\tilde{G}$ Minimalabstand d = 8 hat. Andererseits muß es aber zu je 5 Stellen mindestens eine Oktade geben, die an diesen Stellen Einsen hat, denn

$$\begin{bmatrix}\text{Anzahl der}\\ \text{Oktaden}\end{bmatrix} \times \begin{bmatrix}\text{Anzahl der Möglich-}\\ \text{keiten 5 Einsen von}\\ \text{8 auszuwählen}\end{bmatrix} = 759 \times \frac{8\cdot 7\cdot 6\cdot 5\cdot 4}{5\cdot 4\cdot 3\cdot 2} =$$

$$= \frac{24\cdot 23\cdot 22\cdot 21\cdot 20}{5\cdot 4\cdot 3\cdot 2} = \begin{bmatrix}\text{Anzahl der Möglich-}\\ \text{keiten 5 Stellen aus}\\ \text{24 auszuwählen}\end{bmatrix}$$

Diese bemerkenswerte Eigenschaft des Codes $\tilde{G}$ ist die Lösung eines 1937 von E. Witt untersuchten Problems: „Aus 24 Personen sollen 759 Vereine gebildet werden. Jeder Verein soll aus 8 Mitgliedern bestehen. Fünf beliebige Personen sollen jeweils einem einzigen Verein angehören." Etwas weniger anschaulich ausgedrückt, sollen aus einer 24-elementigen Menge 8-elementige Teilmengen derart ausgewählt werden, daß jede 5-elementige Teilmenge in genau einer dieser 8-elementigen enthalten ist. Eine solche Kollektion von 8-elementigen Teilmengen nennt man „Steinersystem S(5, 8, 24)". Witt zeigte – worauf es ihm eigentlich ankam –, daß die Automorphismengruppe dieses Steinersystems die Mathieu-

Gruppe M_{24} ist (als Automorphismus bezeichnet man hier jede Vertauschung der 24 Elemente, die jede Menge des Steinersystems wieder in eine solche überführt).

Diese Gruppe M_{24} ist eine sogenannte sporadische einfache Gruppe, d. h. eine einfache endliche Gruppe, die sich in keine der bekannten Serien von einfachen endlichen Gruppen einordnen läßt. Was eine einfache Gruppe ist (nämlich „Eine Gruppe ohne nicht-triviale Normalteiler"), wollen wir hier nicht weiter erklären. Ein gewisses Bild erhält man, wenn man sich die einfachen endlichen Gruppen als Grundbausteine für die Gesamtheit aller endlichen Gruppen vorstellt. Daher ist es eine wichtige Aufgabe, sämtliche einfachen Gruppen zu klassifizieren. Zur Zeit dieser Arbeiten von Witt waren neben gewissen Serien einfacher Gruppen nur fünf weitere bekannt: die Mathieu-Gruppen $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$. Die Gruppe M_{24} ist die größte unter ihnen: sie hat 244 823 040 Elemente.

Der erweiterte Golay-Code wird von seinen Oktaden erzeugt (jedes Codewort ist Summe von Oktaden), wie ein Blick auf Abb. 12 zeigt (man ersetzt das letzte Codewort in Abb. 12 durch die Summe des letzten und vorletzten und erhält eine Basis von $\tilde{G}$, die nur aus Oktaden besteht). Die Oktaden bilden ein Steinersystem $S(5, 8, 24)$. Die Automorphismengruppe dieses Systems ist M_{24}. Also ist auch die Automorphismengruppe von $\tilde{G}$ die Gruppe M_{24}. Erwähnenswert ist in diesem Zusammenhang noch, daß der oben erwähnte eigentliche binäre Golay-Code in $(\mathbb{F}_2)^{23}$ als Automorphismengruppe die Gruppe M_{23} hat. Neben diesen beiden binären Golay-Codes gibt es noch zwei weitere nach Golay benannte Codes. Diese sind ternäre Codes, genauer 6-dimensionale Unterräume in $(\mathbb{F}_3)^{11}$ bzw. $(\mathbb{F}_3)^{12}$. Ihre Automorphismengruppen sind M_{11} und M_{12} respektive.

