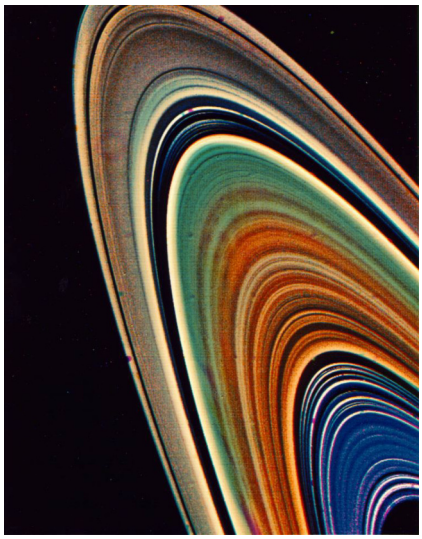
Vorlesungsskript Fehlerkorrigierende Kodes – eine Einführung

Prof. Dr. Hagen Knaf
Studiengang Angewandte Mathematik
Hochschule RheinMain

WS 2022/23



Falschfarbenaufnahme der Saturnringe
Fotografie der Sonde Voyager 2 vom 17. August 1981
Entfernung Sonde – Saturn: 8.9 Millionen Kilometer
Entfernung Sonde – Erde: 1.4 Milliarden Kilometer
(Courtesy NASA/JPL-Caltech)

Hinweis

Vorwort

Die Theorie der fehlerkorrigierenden Kodes ist Teil einer Antwort auf eine drängende technische Fragestellung: Wie kann man Information sicher und schnell über einen Kanal übertragen, der Störungen unterworfen ist, die sich der Kontrolle durch den Sender entziehen? Um sich eine Vorstellung von der Reichweite – im wahrsten Sinne des Wortes – dieser Frage zu machen, betrachte man die wunderbare Aufnahme der Ringe des Planeten Saturn zu Anfang dieses Skripts, die von der Raumsonde Voyager 2 mit einer Sendeleistung von 23 Watt – einer kleinen Glühbirne – über eine Entfernung von 1,4 Milliarden Kilometer zur Erde gesandt wurde. Das Funksignal benötigte für diese Strecke mehr als 75 Minuten, wogegen man mit dem japanischen Schnellzug Shinkansen bei 600 km/h etwa 266 Jahre bräuchte. Ein wenig Nachdenken über dieses Beispiel ist vielleicht schon Motivation genug, um sich mit der Mathematik der fehlerkorrigierenden Kodes zu beschäftigen. Diese ist jedoch nicht nur wegen ihres Anwendungsbezugs interessant, sie ist auch eine faszinierende Kombination von Aspekten mehrerer mathematischer Teilgebiete: der Stochastik, der Algebra und der Theorie metrischer Räume. Als solche ist die Theorie fehlerkorrigierender Kodes ein Musterbeispiel für das Erkenntnis- und Anwendungspotential, das in den durch ein hohes Maß an Kreativität gepaart mit dem Vermögen der Abstraktion in den letzten Jahrhunderten enstandenen mathematischen Teildisziplinen steckt. Schließlich sind fehlerkorrigierende Kodes auch historisch betrachtet ein interessanter Fall: Sie sind in einer besonderen Zeit entwickelt worden, die geprägt war vom »kalten Krieg« als Nachwirkung des zweiten Weltkriegs und von der Aufbruchstimmung des »Space Age«. Für Wissenschaftler der damaligen Zeit hat diese Kombination an Orten wie den Bell Laboratories traumhafte Arbeitsbedingungen geschaffen.

Im vorliegenden Skript und den dazugehörigen Lehrveranstaltungen habe ich versucht ein wenig der oben genannten Aspekte zum Ausdruck zu bringen.

Wünschmichelbach, Februar 2024 Hagen Knaf

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Information

Die Idee der fehlerkorrigierenden Kodes entstand als Antwort auf ein technisches Problem: Wie kann man Information sicher und schnell über einen Informationskanal übertragen, der Störungen unterworfen ist? Um dieses Problem mit mathematischen Mitteln anzugehen, muss man es zunächst begrifflich präzise fassen. Vor allem muss der Begriff »Information« definiert werden. Dies geschieht im vorliegenden Kapitel zusammen mit einer genauen Beschreibung des im Weiteren betrachteten Informationsübertragungsszenarios.

1.1 Zwei einführende Beispiele

Beispiel 1.1 (Phonetisches NATO-Alphabet): Als *Sprechfunk* bezeichnet man die Übertragung von gesprochener Sprache mittels elektromagnetischer Wellen im Frequenzbereich von etwa 30 Kilohertz (kHz) bis 300 Megahertz (MHz). Dabei können zwei Personen auf einer festen Frequenz miteinander sprechen. Einsatzgebiete des Sprechfunks sind beispielsweise Bahn, Schifffahrt, Luftfahrt, Polizei, Militär, wobei jeweils bestimmte Frequenzbereiche genutzt werden.

Elektromagnetische Wellen unterliegen verschiedenen Arten von Störungen, die unter anderem folgende Ursachen besitzen: Durchgang der Wellen durch feste oder flüssige Hindernisse, Reflektion an solchen Hindernissen, elektromagnetische Vorgänge in der Erdatmosphäre, Streuung an der Ionosphäre. Solche Störungen können die Übertragungsqualität beim Sprechfunk erheblich beeinträchtigen, sodass vom Sender gesprochene Wörter und Sätze beim Empfänger möglicherweise nicht mehr verstanden werden. Um die korrekte Übertragung von wichtigen Informationen wie der Art eines Notrufs in der Schifffahrt oder eine Positionsangabe dennoch zu ermöglichen, wird das *phonetische NATO Alphabet* verwendet: Die Wörter werden buchstabiert statt am Stück ausgesprochen, wobei für die einzelnen Buchstaben bestimmte Kodewörter verwendet werden.

Buchstabe	Kodewort	Buchstabe	Kodewort
A	Alpha	N	November
B	Bravo	O	Oscar
C	Charlie	P	Papa
D	Delta	Q	Quebec
E	Echo	R	Romeo
F	Foxtrot	S	Sierra
G	Golf	T	Tango
H	Hotel	U	Uniform
I	India	V	Victor
J	Juliet	W	Whiskey
K	Kilo	X	X-ray
L	Lima	Y	Yankee
M	Mike	Z	Zulu

Tabelle 1: Das phonetische NATO-Alphabet

Das Wort »Hilfe« wird also zum Beispiel als »Hotel India Lima Foxtrot Echo« übertragen.

Die Kodewörter wurden so gewählt, dass je zwei verschiedene möglichst unähnlich klingen und daher auch bei stark gestörter Sprechfunkverbindung nicht leicht verwechselt werden. Dieses Prinzip wird in abstrakter Form später erneut auftreten.

Durch die Verwendung des phonetischen NATO Alphabets wird gesprochene Sprache so kodiert, dass die Wahrscheinlichkeit für eine korrekte Informationsübertragung auch unter schlechten Empfangsbedingungen stark erhöht wird. Allerdings muss hierfür die Menge der zu übermittelnden Information ebenfalls erhöht werden, was den Informationsaustausch verlangsamt. ◇

Beispiel 1.2 (Wiederholungskodes): Die Sicherheit einer Informationsübertragung kann auch durch Verwendung eines *Wiederholungskodes* erhöht werden: Nehmen wir an eine auf dem Planeten Venus gelandete Sonde sendet in regelmäßigen Zeitabständen per Funksignal den Wert der Temperatur am Landeort an die Bodenstation auf der Erde. Dieses Signal muss die Venus- und die Erdatmosphäre passieren, Störungen sind also zu erwarten. Die Tem-

peraturwerte selbst werden im Binärsystem gesendet, wobei die Oberflächentemperatur der Venus aufgrund eines Treibhauseffekts grob zwischen 300°C und 500°C variiert, man kommt also sicher mit 10-stelligen Binärzahlen aus, da $2^{10} = 1024$. Ein Wert von 317°C wird beispielsweise als

$$0100111101 = 2^8 + 2^5 + 2^4 + 2^3 + 2^2 + 2^0$$

gesendet, wobei hier die technische Frage, in welcher Form die Nullen und Einsen gesendet werden, außer acht gelassen wird.

Um die Wahrscheinlichkeit für eine korrekte Übertragung zu erhöhen, wird jede 0 und jede 1 dreimal in Folge gesendet; im Beispiel wird also die Binärfolge

$$000\,111\,000\,000\,111\,111\,111\,111\,000\,111 \tag{1}$$

übermittelt.

Auf der Empfängerseite wird jede empfangene Dreiergruppe von 0en und 1en gemäß der Tabelle 2 konvertiert.

Dreiergruppe	Wert
000	0
001	0
010	0
100	0
011	1
101	1
110	1
111	1

Tabelle 2: Dekodierung eines Wiederholungskodes

Beispielsweise könnte die Sequenz (1) aufgrund von Störungen als

$$000\,101\,100\,000\,111\,011\,111\,111\,110\,111 \tag{2}$$

empfangen werden. Dann liefert die Tabelle den Temperaturwert

$$0100111111 = 2^8 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = 319.$$

Die Wahrscheinlichkeit für eine fehlerhafte Übertragung eines Temperaturwerts ohne Verwendung des Wiederholungskodes beträgt

$$p = 1 - (1 - p_0)^{10},$$

wobei p_0 die Wahrscheinlichkeit dafür ist, dass eine 0 oder 1 inkorrekt übertragen wird. Man nimmt hierbei an, dass die Fehlerwahrscheinlichkeiten in beiden Fällen gleich sind, und weiter dass die Fehler an den einzelnen Stellen der Binärfolge stochastisch unabhängig sind.

Bei Verwendung des Wiederholungskodes besitzt die Wahrscheinlichkeit für die inkorrekte Übertragung einer 0 den Wert

$$p_0' = p_0^3 + 3p_0^2(1 - p_0) = p_0(p_0^2 + 3p_0(1 - p_0)).$$

Derselbe Wert ergibt sich für die inkorrekte Übertragung einer 1. Die Wahr-

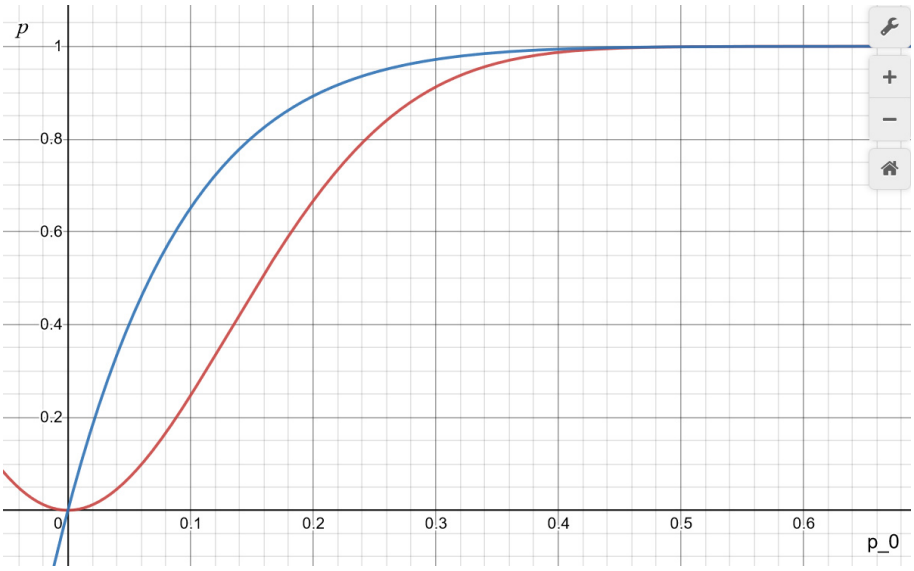


Abbildung 1: Wahrscheinlichkeit eines Fehlers bei der direkten Übertragung von 10 Bit (blau) und bei Verwendung eines 3-fach-Wiederholungskodes (rot) abhängig von der Bitfehlerrate p_0

scheinlichkeit für einen Übertragungsfehler ist nun

$$p' = 1 - (1 - p_0')^{10}.$$

In Abbildung 1 sind die Fehlerwahrscheinlichkeiten abhängig von p_0 für den Fall direkter Übertragung in blau und bei Verwendung des 3-fach-Wiederholungskodes in rot dargestellt. Der Sicherheitsgewinn ist deutlich zu erkennen. Der Preis dafür ist allerdings eine dreimal höhere zu übertragende Informationsmenge. ◇

1.2 Das Sender-Empfänger-Szenario

Die Vorgänge in den beiden im vorigen Abschnitt beschriebenen Beispielen können durch Abstraktion in folgender Form zusammengefasst werden:

1. Ein *Sender* erzeugt Information.

   In den beiden Beispielen ist die gerade sprechende Person bzw. das Temperaturmessgerät der Sonde der Sender.

2. Die Information wird in einer bestimmten Form *kodiert* (kodieren: hier: »in eine bestimmte Form bringen«, *nicht* in der Bedeutung von »verschlüsseln«).

   Im ersten Beispiel wird die Information in eine Folge von NATO-Alphabet-Wörtern kodiert. Im zweiten Beispiel wird eine Folge von Dreiergruppen von Nullen und Einsen als Kodierung des Temperaturwertes verwendet.

3. Die kodierte Information wird über einen *Übertragungskanal* an einen *Empfänger* geschickt.

   Im ersten und im zweiten Beispiel ist der Übertragungskanal der (mit elektromagnetischen Wellen erfüllte) physikalische Raum in Kombination mit den verwendeten Sende- und Empfangsgeräten: Die Schallwellen bzw. eine Binärzahl werden vom Sendegerät in elektromagnetische Wellen umgewandelt und vom Empfangsgerät wieder in das ursprüngliche Format zurücktransformiert.

4. Beim Passieren des Übertragungskanals wird die kodierte Information mit einer gewissen Wahrscheinlichkeit gestört.

   In beiden Beispielen können Störungen durch die Sende- und Empfangstechnik selbst, sowie durch Phänomene wie etwa Blitze oder andere elektromagnetische Vorgänge im durchlaufenen Raum verursacht werden.

5. Der Empfänger *dekodiert* die erhaltene kodierte Information um sie zu »lesen«.

   Zur Dekodierung wird im ersten Beispiel die Liste der NATO-Alphabet-Wörter verwendet, im zweiten Beispiel die Tabelle zur Übersetzung von Bit-Dreiergruppen in einzelne Bits.

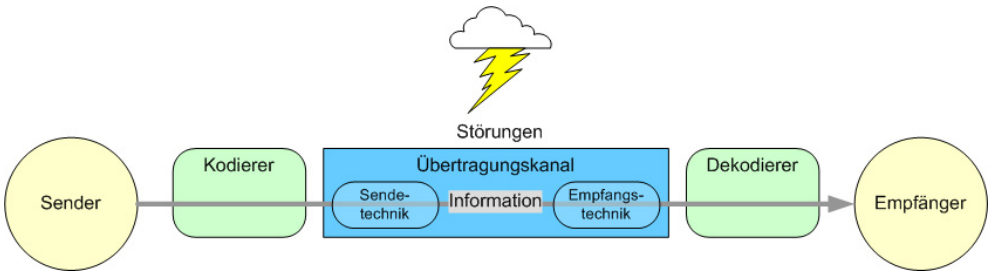


Abbildung 2: Einfaches Sender-Empfänger-Szenario

In den beiden Beispielen befinden sich Sender und Empfänger an verschiedenen Orten und die oben genannten Vorgänge erfolgen entsprechend ihrer Nummerierung in vergleichsweise schneller, zeitlicher Reihenfolge. Das muss im Allgemeinen nicht so sein; das abstrakte Schema erfasst zum Beispiel auch folgendes Szenario: Ein mit einem Textverarbeitungsprogramm von einer Person X erstelltes Dokument wird auf einem USB-Stick gespeichert. Dieselbe Person öffnet das Dokument nach zwei Jahren wieder mit demselben Programm um seinen Inhalt zu lesen. In diesem Szenario sind Sender und Empfänger die Person X. Die Kodierung und Dekodierung der Information erfolgt durch das Textverarbeitungsprogramm, das den eingegebenen Text in ein binäres Format beziehungsweise von diesem binären Format in eine Folge lesbarer Zeichen umwandelt. Der Übertragungskanal besteht aus dem physikalischen Prozess des Schreibens und Lesens von Daten auf und von einem USB-Stick, sowie aus dem USB-Stick selbst. Denn letzterer speichert Information nicht dauerhaft sicher, sondern unterliegt einem durch das Benutzen verursachten Abnutzungsprozess, sowie Störungen durch aus dem Weltraum mit hoher Geschwindigkeit auf die Erde treffenden Elementarteilchen.

Das Grundproblem in dem durch die Punkte 1 bis 5 beschriebenen Szenario besteht darin sicherzustellen, dass die Information vom Sender korrekt zum Empfänger übertragen wird. Hierzu gibt es prinzipiell zwei Ansätze, die in der Praxis kombiniert verfolgt werden: Der *technisch-physikalische Ansatz* verfolgt das Ziel den Übertragungskanal so zu gestalten, dass eine hohe Übertragungsqualität vorliegt. Beim Sprechfunk kann das zum Beispiel durch die Identifikation und Verwendung von Frequenzen geschehen, die nur gering durch atmosphärische Vorgänge gestört werden. Weiter kann etwa am Design von Sende- und Empfangsantennen gearbeitet werden.

Beim *Systemansatz* geht man von einem Übertragungskanal mit einer bestimmten Übertragungsqualität aus und versucht die zu übertragende Information so zu kodieren, dass Übertragungsfehler beim Dekodieren erkannt und möglicherweise sogar korrigiert werden können. Der Systemansatz gründet auf zwei Theorien: In der *Informationstheorie* werden die Eigenschaften eines Übertragungskanals untersucht. Insbesondere wird dort ein Maß zur Quantifizierung von Information eingeführt und es werden theoretische Grenzen für die über einen bestimmten Kanal übertragbare Informationsmenge ermittelt. Die *Kodierungstheorie* dagegen befasst sich mit der konkreten Realisierung effizienter Kodierungs- und Dekodierungsalgorithmen. Effizienz bedeutet hierbei einerseits hohe Erkennungs- und Korrekturraten für Übertragungsfehler und andererseits Schnelligkeit der verwendeten Algorithmen. Sowohl Informations- als auch Kodierungstheorie sind in ihrem Kern mathematische Theorien. Die erstere beruht auf stochastischen Methoden, während in der zweiten Analysis, Algebra und Geometrie eingesetzt werden.

Die Vorlesung liegt mit Ausnahme der beiden folgenden Abschnitte thematisch im algebraisch-geometrischen Teil der Kodierungstheorie. Was dies genau bedeutet, wird später erläutert.

Für manche Anwendungen der Kodierungstheorie reicht die Fehlererkennung aus, da die Möglichkeit zur Rückfrage besteht: Wurde ein Fehler erkannt, so benachrichtigt der Empfänger den Sender und fordert die entsprechende Information erneut an. Erforderlich ist hierzu eine Zwei-Wege-Kommunikation. Mit diesem Szenario befasst sich die Vorlesung nicht.

1.3 Die mathematische Beschreibung von Information

Es ist schwierig den Begriff »Information« allgemein zu definieren und es ist auch keine allgemein anerkannte Definition verfügbar. Dies liegt daran, dass Information aus physikalischer und philosophischer Sicht eine eigene Art »Ding« ist:

Information is information, not matter or energy.

Dieses Zitat stammt von dem amerikanischen Mathematiker Norbert Wiener (1894 – 1964), der als Erfinder der *Kybernetik* gilt, also der Wissenschaft von der Steuerung und Regelung von Systemen, in der der Informationsbegriff eine wesentliche Rolle spielt.

Abbildung 3: Norbert Wiener 1955 in Kalkutta
(Courtesy of the Archives of the Indian Statistical Institute, Kolkata)

Das obige Bild wurde der Webseite zur IEEE 2016 Conference ≫Norbert Wiener in the 21st Century≪ entnommen. Dort wird angegeben, dass die Personen von links nach rechts Norbert Wiener's Ehefrau Margaret Engemann, Norbert Wiener, Mrs. Mahalanobis (Nirmalkumari, die Ehefrau von P. C. Mahalanobis), Mrs. Shewart (Wahrscheinlich ist ≫Shewhart≪ gemeint, und es handelt sich um die Ehefrau Edna Elizabeth Hart des amerikanischen Physikers, Ingenieurs und Statistikers Walter Andrew Shewhart (1891 – 1967), der sich 1954 als Dozent am Indian Statistical Institute aufhielt.), Prasanta Chandra Mahalanobis (stehend, indischer Statistiker, 1893 – 1972) sind. Norbert Wiener befasste sich im Lauf seines wissenschaftlichen Lebens unter anderem mit Zoologie, Philosophie der Mathematik, Mathematik (Logik, Maßtheorie, Stochastik) und Physik (Quantenmechanik).

Um einen Eindruck davon zu gewinnen, wie eine fachgebietübergreifende Definition aussehen könnte, sei hier der Vorschlag des Informationswissenschaftlers Robert Losee von der University of North Carolina angegeben:

Information is produced by all processes and it is the values of characteristics in the processes' output that are information.

In freier Übersetzung:

Information ist etwas, das von allen Prozessen erzeugt wird. Es besteht aus den Werten aller von einem Prozess erzeugten, charakteristischen Größen.

Natürlich müssten jetzt die Begriffe »Prozess« und »charakteristische Größe« definiert werden. Dies soll hier aber nicht weiter verfolgt werden. Stattdessen fassen wir einen enger begrenzten Bereich ins Auge, in dem Information mathematisch definiert werden kann.

Information in einem noch nicht genau definierten Sinn kann in verschiedenen Formen kodiert auftreten: in einer Folge von Schallwellen (Sprache), in einer Folge von Buchstaben (Text), in einer Folge von elektromagnetischen Wellen (Sprechfunk), in einer Folge von elektrischen Impulsen in einem Kabel (Telefon), in einer räumlichen Zusammenstellung von Farben (Bild), um einige Beispiele zu nennen. Eine bestimmte Kodierungsform kann manchmal unter weitgehender Erhaltung der Information in eine andere Kodierungsform umgewandelt werden. So kann man etwa Sprache als Text niederschreiben. Dabei geht allerdings die in der Betonung liegende Information verloren.

Viele Kodierungsformen von Information kann man in endliche Folgen von endlich vielen Symbolen umwandeln: Texte besitzen bereits diese Form; sie sind eine endliche Folge von Buchstaben und Satzzeichen des verwendeten Alphabets. Gesprochenes kann man als endliche Folge von Lauten betrachten, wobei die Laute aus einem endlichen, von der jeweiligen Sprache abhängigen Repertoire stammen. Den Umwandlungsprozess von Information in eine Folge von endlich vielen Symbolen nennt man *Digitalisierung*. Motiviert durch diese Tatsachen definiert man:

Definition 1.3: *Ein Alphabet ist eine endliche Menge $\mathbb{A}$; ihre Elemente $a \in \mathbb{A}$ werden als Buchstaben oder Symbole bezeichnet.*

Ein Wort über $\mathbb{A}$ ist eine endliche Folge von Buchstaben aus $\mathbb{A}$, also eine Abbildung $w : \{1, \ldots, \ell\} \to \mathbb{A}$. Die Zahl ℓ heißt Länge des Wortes w.

Bemerkung: Der mathematische Begriff »Wort« ist allgemeiner als der sprachliche Begriff. Auch der Text eines ganzen Buchs ist mathematisch betrachtet ein Wort.

Bei der Übertragung digital vorliegender Information müssen Sender und Empfänger nicht notwendigerweise dasselbe Alphabet verwenden. Wir betrachten daher nun die folgende speziellere und detailliertere Variante des im vorigen Abschnitt beschriebenen Sender-Empfänger-Szenarios:

1. Ein Sender erzeugt Information.
2. Die Information wird falls nötig digitalisiert.

   Die Venussonde aus dem zweiten Beispiel digitalisiert die analog gemessenen Temperaturwerte in einen ganzzahligen Wert zwischen 0 und 1023.
3. Die digitalisierte Information wird unter Verwendung eines Alphabets $\mathbb{A}$ kodiert.

   Die Venussonde kodiert diesen Wert unter Verwendung des Alphabets $\mathbb{A} = \{000, 111\}$.
4. Die kodierte Information wird über einen Übertragungskanal an einen Empfänger geschickt.
5. Beim Passieren des Übertragungskanals wird die kodierte Information mit einer gewissen Wahrscheinlichkeit gestört.
6. Der Empfänger dekodiert die erhaltene kodierte Information unter Verwendung eines bestimmten Verfahrens in eine im Alphabets $\mathbb{B}$ kodierte Information.