Das zum erweiterten Golay-Code gehörende Gitter Γ hat eine Automorphismengruppe der Ordnung $2^{24} \times |\ M_{24}|$ (als Automorphismus eines Gitters bezeichnet man jede Drehung des zugrunde liegenden euklidischen Raums, die das Gitter in sich überführt). Mittels dieses Gitters konstruierte J. Leech 1964 ein sehr wichtiges Gitter, das nach ihm benannte Leech-Gitter: seine Gitterpunkte sind die Punkte von Γ' und die Punkte $\left(\frac{-3}{2^{3/2}}, \frac{1}{2^{3/2}}, \frac{1}{2^{3/2}}, \ldots, \frac{1}{2^{3/2}}\right) + \Gamma'$ (die um den Vektor $\left(\frac{-3}{2^{3/2}}, \frac{1}{2^{3/2}}, \frac{1}{2^{3/2}}, \ldots, \frac{1}{2^{3/2}}\right)$ verschobenen Punkte von Γ'); dabei ist Γ' das Teilgitter aller Gitterpunkte $\left(\frac{x_1}{\sqrt{2}}, \ldots, \frac{x_{24}}{\sqrt{2}}\right)$ aus Γ, für die $x_1 + x_2 + \ldots + x_{24}$ durch 4 teilbar ist. Etwas bequemer und ähnlich der oben gegebenen Beschreibung des Gitters E_8 kann man das Leech-Gitter (genauer: ein zum eben konstruierten Gitter äquivalentes Gitter) auch beschreiben als die Gesamtheit aller $(x_1, \ldots, x_{25})$ im Minkowski-Raum $\mathbb{R}^{24,1}$, wo die x_i ganze Zahlen sind und $3x_1+5x_2+7x_3+\ldots+45x_{22}+47x_{23}+51x_{24}-145x_{25}=0$ gilt (R. T. Curtis, siehe

J. H. CONWAY, N. J. A. SLOANE: Lorentzian forms for the Leech Lattice, Bull. Am. Math. Soc. 6 (1982), 215–217).

Das Leech-Gitter ist wie das zum Golay-Code gehörende Gitter Γ gerade und unimodular. Es enthält aber keine Vektoren der Länge $\sqrt{2}$. Es gibt genau 24 gerade, unimodulare Gitter (H. Niemeier 1968), aber nur eines unter ihnen enthält keine Vektoren der Länge $\sqrt{2}$, nämlich gerade das Leech-Gitter. Die zum Leech-Gitter gehörende Kugelpackung hat die Dichte $\pi^{12}/121 = 0{,}001929\ldots$; dies ist die dichteste unter allen bis heute bekannten Kugelpackungen (Gitter- oder nicht) in 24 Dimensionen. Es gibt genau 196 560 Vektoren kürzester Länge 2 im Leech-Gitter. Dies ist die maximale Kußzahl in 24 Dimensionen (ODLYZKO, SLOANE 1979). Die Anzahl N_m der Gitterpunkte auf der Kugel vom Radius $\sqrt{2m}$ berechnet man leicht mittels der im letzten Abschnitt skizzierten Theorie (vgl. Abb. 13).

Die Automorphismengruppe des Leech-Gitters hat die Ordnung 8 315 553 613 086 720 000 (J. H. CONWAY 1968). Aus dieser Automorphismengruppe heraus konstruierte Conway auf einen Schlag drei einfache Gruppen, die Gruppen $\cdot 1, \cdot 2, \cdot 3$. Dies war, nach fast 100 Jahren Ruhe auf dem Gebiet der endlichen einfachen Gruppen, ein Durchbruch. Mittlerweile ist die Liste der einfachen Gruppen vollständig. Neben bestimmten Serien gibt es genau 26 sporadische einfache Gruppen (vgl. Abb. 14). Die größte unter ihnen ist das sogenannte Fischer-Monster mit ca. 8.08×10^{53} Elementen. Beim Beweis ihrer Existenz (R. L. GRIESS, 1980) spielte das Leech-Gitter nochmals eine wichtige Rolle.