   Im Fall der Venussonde ist $\mathbb{B} = \{0, 1\}$, da die empfangene Folge von Nullen und Einsen in eine Binärzahl dekodiert wird.

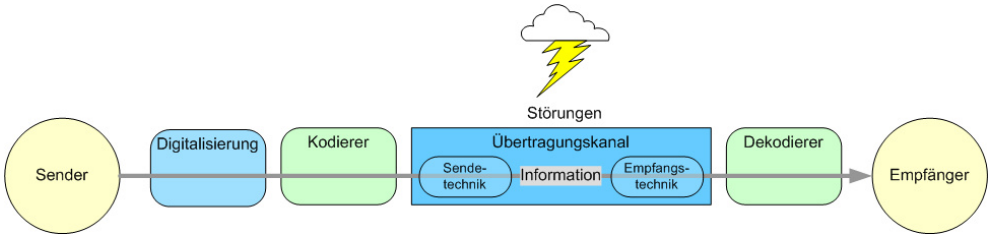


Abbildung 4: Sender-Empfänger-Szenario mit Digitalisierung

Für dieses Szenario wird nun ein stochastisches, mathematisches Modell erstellt: Jedes Symbol $a \in \mathbb{A}$ sollte beim Übertragungsvorgang im Idealfall in ein durch a eindeutig bestimmtes Symbol $b \in \mathbb{B}$ übertragen werden, nämlich dann, wenn im Übertragungskanal keine Störungen auftreten. Im Fall der Venussonde sollte 000 in 0 und 111 in 1 übertragen werden. In der Realität geschieht dies nur mit einer gewissen Wahrscheinlichkeit.

In einem guten mathematischen Modell sollte außerdem die folgende Tatsache ihren Niederschlag finden: Kodiert man Information unter Verwendung eines Alphabets $\mathbb{A}$, so treten die Symbole $a \in \mathbb{A}$ abhängig von der Art der Information mit unterschiedlichen Häufigkeiten auf. So kommt der Buchstabe e in einem hinreichend langen deutschen Text viel häufiger vor, als der Buchstabe x.

Wir entwickeln entsprechend ein stochastisches Modell:

- **Senderseite**: Auf einem Alphabet $\mathbb{A}$, das zur Kodierung der zu sendenden Information verwendet wird, ist eine Wahrscheinlichkeitsverteilung $p_{\mathbb{A}} : \mathbb{A} \to [0,1]$ gegeben; jedem Symbol $a \in \mathbb{A}$ ist eine Auftrittswahrscheinlichkeit $p_{\mathbb{A}}(a)$ so zugeordnet, dass

  $$\sum_{a \in \mathbb{A}} p_{\mathbb{A}}(a) = 1.$$

  Damit ist das Tripel $(\mathbb{A}, P(\mathbb{A}), p_{\mathbb{A}})$ ein Wahrscheinlichkeitsraum, wobei $P(\mathbb{A})$ die Potenzmenge des Alphabets ist, wenn man für $E \in P(\mathbb{A})$ wie üblich

  $$p_{\mathbb{A}}(E) := \sum_{a \in E} p_{\mathbb{A}}(a) \tag{3}$$

  definiert.

  Es ist wichtig zu verstehen, dass mit $p_{\mathbb{A}}$ die Art der gesendeten Information (Romantexte, Temperaturwerte, technische Berichte) modelliert wird.

- **Übertragungskanal**: Es sei $\mathbb{B}$ das zur Kodierung der Information auf Empfängerseite verwendete Alphabet. Dann ist auf jeder der Mengen $\{a\} \times \mathbb{B}$ eine Wahrscheinlichkeitsverteilung

  $$p_{\mathrm{rc}}(\cdot|a) : \ \{a\} \times \mathbb{B} \to [0,1], \ (a,b) \mapsto p_{\mathrm{rc}}(b|a) \tag{4}$$

  gegeben. Der Wert $p_{\mathrm{rc}}(b|a)$ gibt die Wahrscheinlichkeit dafür an das Symbol b zu empfangen (receive), wenn das Symbol a gesendet wurde.

Die Wahrscheinlichkeitsverteilungen $p_{\mathrm{rc}}(\cdot|a)$, $a \in \mathbb{A}$, beschreiben zwei Einflüsse auf die Informationsübertragung:

- die Qualität des Übertragungskanals bei Verwendung der Alphabete $\mathbb{A}$ und $\mathbb{B}$ zur Kodierung von Information,
- den Einfluss des Dekodierers.

Dabei wird angenommen, dass durch das Senden selbst diese Effekte nicht beeinflusst werden, denn die Verteilungen ändern sich nicht in Abhängigkeit von der erfolgten Anzahl von Sendevorgängen. Man spricht in diesem Fall von einem *gedächtnislosen Übertragungskanal* (engl.: memoryless channel). Diese Annahme ist nicht immer gerechtfertigt: Die Sende- und Empfangstechnik etwa altert durch Gebrauch.

Man beachte, dass beim Systemansatz die Qualität des Übertragungskanals eine fest vorgegebene Größe ist, während der Dekodierer variiert werden kann.

Die Wahrscheinlichkeitsverteilungen $p_{\mathbb{A}}$ und $p_{\mathrm{rc}}(\cdot|a)$, $a \in \mathbb{A}$, liefern eine Wahrscheinlichkeitsverteilung auf dem Produkt $\mathbb{A} \times \mathbb{B}$:

$$p_{\mathbb{A}\times\mathbb{B}} : \mathbb{A} \times \mathbb{B} \to [0,1],\ (a,b) \mapsto p_{\mathbb{A}\times\mathbb{B}}(a,b) := p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b|a). \qquad (5)$$

Der Wert $p_{\mathbb{A}\times\mathbb{B}}(a,b)$ ist die Wahrscheinlichkeit dafür in einem Sendewort das Symbol a und im zugehörigen Empfangswort an der entsprechenden Position das Symbol b zu lesen.

Wie im Fall von $p_{\mathbb{A}}$ erhält man auch hier einen Wahrscheinlichkeitsraum $(\mathbb{A} \times \mathbb{B}, P(\mathbb{A} \times \mathbb{B}), p_{\mathbb{A}\times\mathbb{B}})$.

- **Empfängerseite**: Auf dem empfängerseitigen Alphabet $\mathbb{B}$ ist nun eine Wahrscheinlichkeitsverteilung p_{rc} durch die Gleichungen

$$\forall b \in \mathbb{B} \quad p_{\mathrm{rc}}(b) := \sum_{a\in\mathbb{A}} p_{\mathbb{A}\times\mathbb{B}}(a,b) \qquad (6)$$

definiert. Der Wert $p_{\mathrm{rc}}(b)$ gibt die Wahrscheinlichkeit dafür an das Symbol b in einem Empfangswort zu lesen. Man beachte, dass im Allgemeinen

$$p_{\mathrm{rc}}(b) \neq p_{\mathbb{B}}(b)$$

gilt, da die a priori Häufigkeit von Symbolen in Wörtern bestimmter Form über $\mathbb{B}$ durch die Eigenschaften des Übertragungskanals geändert wird.

Wie im Fall von $p_{\mathbb{A}}$ erhält man durch

$$p_{\mathrm{rc}}(E) := \sum_{b \in E} p_{\mathrm{rc}}(b) \tag{7}$$

einen Wahrscheinlichkeitsraum $(\mathbb{B}, P(\mathbb{B}), p_{\mathrm{rc}})$.

FESTSTELLUNG 1.4: *Die Wahrscheinlichkeitsverteilungen $p_{\mathbb{A}}$ und p_{rc} sind die Randverteilungen der Wahrscheinlichkeitsverteilung $p_{\mathbb{A}\times\mathbb{B}}$ und damit durch letztere eindeutig festgelegt.*

BEWEIS: Die Behauptung gilt nach Definition für die Wahrscheinlichkeitsverteilung p_{rc}.
Für jedes $a \in \mathbb{A}$ gilt andererseits

$$\sum_{b \in \mathbb{B}} p_{\mathbb{A}\times\mathbb{B}}(a,b) = \sum_{b \in \mathbb{B}} p_{\mathbb{A}}(a) p_{\mathrm{rc}}(b|a) = p_{\mathbb{A}}(a) \sum_{b \in \mathbb{B}} p_{\mathrm{rc}}(b|a) = p_{\mathbb{A}}(a).$$

□

Die Wahrscheinlichkeiten $p_{\mathrm{rc}}(b|a)$ sind bedingte Wahrscheinlichkeiten, denn es gilt nach Definition

$$p_{\mathrm{rc}}(b|a) = \frac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{A}}(a)}. \tag{8}$$

Entsprechend kann man nun auch die bedingte Wahrscheinlichkeit $p_{\mathrm{sd}}(a|b)$ dafür berechnen, dass das Symbol a gesendet (send) wurde, wenn das Symbol b empfangen wurde:

$$p_{\mathrm{sd}}(a|b) = \frac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{B}}(b)}. \tag{9}$$

BEISPIEL 1.5 (Proteinsynthese): Proteine, auch Eiweiße genannt, bilden die Grundbausteine von Organismen. Jedes Protein ist eine spezifische Kombination von Aminosäuren, einer speziellen Klasse von chemischen Verbindungen auf Kohlenstoffbasis. In den Proteinen des menschlichen Körpers kommen insgesamt 20 Aminosäuren als Bausteine vor. Der Bauplan der verschiedenen Proteine ist in der Desoxyribonukleinsäure (DNS) im Zellkern jeder Körperzelle gespeichert. Die DNS ist im Wesentlichen eine Kette bestehend aus vier chemischen Substanzen, den Basen **A**denin, **T**hymin, **G**uanin

und **C**ytosin. Jeweils drei aufeinanderfolgende Basen stehen für eine Aminosäure. Da es theoretisch $4^3 = 64$ solche Basentriplets gibt, aber nur 20 Aminosäuren zum Bau von Proteinen benutzt werden, kann jede Aminosäure eindeutig als Wort der Länge 3 über dem Alphabet $\mathbb{A} = \{A, T, G, C\}$ der vier Basen dargestellt werden, wobei manche Triplets nicht vorkommen.

Der Bauplan jeweils eines Proteins bildet eine zusammenhängende Folge von Basentriplets im DNS-Molekül. Ein solche Folge wird durch ein Starttriplet eingeleitet und durch ein Stoptriplet beendet. Beide Triplets entsprechen keiner Aminosäure. Jeden solchen Bauplan bezeichnet man als Gen – ein Gen ist also ein Wort über dem Alphabet $\mathbb{A}$ mit einer durch 3 teilbaren Länge.

Der Aufbau von Proteinen findet in der Zelle in den Ribosomen statt, die Bauplaninformation muss also vom Zellkern zu den Ribosomen gebracht werden. Dies geschieht durch Herstellen einer Kopie des entsprechenden Gens im Zellkern. Das dabei entstehende Kettenmolekül nennt man Messenger-Ribonukleinsäure (mRNS); es kann zu den Ribosomen wandern und dort die Synthese des durch das Gen bestimmten Proteins steuern. Die mRNS verwendet ein leicht geändertes Alphabet zur Speicherung des kopierten Gens, nämlich $\mathbb{B} = \{A, U, G, C\}$, wobei das Symbol U für die Base **U**racil steht. Der Kopiervorgang erfolgt nach folgender Regel:

$$A \mapsto U,\ T \mapsto A,\ G \mapsto C,\ C \mapsto G. \tag{10}$$

In einem Ribosom angekommen wird die mRNS als Grundlage für den Aufbau eines Proteins verwendet. Dabei lagern sich an das mRNS-Molekül sogenannte Transfer-Ribonukleinsäuremoleküle (tRNS) an, die jeweils aus einem Basentriplet und einer Aminosäure bestehen. Damit der Proteinaufbau an jeweils aktuelle Erfordernisse des Körpers angepasst werden kann, sowie aus komplexen anderen Gründen, findet im Ribosom auch ein Editieren des mRNS-Moleküls statt. In ihrer Gesamtheit können diese Vorgänge zu Übersetzungsfehlern führen, sodass das dem kopierten Gen entsprechende Protein nicht korrekt aufgebaut wird.

Bis hier wurde eine sehr stark vereinfachte Beschreibung der Proteinsynthese in der Zelle gegeben. Die folgenden Ausführungen entsprechen *nicht* den tatsächlichen Vorgängen bei der Entstehung von Fehlern in der Proteinsynthese, sondern stellen eine Illustration des Sender-Empfänger-Szenarios im Kontext der Proteinsynthese dar. In dieser Illustration wird angenommen, dass Fehler in der Proteinsynthese durch Kopierfehler in der Abbildung (10) entstehen. Man betrachtet also den Zellkern als Sender von Information, die mit den Symbolen des Alphabets $\mathbb{A}$ geschrieben ist, und das Ribosom

als Empfänger von Information, die mit den Symbolen des Alphabets $\mathbb{B}$ geschrieben ist. Der Übertragungskanal besteht aus dem im Zellkern erfolgenden Kopiervorgang. Entsprechend dem allgemeinen stochastischen Modell des Übertragungskanals kann man die vorliegende Situation nun wie folgt mathematisch beschreiben:

- **Senderseite**: Die Häufigkeit der Basen in der DNS des Menschen liefert die Wahrscheinlichkeitsverteilung $p_{\mathbb{A}}$. Experimentell wurde sie zu

$$p_{\mathbb{A}}(A) = 0,299,\ p_{\mathbb{A}}(T) = 0,298,\ p_{\mathbb{A}}(G) = 0,195,\ p_{\mathbb{A}}(C) = 0,201.$$

  bestimmt. Die Tatsache, dass A und T, sowie C und G etwa gleich wahrscheinlich sind, wird nach dem Biochemiker und Schriftsteller Erwin Chargaff (1905 – 2002), der dieses Phänomen entdeckte, als Chargaff-Regel bezeichnet.

- **Übertragungskanal**: Die folgenden Angaben zu den vier Verteilungen $p_{\mathrm{rc}}(\cdot|A)$, $p_{\mathrm{rc}}(\cdot|T)$, $p_{\mathrm{rc}}(\cdot|G)$ und $p_{\mathrm{rc}}(\cdot|C)$ sind frei erfunden. Man beachte aber die Kopierabbildung (10).

Verteilung	U	A	C	G
$p_{\mathrm{rc}}(\cdot\|A)$	0.95	0.01	0.03	0.01
$p_{\mathrm{rc}}(\cdot\|T)$	0.02	0.91	0.03	0.04
$p_{\mathrm{rc}}(\cdot\|G)$	0.03	0.05	0.89	0.03
$p_{\mathrm{rc}}(\cdot\|C)$	0.02	0.01	0.01	0.96

  Hieraus errechnet sich die Verteilung $p_{\mathbb{A}\times\mathbb{B}}$ nach Formel (5) zu:

	U	A	C	G
A	0.28405	0.00299	0.00897	0.00299
T	0,00596	0,27118	0,00894	0,01192
G	0,00585	0,00975	0,17355	0,00585
C	0,00402	0,00201	0,00201	0,19296

- **Empfängerseite**: Für die Verteilung p_{rc} ergibt sich nach Formel (6):

$$\begin{aligned} p_{\mathrm{rc}}(U) &= 0,29988, \quad p_{\mathrm{rc}}(A) = 0,28593, \\ p_{\mathrm{rc}}(C) &= 0,19347, \quad p_{\mathrm{rc}}(G) = 0,21372. \end{aligned}$$

$\diamond$

Mit Hilfe des stochastischen Modells des Übertragungskanals kann man sich einem präzisen Begriff der Information annähern:

DEFINITION 1.6: *Für $a \in \mathbb{A}$ und $b \in \mathbb{B}$ gelte $p_{\mathbb{A}\times\mathbb{B}}(a,b) \neq 0$. Die Größe*

$$I(a,b) := \log_2\left(\frac{p_{\mathrm{sd}}(a|b)}{p_{\mathbb{A}}(a)}\right) = \log_2\left(\frac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}\right)$$

wird als »Information von b über a« bezeichnet. Hierbei bezeichnet $\log_2$ den Logarithmus zur Basis 2.

BEMERKUNGEN:

1. Aus $p_{\mathbb{A}\times\mathbb{B}}(a,b) \neq 0$ folgt nach Definition $p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b) \neq 0$, weswegen $I(a,b)$ wohldefiniert ist.

2. Der Logarithmus zur Basis 2 existiert wie der natürliche Logarithmus für reelle Zahlen $x > 0$ und ist durch die Gleichung

   $$2^{\log_2(x)} = x$$

   charakterisiert. Entsprechend gilt die Umrechnungsformel

   $$\log_2(x) = \frac{\ln(x)}{\ln(2)}.$$

   Auf den Grund für die Verwendung des Logarithmus' zur Basis 2 wird später eingegangen werden.

   Die Logarithmusfunktion $\log_2(\cdot)$ ist streng monoton wachsend und konkav, zwei Eigenschaften, die im Folgenden noch benötigt werden.

3. Im Kontext des Sender-Empfänger-Szenarios sollte man $I(a,b)$ genauer als Information des Ereignisses »b wurde empfangen« über das Ereignis »a wurde gesendet« bezeichnen.

4. Es ist $I(a,b) > 0$ genau dann, wenn $p_{\mathrm{sd}}(a|b) > p_{\mathbb{A}}(a)$, das heißt die Wahrscheinlichkeit für das Ereignis »a wurde gesendet gegeben, dass b empfangen wurde« ist größer als die Auftrittswahrscheinlichkeit von a in einem (langen) Wort über $\mathbb{A}$. Intuitiv bedeutet dies, dass der Empfang von b tatsächlich eine Information ist, die die Richtigkeit der Aussage »a wurde gesendet« stützt, und zwar wegen der Monotonie von $\log_2(\cdot)$ umso stärker, je größer $p_{\mathrm{sd}}(a|b)$ in dieser Situation ausfällt.

Analog ist $I(a,b) < 0$ genau dann, wenn $p_{\mathrm{sd}}(a|b) < p_{\mathbb{A}}(a)$. Der Wert von $I(a,b)$ stützt die Richtigkeit der Aussage »a wurde nicht gesendet« umso stärker, je kleiner er ist.

FESTSTELLUNG 1.7: *Die Größe $I(a,b)$ besitzt folgende Eigenschaften:*

1. *Es gilt $I(a,b) = 0$ genau dann, wenn die Ereignisse »a wurde gesendet« und »b wurde empfangen« stochastisch unabhängig sind.*

2. $I(a,b) \leq -\log_2(p_{\mathbb{A}}(a))$.

   Die obere Schranke wird von $I(a,b)$ genau dann angenommen, wenn $p_{\mathrm{sd}}(a|b) = 1$ gilt.

BEWEIS: Zu 1.: $I(a,b) = 0$ gilt genau dann, wenn $p_{\mathbb{A}\times\mathbb{B}}(a,b) = p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)$ gilt. Nach Festellung 1.4 ist

$$p_{\mathbb{A}}(a) = p_{\mathbb{A}\times\mathbb{B}}(\{a\}\times\mathbb{B}),\ p_{\mathrm{rc}}(b) = p_{\mathbb{A}\times\mathbb{B}}(\mathbb{A}\times\{b\})$$

und daher

$$p_{\mathbb{A}\times\mathbb{B}}(a,b) = p_{\mathbb{A}\times\mathbb{B}}((\{a\}\times\mathbb{B})\cap(\mathbb{A}\times\{b\})) = p_{\mathbb{A}\times\mathbb{B}}(\{a\}\times\mathbb{B})p_{\mathbb{A}\times\mathbb{B}}(\mathbb{A}\times\{b\}),$$

die Ereignisse $\{a\}\times\mathbb{B}$ und $\mathbb{A}\times\{b\}$ sind also stochastisch unabhängig. Diese Ereignisse entsprechen aber gerade den in der Feststellung genannten.

Zu 2.: Es gilt $I(a,b) = \log_2(p_{\mathrm{sd}}(a|b)) - \log_2(p_{\mathbb{A}}(a))$, wobei der erste Summand negativ und der zweite positiv ist. □

Als quantitatives Maß für die Qualität des Übertragungskanals bei Verwendung der Alphabete $\mathbb{A}$ und $\mathbb{B}$ definiert man nun folgerichtig:

DEFINITION 1.8: *Die Größe*

$$I(p_{\mathbb{A}}, p_{\mathrm{rc}}) := \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)I(a,b)$$

wird als »Information von p_{rc} über $p_{\mathbb{A}}$« bezeichnet.

BEMERKUNG: Die Größe $I(p_{\mathbb{A}}, p_{\mathrm{rc}})$ ist das mit den Wahrscheinlichkeiten $p_{\mathbb{A}\times\mathbb{B}}(a,b)$ gewichtete Mittel der Informationen, die von den Ereignissen »b wurde empfangen« über die Ereignisse »a wurde gesendet« geliefert werden.

SATZ 1.9: *Die Information von p_{rc} über $p_{\mathbb{A}}$ besitzt folgende Eigenschaften:*

1. $I(p_{\mathbb{A}}, p_{\mathrm{rc}}) \geq 0$.

2. $I(p_{\mathbb{A}}, p_{\mathrm{rc}}) = 0$ *gilt genau dann, wenn für alle* $a \in \mathbb{A}$ *und* $b \in \mathbb{B}$ *die Ereignisse »a wurde gesendet« und »b wurde empfangen« stochastisch unabhängig sind.*

3. $I(p_{\mathbb{A}}, p_{\mathrm{rc}}) \leq -\sum_{a \in \mathbb{A}:\, p_{\mathbb{A}}(a) \neq 0} p_{\mathbb{A}}(a) \log_2 p_{\mathbb{A}}(a) =: H(p_{\mathbb{A}})$.

   Die Größe $H(p_{\mathbb{A}})$ *wird als* Entropie der Verteilung $p_{\mathbb{A}}$ *bezeichnet.*

4. $I(p_{\mathbb{A}}, p_{\mathrm{rc}}) = H(p_{\mathbb{A}})$ *gilt genau dann, wenn für jedes* $a \in \mathbb{A}$ *ein* $b \in \mathbb{B}$ *mit* $p_{\mathbb{A}\times\mathbb{B}}(a, b) = 1$ *existiert.*

BEWEIS: Zu 1.: Wir benutzen die Jensen'sche Ungleichung[1] für konvexe Funktionen:

LEMMA 1.10: *Es sei* $f : I \to \mathbb{R}$ *eine auf dem Intervall* I *konvexe Funktion. Dann gilt für* $x_1, \ldots, x_r \in I$ *und* $\lambda_1, \ldots, \lambda_r \in [0, 1]$ *mit* $\lambda_1 + \ldots + \lambda_r = 1$ *die Ungleichung*

$$f(\sum_{i=1}^{r} \lambda_i x_i) \leq \sum_{i=1}^{r} \lambda_i f(x_i).$$

Ist f *strikt konvex und gilt* $\lambda_i > 0$ *für alle* i*, so gilt die Gleichheit genau dann, wenn alle* x_i *gleich sind.*

[1] Johan Ludwig William Valdemar Jensen: dänischer Mathematiker, 1859 – 1925.

Die Funktion $-\log_2(\cdot)$ ist strikt konvex. Damit ergibt sich

$$\begin{aligned}
I(p_{\mathbb{A}}, p_{\mathrm{rc}}) &= \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)\log_2\left(\tfrac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}\right)\\
&= \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)(-\log_2)\left(\tfrac{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}{p_{\mathbb{A}\times\mathbb{B}}(a,b)}\right)\\
&\geq (-\log_2)\Big(\sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)\tfrac{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}{p_{\mathbb{A}\times\mathbb{B}}(a,b)}\Big)\\
&= (-\log_2)\Big(\sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)\Big)\\
&\geq (-\log_2)\Big(\sum_{(a,b)\in\mathbb{A}\times\mathbb{B}} p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)\Big)\\
&= (-\log_2)\Big(\sum_{a\in\mathbb{A}}\sum_{b\in\mathbb{B}} p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)\Big)\\
&= (-\log_2)\Big(\sum_{a\in\mathbb{A}} p_{\mathbb{A}}(a)\sum_{b\in\mathbb{B}} p_{\mathrm{rc}}(b)\Big)\\
&= (-\log_2)\Big(\sum_{a\in\mathbb{A}} p_{\mathbb{A}}(a)\cdot 1\Big)\\
&= -\log_2(1) = 0,
\end{aligned}$$

wobei bei der zweiten Ungleichung benutzt wird, dass $-\log_2(\cdot)$ monoton fallend ist. Insgesamt beweist dies Punkt 1.