THE LEECH LATTICE IN R^{24}

m	N_m	Prime Factors of N_m
0	1	1
1	0	0
2	196560	$2^4 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13$
3	16773120	$2^{12} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$
4	398034000	$2^4 \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 13$
5	4629381120	$2^{14} \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 23$
6	34417656000	$2^6 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 17 \cdot 103$
7	187489935360	$2^{12} \cdot 3^7 \cdot 5 \cdot 7 \cdot 13 \cdot 23$
8	814879774800	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13 \cdot 17^2 \cdot 19 \cdot 151$
9	2975551488000	$2^{13} \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 13 \cdot 887$
10	9486551299680	$2^5 \cdot 3^7 \cdot 5 \cdot 7 \cdot 13 \cdot 23 \cdot 12953$
11	27052945920000	$2^{12} \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$
12	70486236999360	$2^6 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13^2 \cdot 59 \cdot 50093$
13	169931095326720	$2^{14} \cdot 3^7 \cdot 5 \cdot 7^2 \cdot 13 \cdot 1489$
14	384163586352000	$2^7 \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 23 \cdot 83 \cdot 5119$
15	820166620815360	$2^{13} \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 1097$
16	1668890090322000	$2^4 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 13 \cdot 751 \cdot 1861$
17	3249631112232960	$2^{15} \cdot 3^4 \cdot 5 \cdot 7 \cdot 13 \cdot 23 \cdot 116993$
18	6096882661243920	$2^4 \cdot 3^3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 17 \cdot 260654803$
19	11045500816896000	$2^{12} \cdot 3^8 \cdot 5^3 \cdot 7 \cdot 13 \cdot 23 \cdot 1571$
20	19428439855275360	$2^5 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 13 \cdot 23 \cdot 1747 \cdot 175709$

Abb. 13: Die Anzahl N_m der Gitterpunkte auf der Kugel vom Radius $\sqrt{2m}$ beim Leech-Gitter.

Group Notation	Discoverer(s)	Date	Order
M_{11}	Mathieu Mathieu-Cole	1861	$2^4 3^2 5 \cdot 11 = 7{,}920$
M_{12}	Mathieu Mathieu-Miller	1861	$2^6 3^3 5 \cdot 11 = 95{,}040$
M_{22}	Mathieu Mathieu-Miller	1873	$2^7 3^2 5 \cdot 7 \cdot 11 = 443{,}520$
M_{23}	Mathieu Mathieu-Miller	1873	$2^7 3^2 5 \cdot 7 \cdot 11 \cdot 23 = 10{,}200{,}960$
M_{24}	Mathieu Mathieu-Miller	1873	$2^{10} 3^3 5 \cdot 7 \cdot 11 \cdot 23 = 244{,}823{,}040$
J or Js or J_1	Janko	1965	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19 = 175{,}560$
$HaJW$ or J_2 or HaJ or J_2	Hall and Wales Hall-Janko	1967	$2^7 3^3 5^2 7 = 604{,}800$
HS	D. Higman and Sims	1967	$2^9 3^2 5^3 7 \cdot 11 = 44{,}352{,}000$
McL	Mclaughlin	1968	$2^7 3^6 5^3 7 \cdot 11 = 898{,}128{,}000$
Sz or Suz	Suzuki	1968	$2^{13} 3^7 5^2 7 \cdot 11 \cdot 13 = 448{,}345{,}497{,}600$
$HJMcK$ or J_3 or HJM or J_3	G. Higman and McKay Hall-Janko-McKay Janko-Higman and McKay	1968	$2^7 3^5 5 \cdot 17 \cdot 19 = 50{,}232{,}960$
$\cdot 1$ or Co_1	Conway Conway-Thompson	1968	$2^{21} 3^9 5^4 7^2 11 \cdot 13 \cdot 23 = 4{,}157{,}771{,}806{,}543{,}360{,}000$
$\cdot 2$ or Co_2	Conway Conway-Thompson	1968	$2^{18} 3^6 5^3 7 \cdot 11 \cdot 23 = 42{,}305{,}421{,}312{,}000$
$\cdot 3$ or Co_3	Conway Conway-Thompson	1968	$2^{10} 3^7 5^3 7 \cdot 11 \cdot 23 = 495{,}766{,}656{,}000$
He or $HHMcK$ or HHM	Held. G. Higman and McKay	1968	$2^{10} 3^3 5^2 7^3 \cdot 17 = 4{,}030{,}387{,}200$
$M(22)$ or Fi_{22} or F_{22}	Fischer	1969	$2^{17} 3^9 5^2 7 \cdot 11 \cdot 13 = 64{,}561{,}751{,}654{,}400$
$M(23)$ or Fi_{23} or F_{23}	Fischer	1969	$2^{18} 3^{13} 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23 = 4{,}089{,}470{,}473{,}293{,}004{,}800$
$M(24)'$ or Fi'_{24} or Fi_{24} or F_{24}	Fischer	1969	$2^{21} 3^{16} 5^2 7^3 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29 = 1{,}255{,}205{,}709{,}190{,}661{,}721{,}292{,}800$
Ly or $Ly5$	Lyons-Sims	1970	$2^8 3^7 5^6 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67 = 51{,}765{,}179{,}004{,}000{,}000$
R or RCW or Rud	Rudvalis-Conway-Wales Rudvalis	1972	$2^{14} 3^3 5^3 7 \cdot 13 \cdot 29 = 145{,}926{,}144{,}000$
$O'N$ or $O'NS$	O'Nan-Sims	1973	$2^9 3^4 5 \cdot 7^3 11 \cdot 19 \cdot 31 = 460{,}815{,}505{,}920$
F or FIS or B or F_1	Fischer and Leon-Sims Fischer	1973	$2^{41} 3^{13} 5^6 7^2 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47 = 4.15 \times 10^{33}$
T or F_3 or E	Thompson-Smith Fischer-Smith-Thompson	1974	$2^{15} 3^{10} 5^3 7^2 13 \cdot 19 \cdot 31 = 90{,}745{,}943{,}887{,}872{,}000$
$HaCNS$ or F_5 or F	Harada-Conway-Norton-Smith Fischer-Smith Harada-Norton and Smith	1974	$2^{14} 3^6 5^6 7 \cdot 11 \cdot 19 = 273{,}030{,}912{,}000{,}000$
M or F_1	Fischer Fischer-Griess	1974	$2^{46} 3^{20} 5^9 7^6 11^2 13^3 17 \cdot 19 \cdot 23 \cdot 29$ $\cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71 = 8.08 \times 10^{53}$
J_4	Janko Norton-Parker-Benson-Conway-Thackray	1975	$2^{21} 3^3 5 \cdot 7 \cdot 11^3 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43 = 86{,}775{,}571{,}046{,}077{,}562{,}880$