Zu 2.: Gilt in der Ungleichung aus Punkt 1 die Gleichheit, so gilt in der ersten Ungleichung des Beweises von Punkt 1 die Gleichheit. Da $-\log_2(\cdot)$ strikt konvex ist, müssen nach Lemma 1.10 alle Werte

$$\frac{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}{p_{\mathbb{A}\times\mathbb{B}}(a,b)}$$

gleich sein. Es gilt also stets $p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b) = cp_{\mathbb{A}\times\mathbb{B}}(a,b)$ mit einer Konstanten $c\in\mathbb{R}$ gilt. Summation über alle $(a,b)\in\mathbb{A}\times\mathbb{B}$ liefert

$$c = \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}} p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b) = 1,$$

woraus die Behauptung folgt – siehe den Beweis von Punkt 1 von Feststellung 1.7.

Gilt andererseits die stochastische Unabhängigkeit der Ereignisse, so ist stets

$$\frac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)} = 1,$$

woraus die Behauptung unmittelbar folgt.

Zu 3.: Es gilt stets $p_{\mathbb{A}\times\mathbb{B}}(a,b) \leq p_{\mathrm{rc}}(b)$, da nach Feststellung 1.4 p_{rc} Randverteilung von $p_{\mathbb{A}\times\mathbb{B}}$ ist. Hieraus folgt wegen der Monotonie des Logarithmus':

$$\begin{aligned} I(p_{\mathbb{A}}, p_{\mathrm{rc}}) &= \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)\log_2\left(\tfrac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathbb{A}}(a)p_{\mathrm{rc}}(b)}\right) \\ &\leq \sum_{(a,b)\in\mathbb{A}\times\mathbb{B}:\, p_{\mathbb{A}\times\mathbb{B}}(a,b)\neq 0} p_{\mathbb{A}\times\mathbb{B}}(a,b)\log_2\left(\tfrac{1}{p_{\mathbb{A}}(a)}\right) \\ &= \sum_{a\in\mathbb{A}:\, p_{\mathbb{A}}(a)\neq 0}\ \sum_{b\in\mathbb{B}} p_{\mathbb{A}\times\mathbb{B}}(a,b)\log_2\left(\tfrac{1}{p_{\mathbb{A}}(a)}\right) \\ &= \sum_{a\in\mathbb{A}:\, p_{\mathbb{A}}(a)\neq 0} p_{\mathbb{A}}(a)\log_2\left(\tfrac{1}{p_{\mathbb{A}}(a)}\right) \\ &= H(p_{\mathbb{A}}). \end{aligned}$$

Zu 4.: Die angegebene Gleichung gilt genau dann, wenn in der im Beweis von Punkt 3 auftretenden Ungleichung die Gleichheit gilt. Dies ist genau dann der Fall, wenn für jedes Paar $(a,b) \in \mathbb{A}\times\mathbb{B}$ mit $p_{\mathbb{A}\times\mathbb{B}}(a,b) \neq 0$ die Gleichung

$$\frac{p_{\mathbb{A}\times\mathbb{B}}(a,b)}{p_{\mathrm{rc}}(b)} = 1$$

gilt. Nach Definition von p_{rc} kann dies bei vorgegebenem a nur für genau ein b gelten, was die Behauptung beweist. □

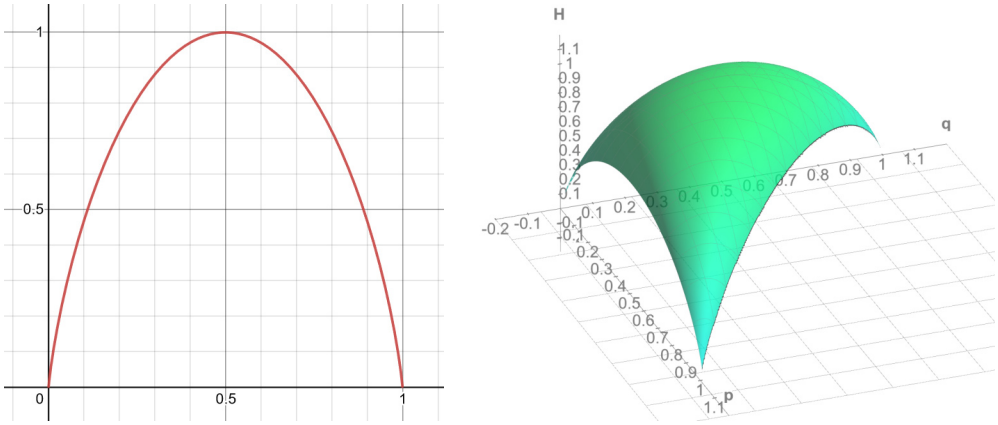


Abbildung 5: Entropiefunktionen für Alphabete mit zwei (links) und drei Symbolen (rechts)

Die Entropie $H(p_{\mathbb{A}})$ ist ein Maß für die Komplexität der Verteilung $p_{\mathbb{A}}$: Je größer ihr Wert ist, desto weniger strukturiert/komplex ist die Verteilung. Es gilt:

FESTSTELLUNG 1.11: *Es sei $W(\mathbb{A})$ die Menge aller Wahrscheinlichkeitsverteilungen auf dem Alphabet $\mathbb{A}$. Die Entropiefunktion*

$$H : W(\mathbb{A}) \to \mathbb{R},\ p_{\mathbb{A}} \mapsto H(p_{\mathbb{A}})$$

besitzt genau ein Maximum und zwar bei der uniformen Verteilung auf $\mathbb{A}$ – siehe Abbildung 5.

BEWEIS: Es sei $N := |\mathbb{A}|$ und $\mathbb{A} = \{a_1, \ldots, a_N\}$, sowie

$$S := \{(x_1, \ldots, x_N) \in [0,1]^N : x_1 + \ldots + x_N = 1\}.$$

Die Abbildung

$$\phi : W(\mathbb{A}) \to S,\ p_{\mathbb{A}} \mapsto (p_{\mathbb{A}}(a_1), \ldots, p_{\mathbb{A}}(a_N))$$

ist eine Bijektion. Man kann also anstelle von H die Abbildung $h := H \circ \phi^{-1}$ auf Maxima untersuchen; diese besitzt S als Definitionsbereich:

$$h : S \to \mathbb{R},\ (x_1, \ldots, x_N) \mapsto -\sum_{x_i \neq 0} x_i \log_2(x_i).$$

Die Menge S ist wegen der Stetigkeit der Addition abgeschlossen und offensichtlich beschränkt, also kompakt. Daher besitzt h ein Maximum.

Die Menge S besitzt allerdings kein offenes Inneres, weswegen man das Maximum von h nicht über die notwendige Bedingung $h'(x_1, \ldots, x_N) = 0$ bestimmen kann. Eine Möglichkeit der Maximumsbestimmung ist die Verwendung von Lagrange-Multiplikatoren, also der Theorie von Extrema unter Nebenbedingungen. Die hier vorliegende Nebenbedingung

$$x_N = \sum_{i=1}^{N-1} x_i$$

kann man allerdings auch direkt nutzen, um die Funktion h als Funktion von $N-1$ Variablen aufzufassen:

$$\begin{array}{rcl} h : S' & \to & \mathbb{R} \\ (x_1, \ldots, x_{N-1}) & \mapsto & \begin{cases} -(\sum\limits_{x_i \neq 0}^{N-1} x_i \log_2(x_i) + (1 - \sum\limits_{i=1}^{N-1} x_i) \log_2(1 - \sum\limits_{i=1}^{N-1} x_i)) & \text{falls } \sum\limits_{i=1}^{N-1} x_i \neq 1 \\ -(\sum\limits_{x_i \neq 0}^{N-1} x_i \log_2(x_i)) & \text{falls } \sum\limits_{i=1}^{N-1} x_i = 1, \end{cases} \end{array}$$

wobei

$$S' := \{(x_1, \ldots, x_{N-1}) \in [0,1]^{N-1} : \sum_{i=1}^{N-1} x_i \leq 1\}.$$

Die Fälle $N = 2$ und $N = 3$ sind in Abbildung 5 dargestellt.

Maxima von h können im Inneren von S' liegen, in welchem Fall man sie mittels Differentialrechnung ermitteln kann, oder auf dem Rand von S, ein Fall der gesondert betrachtet werden muss.

Wir beweisen, dass h genau ein Maximum im Inneren von S' besitzt, nämlich bei $x_k := \frac{1}{N}$ und per Induktion nach N, dass es auf dem Rand von S' keine Maxima gibt.

Im Inneren von S' gilt:

$$\begin{aligned} \frac{\partial h}{\partial x_k} &= -(\tfrac{1}{\ln(2)}(\ln(x_k)+1) + (-1)\tfrac{1}{\ln(2)}\ln(1 - \sum_{i=1}^{N-1} x_i) + \tfrac{1}{\ln(2)}(1 - \sum_{i=1}^{N-1} x_i)\tfrac{1}{(1-\sum_{i=1}^{N-1} x_i)}(-1)) \\ &= -\tfrac{1}{\ln(2)}(\ln(x_k) - \ln(1 - \sum_{i=1}^{N-1} x_i)). \end{aligned}$$

Die notwendigen Bedingungen $\frac{\partial h}{\partial x_k} = 0$ für das Vorliegen eines lokalen Maximums liefern die Gleichungen

$$\ln(x_k) = \ln(1 - \sum_{i=1}^{N-1} x_i),$$

womit $x_k = c \in (0,1)$ für $k \in \{1, 2, \ldots, N-1\}$ und daher $c = 1 - (N-1)c$ gelten muss. Es folgt $c = \frac{1}{N}$.

Für $\ell \neq k$ ist

$$\frac{\partial^2 h}{\partial x_k x_\ell} = -\tfrac{1}{\ln(2)} x_\ell (1 - \sum_{i=1}^{N-1} x_i)^{-1},$$

und für $\ell = k$

$$\frac{\partial^2 h}{\partial x_k^2} = -\tfrac{1}{\ln(2)}(\tfrac{1}{x_k} + x_k(1 - \sum_{i=1}^{N-1} x_i)^{-1}).$$

Damit ergibt sich für die Hesse-Matrix am ermittelten stationären Punkt

$$H(\tfrac{1}{N}, \ldots, \tfrac{1}{N}) = -\tfrac{1}{\ln(2)} \begin{pmatrix} N+1 & 1 & 1 & \cdots & 1 \\ 1 & N+1 & 1 & \cdots & 1 \\ 1 & 1 & N+1 & \cdots & 1 \\ \vdots & \vdots & \cdots & \cdots & \vdots \\ 1 & 1 & \cdots & 1 & N+1 \end{pmatrix}.$$

Die Matrix ohne den Vorfaktor ist symmetrisch mit positiven Diagonalelementen und strikt diagonaldominant, folglich positiv definit. Daher ist die Matrix inklusive Vorfaktor negativ definit und es liegt ein Maximum vor.

Der Funktionswert im Maximum ist

$$h(\frac{1}{N}, \ldots, \frac{1}{N}) = \log_2(N).$$

Nun ist noch der Rand von S' zu betrachten. Diesen kann man wie folgt schreiben:

$$\text{Rand}(S') = S'_1 \cup S'_2 \cup \ldots \cup S'_{N-1} \cup S'_N,$$

wobei S'_k, $k \in \{1, 2, \ldots, N-1\}$, die Menge aller $x \in S'$ mit $x_k = 0$ ist. Die Menge S'_N besteht aus allen $x \in S'$ mit $\sum_{i=1}^{N-1} x_i = 1$. Damit gilt aber Folgendes: Jedes S_k entspricht der Menge aller Wahrscheinlichkeitsverteilungen auf einem Alphabet mit $N-1$ Symbolen. Damit kann man induktiv annehmen, dass h auf S_k ein globales Maximum bei $(\frac{1}{N-1}, \ldots, \frac{1}{N-1})$ besitzt. Sein Funktionswert ist

$$\log_2(N-1) < \log_2(N),$$

was beweist, dass im Fall von N Symbolen $(\frac{1}{N}, \ldots, \frac{1}{N})$ ein globales Maximum ist.

Es fehlt der Induktionsanfang bei $N = 2$. Dieser ist trivial – siehe Abbildung 5 links. □

Um etwa experimentell zu bestimmen, welche Kapazität ein Übertragungskanal besitzt, muss man die Empfangsqualität bei der Übertragung möglichst komplexer Wörter ermitteln. Dies ist vergleichbar mit der Bestimmung des Durchmessers eines in der Erde verlegten, und daher unzugänglichen Wasserrohrs: Will man seinen Durchmesser experimentell durch Hindurchleiten von Wasser ermitteln, so nützt es nichts ein Rinnsal durchs Rohr zu schicken, sondern man muss soviel Wasser wie möglich einleiten.

Analog verschickt ein Börsenhändler weniger komplexe Texte an seinen Agenten an der Börse als ein Romanautor an seinen Verlag. Der verwendete Übertragungskanal kann aber derselbe sein. Die Verteilung $p_{\mathbb{A}}$ modelliert die Komplexität der Sendewörter, daher wird man zur Definition der Kapazität das Supremum über alle Verteilungen auf $\mathbb{A}$ heranziehen:

Definition 1.12: *Als Kapazität eines Übertragungskanals (inklusive Dekodierer) bezeichnet man die Größe*

$$C := \sup(I(p_{\mathbb{A}}, p_{\text{rc}}) : p_{\mathbb{A}} \in W(\mathbb{A})).$$

BEMERKUNG: Die Kapazität C ist endlich: Nach Satz 1.9, Punkt 3 ist $I(p_{\mathbb{A}}, p_{\mathrm{rc}}) \leq H(p_{\mathbb{A}})$. Die Entropie lässt sich aber wie folgt nach oben abschätzen:

$$\begin{aligned} H(p_{\mathbb{A}}) &= \sum_{a\in\mathbb{A}:p_{\mathbb{A}}(a)\neq 0} p_{\mathbb{A}}(a)\log_2(\tfrac{1}{p_{\mathbb{A}}(a)}) \\ &= \sum_{a\in\mathbb{A}:p_{\mathbb{A}}(a)\neq 0} p_{\mathbb{A}}(a)\tfrac{\ln(\frac{1}{p_{\mathbb{A}}(a)})}{\ln(2)} \\ &\leq \sum_{a\in\mathbb{A}:p_{\mathbb{A}}(a)} p_{\mathbb{A}}(a)\tfrac{\frac{1}{p_{\mathbb{A}}(a)}}{\ln(2)} \leq \tfrac{|\mathrm{A}|}{\ln(2)}. \end{aligned}$$

Als Anwendung betrachten wir einen für die Praxis wichtigen Übertragungskanal, der in dieser Vorlesung eine zentrale Rolle spielt:

DEFINITION 1.13: *Den Übertragungskanal mit den Alphabeten* $\mathbb{A} = \{0,1\} = \mathbb{B}$ *und den bedingten Wahrscheinlichkeiten*

$$p_{\mathrm{rc}}(b = 1|a = 0) = p_0 = p_{\mathrm{rc}}(b = 0|a = 1)$$

mit einem $p_0 \in [0,1]$ *nennt man den binären, symmetrischen gedächtnislosen Übertragungskanal (englisch: binary symmetric memoryless channel – BSMC) mit Bitfehlerwahrscheinlichkeit (englisch: bit error rate – BER)* p_0.

Um seine Kapazität zu berechnen, bestimmt man zunächst die Verteilungen $p_{\mathbb{A}\times\mathbb{B}}$ und p_{rc} zu einer gegebenen Verteilung $p_{\mathbb{A}}$:

$$p_{\mathbb{A}}(0) = q,\ p_{\mathbb{A}}(1) = 1 - q,\ q \in [0,1].$$

Nach Definition gelten dann

$$\begin{aligned} p_{\mathbb{A}\times\mathbb{B}}(0,0) &= q(1-p_0), \\ p_{\mathbb{A}\times\mathbb{B}}(0,1) &= qp_0, \\ p_{\mathbb{A}\times\mathbb{B}}(1,0) &= (1-q)p_0, \\ p_{\mathbb{A}\times\mathbb{B}}(1,1) &= (1-q)(1-p_0). \end{aligned}$$

Daraus ergibt sich

$$\begin{aligned} p_{\mathrm{rc}}(0) &= q(1-p_0) + (1-q)p_0, \\ p_{\mathrm{rc}}(1) &= qp_0 + (1-q)(1-p_0). \end{aligned}$$

Dies liefert im Fall $p_0 \neq 0$, $p_0 \neq 1$:

$$\begin{aligned} I(p_{\mathbb{A}}, p_{\mathrm{rc}}) &= q(1-p_0)\log_2(\tfrac{1-p_0}{q(1-p_0)+(1-q)p_0}) + qp_0\log_2(\tfrac{p_0}{qp_0+(1-q)(1-p_0)}) \\ &\quad +(1-q)p_0\log_2(\tfrac{p_0}{q(1-p_0)+(1-q)p_0}) + (1-q)(1-p_0)\log_2(\tfrac{1-p_0}{qp_0+(1-q)(1-p_0)}) \\ &= q(1-p_0)\log_2(1-p_0) - (q(1-p_0)+(1-q)p_0)\log_2(q(1-p_0)+(1-q)p_0) \\ &\quad +qp_0\log_2(p_0) - (qp_0+(1-q)(1-p_0))\log_2(qp_0+(1-q)(1-p_0)) \\ &\quad +(1-q)p_0\log_2(p_0) + (1-q)(1-p_0)\log_2(1-p_0) \\ &= (1-p_0)\log_2(1-p_0) + p_0\log_2(p_0) \\ &\quad -(q(1-p_0)+(1-q)p_0)\log_2(q(1-p_0)+(1-q)p_0) \\ &\quad -(qp_0+(1-q)(1-p_0))\log_2(qp_0+(1-q)(1-p_0)). \end{aligned}$$

Man erkennt, dass $I(p_{\mathbb{A}}, p_{\mathrm{rc}})$ eine differenzierbare Funktion von q ist, dem Parameter also, der die Verteilung $p_{\mathbb{A}}$ festlegt. Die Kapazität des BSMC lässt sich damit durch Differenzieren berechnen. Hierzu substituiert man

$$t := q(1-p_0) + (1-q)p_0$$

und nutzt die Gleichung

$$qp_0 + (1-q)(1-p_0) = 1 - t.$$

Es folgt

$$I(p_{\mathbb{A}}, p_{\mathrm{rc}}) = c - t\log_2(t) - (1-t)\log_2(1-t)$$

mit einer Konstanten $c \in \mathbb{R}$, und damit

$$\frac{dI(p_{\mathbb{A}}, p_{\mathrm{rc}})}{dt} = -\log_2(t) - \frac{t}{\ln(2)t} + \log_2(1-t) + \frac{1-t}{\ln(2)(1-t)} = \log_2(1-t) - \log_2(t).$$

Da die Funktion $\log_2(\cdot)$ injektiv ist, folgt aus $\log_2(1-t) - \log_2(t) = 0$ die Gleichung $1 - t = t$ und damit $t = \frac{1}{2}$, also auch $q = \frac{1}{2}$.

Es gilt

$$\frac{d^2 I(p_{\mathbb{A}}, p_{\mathrm{rc}})}{dt^2} = -\frac{1}{\ln(2)(1-t)} - \frac{1}{\ln(2)t},$$

womit bei $t = \frac{1}{2}$ tatsächlich ein Maximum von $I(p_{\mathbb{A}}, p_{\mathrm{rc}})$ vorliegt.

Insgesamt wurde bewiesen:

Satz 1.14: *Für die Kapazität des BSMC mit Fehlerwahrscheinlichkeit $p_0 \in (0,1)$ gilt*

$$C = 1 + p_0\log_2(p_0) + (1-p_0)\log_2(1-p_0).$$

Bemerkungen:

1. Die Fehlerwahrscheinlichkeit p_0 definiert eine Wahrscheinlichkeitsverteilung p auf der Menge $\{0,1\}$ durch $p(0) = 1 - p_0$ und $p(1) = p_0$. Es wird also 1 als »Übertragungsfehler« und 0 als »kein Übertragungsfehler« interpretiert. Dann gilt für die Entropie von p nach Definition

$$H(p) = -(p_0 \log_2(p_0) + (1 - p_0) \log_2(1 - p_0))$$

und man schreibt auch $H(p_0)$ anstelle von $H(p)$. Die Kapazität eines BSMC ist also $C = 1 - H(p_0)$.

2. Da $\lim\limits_{t \to 0+} t \log_2(t) = 0$, ist im Fall $p_0 = 0$ die Kanalkapazität gleich 1. Im Fall $p_0 = \frac{1}{2}$ ergibt sich als minimaler Wert der Kanalkapazität

$$C = 1 - \frac{1}{2} - \frac{1}{2} = 0.$$

3. Die Kapazitätsfunktion ist achsensymmetrisch zur Geraden $p_0 = \frac{1}{2}$.

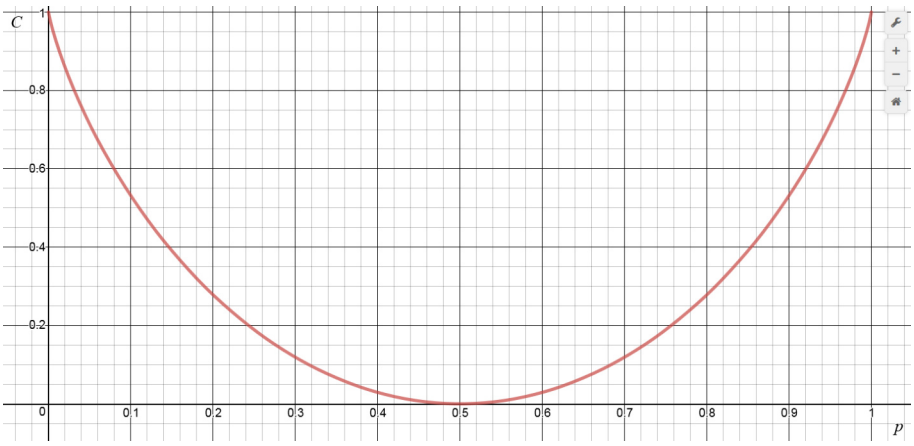


Abbildung 6: Kapazität des BSMC

1.4 Der Raum der Binärwörter fester Länge

In der Informationstechnik ist es inzwischen ein Standard Information *binär* zu digitalisieren, das heißt unter Verwendung eines Alphabets, das nur zwei Symbole besitzt. Üblicherweise werden die Symbole 0 und 1 genutzt, wobei diese *nicht* für die entsprechenden reellen Zahlen stehen.

Definition 1.15: *Die zweielementige Menge* $\{0,1\}$ *wird im Weiteren mit* $\mathbb{F}_2$ *bezeichnet. Ein Element von* $\mathbb{F}_2$ *nennt man auch ein Bit.*

Binäre Digitalisierung führt nun nicht etwa zur Abschaffung aller anderen Alphabete, die man zur Digitalisierung verwenden kann. Vielmehr werden die Symbole eines gegebenen Alphabets $\mathbb{A}$ bei binärer Digitalisierung und vor der Weiterverarbeitung der Information zunächst in Wörter über dem Alphabet $\mathbb{F}_2$ übersetzt. Mathematisch geschieht dies durch eine injektive Abbildung

$$\alpha : \mathbb{A} \to \mathbb{F}_2^m$$

in die Menge $\mathbb{F}_2^m$ der Wörter der Länge m über $\mathbb{F}_2$. Die Wortlänge m ist geeignet zu wählen. Man bezeichnet α als *Alphabetwechselabbildung*. Man beachte, dass α nicht surjektiv sein muss. Ein bekanntes Beispiel einer solchen Abbildung ist der weltweit auf Computern verwendete UTF-8-Kode (früher ASCII-Kode), also die Darstellung der im europäischen Sprachraum verwendeten Buchstaben und Sonderzeichen als Elemente von $\mathbb{F}_2^8$.