Abb. 14: Die 26 sporadischen einfachen Gruppen. Das Datum der Entdeckung ist im Allgemeinen nicht identisch mit dem Zeitpunkt des Nachweises ihrer Existenz.

Literatur

Zur Geschichte der Codierungstheorie und ihres Zusammenhangs mit Kugelpackungen und endlichen einfachen Gruppen:

T. M. Thompson: From Error-Correcting Codes through Sphere Packings to Simple Groups, The Mathematical Association of America 1983.

Mehr Informationen über Kugelpackungsprobleme und ihre Beziehungen zu nachrichtentechnischen Problemen sind zu finden in

N. J. A. Sloane: Kugelpackungen im Raum, in Spektrum der Wissenschaft, Ausgabe März 1984.

Tiefergehende Betrachtungen über alle hier erwähnten Codes findet man in der umfangreichen Monographie:

F. J. Mac Williams, N. J. A. Sloane: The Theory of Error Correcting Codes, North-Holland, Amsterdam, dritte Auflage 1981.

Quellenverzeichnis der Abbildungen

Abb. 1: New Scientist 3 July 1986, S. 38.

Abb. 2: Robert J. McEliece: The Reliability of Computer Memories, Scientific American Vol. 252 # 1 Jan. 1985, S. 72.

Abb. 6, 7: Spektrum der Wissenschaft, März 1984, S. 122–123.

Abb. 9: nach T. M. Thompson, loc. cit., S. 178.

Abb. 10, 11 (außer D_5), 13: N. J. A. Sloane: Tables of Sphere Packings and Spherical Codes, IEEE Transactions on Information Theory, vol. IT-27, No. 3, May 1981, S. 331, 332, 334, 335, 337 (Numerierung in Abb. 13 geändert).

Abb. 14: T. M. Thompson, loc. cit., S. 212–215.

Zusatz (Dezember 1987): Soeben erschien das schöne Buch von J. H. Conway und N. J. A. Sloane „Sphere Packings, Lattices and Groups", Grundlehren der mathematischen Wissenschaften 290, Springer-Verlag 1987; darin kann man sich über alle in diesem kurzen Bericht angeschnittenen Fragen und auch über die historische Entwicklung bestens informieren.