Symbol	Kodewort
A	01000001
B	01000010
a	01100001
b	01100010
+	00101011

Abbildung 7: Beispiele von UTF-8-Kodewörtern

Die binären Darstellungen $\alpha(a) \in \mathbb{F}_2^m$ der Symbole $a \in \mathbb{A}$ werden durch den Kodierer im Sender-Empfänger-Szenario (Abbildung 4) in Wörter der Länge $\ell > m$ transformiert. Hierfür verwendet man eine geeignete injektive Abbildung $i : \mathbb{F}_2^m \to \mathbb{F}_2^\ell$. Die Verkettung $i \circ \alpha : \mathbb{A} \to \mathbb{F}_2^\ell$ wird dann als Kodierungsabbildung bezeichnet – siehe Abschnitt 2.

Die Menge $\mathbb{F}_2^\ell$ kann mit verschiedenen, nützlichen mathematischen Strukturen versehen werden; die erste hier relevante ist eine Metrik:

FESTSTELLUNG 1.16: *Die Abbildung*

$$h : \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \{0, 1, \ldots, \ell\},\ ((x_1, \ldots, x_\ell), (y_1, \ldots, y_\ell)) \mapsto |\{k : x_k \neq y_k\}|$$

ist eine Metrik.

BEWEIS: Die Reflexivität und die Symmetrie der Abbildung h sind offensichtlich. Es bleibt also die Dreiecksungleichung zu beweisen. Es seien $(x_1, \ldots, x_\ell), (y_1, \ldots, y_\ell), (z_1, \ldots, z_\ell) \in \mathbb{F}_2^\ell$ und es gelte $x_k \neq z_k$. Dann muss entweder $x_k \neq y_k$ oder $y_k \neq z_k$ gelten, was nach Definition von h die Dreiecksungleichung bereits beweist. □

Die Metrik h wird zu Ehren des amerikanischen Mathematikers Richard Hamming (1915 – 1998) als Hamming-Metrik bezeichnet. Mit der 1950 im *Bell System Technical Journal* veröffentlichten Arbeit *Error detecting and error correcting codes* zählt Hamming zu den Begründern der Theorie der fehlerkorrigierenden Kodes.

Abbildung 8: Richard Wesley Hamming 1938 und ca. 1980
(Links: Copyright unbekannt; rechts: Courtesy of the Naval Postgraduate School)

Die in Abbildung 8 links gezeigte Fotographie von Richard Hamming aus dem Jahr 1938 wurde der Webseite zum digitalen Archiv der University of Illinois (`https://archon.library.illinois.edu`) entnommen, wo Hamming im Jahr 1942 mit

einer Arbeit über Randwertprobleme linearer Differentialgleichungen promovierte. Von 1945 bis 1946 arbeitete er im so genannten Manhattan-Projekt in Los Alamos an der Entwicklung der Atombombe mit. Ab 1946 und bis 1976 war er als Mathematiker bei den Bell Laboratories, der Forschungsabteilung von AT&T Bell Telephones (heute Nokia), tätig. Neben Kodierungstheorie zählten auch die numerische Analysis und die damals noch nicht so bezeichnete Informatik zu seinen Arbeitsgebieten. Ab 1976 bis zu seinem Tod lehrte Hamming als Professor für Computer Science an der Naval Postgraduate School in Monterey, Kalifornien, von deren Webseite auch das rechts zu sehende Bild aus den 1980er Jahren stammt. Er schrieb eine Reihe von Büchern über Mathematik, Ingenieurwissenschaft etc., in denen er jeweils versuchte einen unkonventionellen Zugang zu dem Gebiet zu vermitteln.

DEFINITION 1.17: *Es sei $x \in \mathbb{F}_2^\ell$ und $r \geq 0$. Die abgeschlossene Kugel mit Mittelpunkt x und Radius r im metrischen Raum $(\mathbb{F}_2^\ell, h)$ ist durch*

$$B[x,r] := \{y \in \mathbb{F}_2^\ell : h(y,x) \leq r\} \tag{11}$$

definiert.

Die Elementezahl abgeschlossener Kugeln wird in dieser Vorlesung immer wieder benötigt:

FESTSTELLUNG 1.18: *Für alle $x \in \mathbb{F}_2^\ell$ und $r \in \{0,1,\ldots,\ell\}$ gilt:*

$$|B[x,r]| = \sum_{i=0}^{r} \binom{\ell}{i}. \tag{12}$$

BEWEIS: Um x in ein Element y mit $h(x,y) = i \leq r$ umzuwandeln, muss man x an genau i Komponenten verändern, was auf $\binom{\ell}{i}$ verschiedene Weisen möglich ist. □

Die Menge $\mathbb{F}_2^\ell$ trägt auch eine algebraische Struktur, die wir später intensiv nutzen werden:

FESTSTELLUNG 1.19: *Die Menge $\mathbb{F}_2 = \{0,1\}$ wird zu einem Körper, wenn man die Addition und die Multiplikation so definiert, dass 0 beziehungsweise 1 das jeweilige neutrale Element ist:*

$$0+0=0=1+1,\ 0+1=1+0=1,$$

$$0\cdot 0=0,\ 1\cdot 0=0=0\cdot 1,\ 1\cdot 1=1.$$

Die Menge $\mathbb{F}_2^\ell$ wird zu einem Vektorraum über dem Körper $\mathbb{F}_2$, wenn man die Addition und die skalare Multiplikation komponentenweise definiert.

Die Dimension von $\mathbb{F}_2^\ell$ ist dann gleich ℓ.

BEMERKUNGEN:

1. Elemente von $\mathbb{F}_2^\ell$ werden aus Platzgründen häufig in Zeilenform notiert, wie zum Beispiel $(0,1,0,1,1)^t$. Hier bezeichnet ^{t} die Operation des Transponierens.

2. Der Beweis der Feststellung besteht in dem hier sehr einfachen aber etwas langwierigen Nachprüfen der Körper- und Vektorraumaxiome. Die Aussage zur Dimension folgt aus der Tatsache, dass die Vektoren

$$e_1 := (1,0,\ldots,0)^t, e_2 := (0,1,0,\ldots,0)^t, \ldots, e_\ell := (0,0,\ldots,1)^t \quad (13)$$

   ein linear unabhängiges Erzeugendensystem bilden.

3. Der Vektor $(0,\ldots,0)^t$ ist das neutrale Element der Gruppe $(\mathbb{F}_2^\ell, +)$.

4. Man beachte die etwas gewöhnungsbedürftige Tatsache, dass in $\mathbb{F}_2^\ell$ stets $x + x = 0$ also $x = -x$ gilt.

Da es für den Vektorraum $\mathbb{F}_2^\ell$ nur zwei Skalare gibt, gilt die folgende etwas erstaunliche Tatsache:

FESTSTELLUNG 1.20: *Eine Teilmenge $U \subseteq \mathbb{F}_2^\ell$ ist genau dann ein Untervektorraum, wenn U eine Untergruppe der Gruppe $(\mathbb{F}_2^\ell, +)$ ist.*

In jedem Untervektorraum $U \subseteq \mathbb{F}_2^\ell$ gibt es endlich viele Elemente $u_1, \ldots, u_r$, $r \leq \ell$, derart, dass jedes $u \in U$ sich in eindeutiger Weise als Summe einiger der u_i darstellen lässt:

$$u = u_{i_1} + \ldots + u_{i_s}$$

mit eindeutig bestimmten $i_1, \ldots, i_s$.

BEWEIS: Ein Untervektorraum U eines Vektorraums V über einem Körper K ist nach Definition eine Untergruppe der additiven Gruppe $(V, +)$ mit der Eigenschaft $K \cdot U \subseteq U$.

Sei nun $U \subseteq \mathbb{F}_2^\ell$ eine Untergruppe von $(\mathbb{F}_2^\ell, +)$. Dann gelten für jedes $u \in U$ die Gleichungen $0 \cdot u = 0 \in U$ und $1 \cdot u = u \in U$, also $\mathbb{F}_2 \cdot U \subseteq U$.

Ein Untervektorraum U eines Vektorraums V der Dimension ℓ besitzt selbst eine Dimension $r \leq \ell$. Folglich besitzt ein Untervektorraum $U \subseteq \mathbb{F}_2^\ell$

eine Dimension $r \leq \ell$. Die verbleibende Aussage ist klar, wenn man für $u_1, \ldots, u_r$ eine Basis von U wählt. $\square$

Um ein Gefühl für die Geometrie in $\mathbb{F}_2^\ell$ zu bekommen, werden im Folgenden einige ausgewählte Eigenschaften dieses Vektorraums zusammengestellt:

- Zwei Vektoren $x \neq 0$ und $y \neq 0$ sind genau dann linear unabhängig, wenn sie verschieden sind.
- Ein 1-dimensionaler Untervektorraum U besitzt zwei Elemente: $U = \{0, x\}$, $x \neq 0$.

  Jede Teilmenge dieser Form ist ein 1-dimensionaler Untervektorraum. Insbesondere gibt es also $2^\ell - 1$ verschiedene solche Untervektorräume.
- Die Geraden in $\mathbb{F}_2^\ell$ sind genau die 2-elementigen Teilmengen von $\mathbb{F}_2^\ell$, insbesondere gibt es

  $$\binom{2^\ell}{2} = \frac{2^\ell!}{2!(2^\ell - 2)!} = 2^{\ell-1}(2^\ell - 1)$$

  Geraden.
- Ein 2-dimensionaler Untervektorraum U besitzt vier Elemente: $U = \{0, x, y, x + y\}$ mit $x \neq 0$, $y \neq 0$, $x \neq y$.

  Jede Teilmenge dieser Form ist ein 2-dimensionaler Untervektorraum.
- Die Ebenen in $\mathbb{F}_2^\ell$ sind genau die 4-elementigen Teilmengen von $\mathbb{F}_2^\ell$ der Form $\{z, x + z, y + z, x + y + z\}$.

Im Weiteren werden auch lineare Abbildungen $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ eine Rolle spielen. Hierzu einige Bemerkungen:

- Die Abbildung $L : \mathbb{F}_2^n \to \mathbb{F}_2^m$ ist genau dann linear, wenn sie additiv ist, wenn also $L(x + y) = L(x) + L(y)$ für alle $x, y \in \mathbb{F}_2^n$ gilt.
- Wie für die rationalen, reellen oder komplexen Zahlen kann man die Menge $\mathbb{F}_2^{m \times n}$ der Matrizen mit Koeffizienten in $\mathbb{F}_2$ definieren. Diese können koeffizientenweise addiert und mit Skalaren multipliziert werden. Eine Matrix $A \in \mathbb{F}_2^{m \times n}$ und eine Matrix $B \in \mathbb{F}_2^{n \times p}$ können wie im Fall von Zahlen als Koeffizienten miteinander multipliziert werden. Für das Produkt gilt: $AB \in \mathbb{F}_2^{m \times p}$.

Die Rechengesetze für diese Matrixoperationen sind dieselben wie im Fall von $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, da für den Beweis ihrer Gültigkeit nur die Axiome eines Körpers genutzt werden.

- Wählt man Basen $b_1, \ldots, b_n \in \mathbb{F}_2^n$ und $c_1, \ldots, c_m \in \mathbb{F}_2^m$, so kann man L durch eine Matrix $A \in \mathbb{F}_2^{m \times n}$ darstellen: Ist $x = \sum_{i=1}^{n} x_i b_i$, so gilt $L(x) = \sum_{j=1}^{m} y_j c_j$ mit

$$(y_1, \ldots, y_m)^t = A(x_1, \ldots, x_n)^t.$$

- Ist im letzten Punkt $n = m$, so ist L bijektiv genau dann, wenn A eine invertierbare Matrix ist, wenn also eine Matrix $B \in \mathbb{F}_2^{n \times n}$ mit $AB = BA = E$ existiert, wobei $E = (e_{ij})$ mit $e_{ii} = 1$ und $e_{ij} = 0$ für $i \neq j$ gilt.

Beispiel 1.21: Wir betrachten lineare Abbildungen $L : \mathbb{F}_2^2 \to \mathbb{F}_2^2$. Eine solche Abbildung ist eindeutig festgelegt, wenn man die Bilder $L(b_1)$, $L(b_2)$ einer Basis von $\mathbb{F}_2^2$ festlegt. Eine solche Basis ist zum Beispiel $b_1 = (1, 0)^t$ und $b_2 = (0, 1)^t$. Da man jedes der Elemente $L(b_1)$, $L(b_2)$ unabhängig voneinander auf vier verschiedene Weisen wählen kann, gibt es insgesamt 16 lineare Abbildungen $L : \mathbb{F}_2^2 \to \mathbb{F}_2^2$.

Eine lineare Abbildung L ist bijektiv, falls die Vektoren $L(b_1)$, $L(b_2)$ linear unabhängig sind. Wie früher festgestellt ist dies genau dann der Fall, wenn $L(b_1) \neq L(b_2)$ gilt und keiner der beiden Vektorren der Nullvektor ist. Folglich kann man $L(b_1)$ auf drei verschiedene Weisen und nachfolgend $L(b_2)$ auf zwei verschiedene Weisen wählen. Insgesamt gibt es also $3 \cdot 2 = 6$ invertierbare lineare Abbildungen $L : \mathbb{F}_2^2 \to \mathbb{F}_2^2$.

Wählt man die Standardbasis auch im Wertebereich von L, so ergibt sich die zu einer linearen Abbildung L bezüglich dieser Basiswahl gehörende Matrix A zu

$$A = [L(b_1)\ L(b_2)].$$

Kombiniert man dies mit den Überlegungen zur Invertierbarkeit von L, so erhält man alle invertierbaren Matrizen $A \in \mathbb{F}_2^{2 \times 2}$:

$$A_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ A_2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ A_3 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ A_4 = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix},$$

$$A_5 = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ A_6 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Die Menge der invertierbaren $n \times n$-Matrizen $\mathrm{GL}(n, K)$ mit Koeffizienten in einem Körper K bilden stets eine Gruppe bezüglich der Matrixmultiplikation. Im vorliegenden Fall ist $\mathrm{GL}(2, \mathbb{F}_2) \subset \mathbb{F}_2^{2\times 2}$ eine nicht-abelsche Gruppe mit 6 Elementen also isomorph zur Permutationsgruppe S_3: Die bijektiven linearen Abbildungen $L : \mathbb{F}_2^2 \to \mathbb{F}_2^2$ permutieren nämlich die drei vom Nullvektor verschiedenen Elemente.

Für Matrizen $A \in \mathbb{F}_2^{2\times 2}$ vom Rang 1 gilt: Entweder sind beide Spalten gleich und ungleich 0 oder eine Spalte ist 0 und die zweite nicht. Folglich gibt es $3 + 3 + 3 = 9$ solche Matrizen. ◇

Die Hamming-Metrik ist mit den Rechenoperationen in dem Vektorraum $\mathbb{F}_2^\ell$ verträglich:

Feststellung 1.22: *Für die Hamming-Metrik gilt*

$$\forall x, y \in \mathbb{F}_2^\ell \quad h(x, y) = h(x - y, 0),$$

wobei 0 *den Nullvektor* $(0, \ldots, 0)^t$ *bezeichnet.*

Die Abbildung

$$w : \mathbb{F}_2^\ell \to \{0, 1, \ldots, \ell\},\ x \mapsto h(x, 0) =: w(x)$$

wird als Hamming-Norm oder Gewichtsfunktion bezeichnet. Sie besitzt zwei von drei Eigenschaften einer Normfunktion, wie sie aus der reellen Analysis bekannt sind:

1. $\forall x \in \mathbb{F}_2^\ell \quad w(x) = 0 \Leftrightarrow x = 0$,
2. $\forall x, y \in \mathbb{F}_2^\ell \quad w(x + y) \leq w(x) + w(y)$.

Alle in der Feststellung aufgeführten Behauptungen sind einfach und direkt nachprüfbar. Sie werden daher den Leser:innen als Übung überlassen.

Als eine wichtige Konsequenz aus Feststellung 1.22 ergibt sich die Homogenität des metrischen Raums $(\mathbb{F}_2^\ell, h)$:

$$\forall r > 0, x \in \mathbb{F}_2^\ell \quad B[x, r] = x + B[0, r]. \tag{14}$$

Die abgeschlossenen Kugeln ergeben sich durch Translation aus den abgeschlossenen Kugeln mit Mittelpunkt 0.

In Abbildung 9 ist der metrische Raum $\mathbb{F}_2^5$ dargestellt. Die Elemente erscheinen als Kreisscheiben und sind mit einer Linie verbunden genau dann, wenn ihr Hamming-Abstand gleich 1 ist. Allgemein ist der Hamming-Abstand zweier Elemente in der Darstellung gleich der Anzahl der auf dem kürzesten Weg zwischen den beiden Elementen durchlaufenen weiteren Elemente, wobei das Startelement nicht mitzählt. Dargestellt sind auch die Kugeln $B[0,1]$ (orangefarben) und $B[(1,0,1,0,1),1]$ (grün).

Die Darstellung wird der hohen Symmetrie dieses Raums nicht gerecht: $\mathbb{F}_2^5$ kann als Menge der Ecken eines Würfels mit Kantenlänge 1 im 5-dimensionalen Raum $\mathbb{R}^5$ aufgefasst werden. Leider gibt es für diesen Würfel keine entsprechend symmetrische, 2-dimensionale Darstellung.

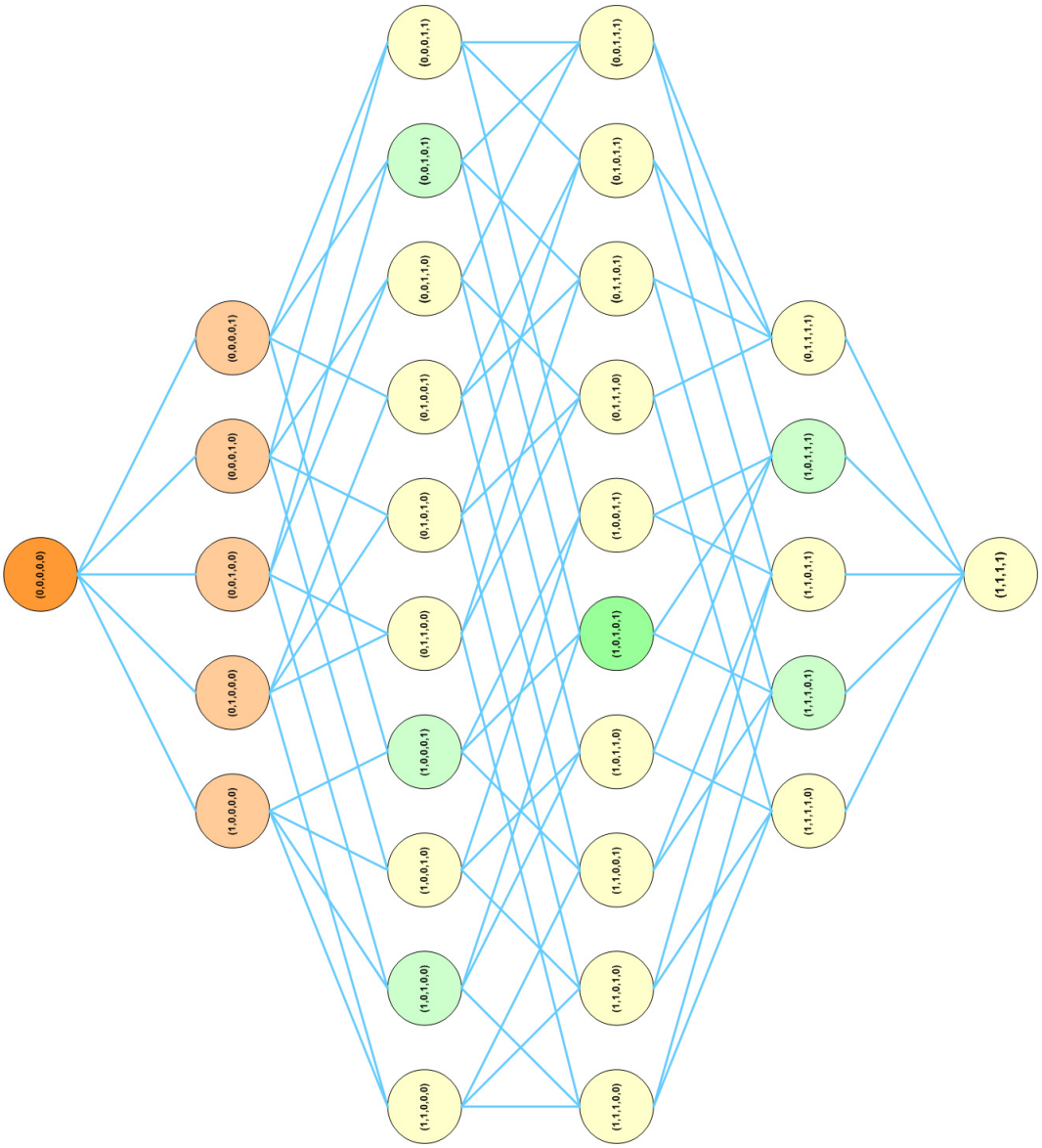


Abbildung 9: Der metrische Raum $\mathbb{F}_2^5$ und zwei Kugeln vom Radius 1.

2 Binäre Blockkodes

Nachdem im vorigen Kapitel für die Theorie fehlerkorrigierender Kodes grundlegende Begriffe aus der Informationstheorie im Fall digital vorliegender Information diskutiert wurden, werden im vorliegenden Kapitel die im Sender-Empfänger-Szenario auftretenden Entitäten »Kodierer« und »Dekodierer« mathematisch definiert. Weiter werden die Ergebnisse des Abschnitts 1.3 verwendet um das Grundproblem der Kodierungstheorie präzise zu formulieren. Schließlich werden Hadamard-Kodes und perfekte Kodes als Beispielklassen diskutiert, sowie die Maximum-Likelihood-Dekodierung als ein universell verwendbarer Dekoder eingeführt.

2.1 Das Grundproblem der Kodierungstheorie

Wir betrachten das Sender-Empfänger-Szenario bei binärer Digitalisierung wie sie im Abschnitt 1.4 eingeführt wurde:

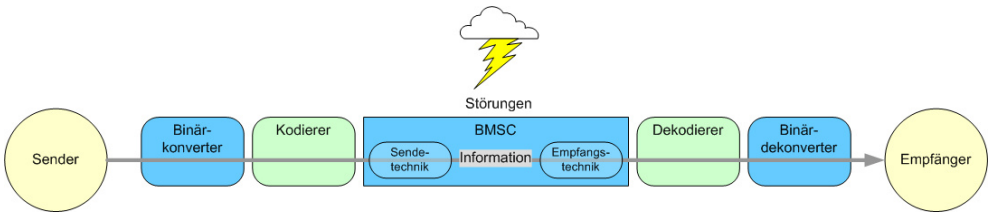


Abbildung 10: Sender-Empfänger-Szenario bei binärer Digitalisierung

1. Ein Sender erzeugt Information, die nicht notwendig in digitaler Form vorliegt.

2. Die vom Sender erzeugte Information wird durch einen Binärkonverter binär digitalisiert. Wie dies genau geschieht hängt vom Kontext ab. Im Rahmen dieser Vorlesung ist es ausreichend sich den Digitalisierungsprozess wie folgt vorzustellen: Liegt die zu übertragende Information nicht digital vor, so wird sie unter Zuhilfenahme eines Alphabets $\mathbb{A}$ digitalisiert. Danach wird ein Alphabetwechsel $\alpha : \mathbb{A} \to \mathbb{F}_2^m$ durchgeführt.

3. Im Kodierer wird die Sendeinformation symbolweise kodiert, indem jedem Symbol $\alpha(a) \in \mathbb{F}_2^m$ ein eindeutig bestimmtes Wort $c(\alpha(a)) \in \mathbb{F}_2^\ell$

zugewiesen wird. Die Länge ℓ der verwendeten Wörter ist unabhängig vom jeweiligen Symbol, es liegt also eine injektive Abbildung

$$c : \alpha(\mathbb{A}) \to \mathbb{F}_2^\ell$$

vor. Der Sinn dieser Operation besteht darin, Übertragungsfehler erkenn- und eventuell auch korrigierbar zu machen. Stets ist $\ell \geq m$.

4. Die kodierte Information wird über einen binären, symmetrischen, gedächtnislosen Kanal (BSMC) an einen Empfänger geschickt.

5. Beim Passieren des Übertragungskanals werden die einzelnen Bits der kodierten Information mit der Wahrscheinlichkeit p_0 gestört. Es können zwei Arten von Störungen auftreten:

   - *Einzelfehler*: Ein einzelnes Bit wird gestört; die »umgebenden« Bits sind ungestört.
   - *Salvenfehler* (engl.: burst error): Eine zusammenhängende Gruppe von Bits wird gestört.

   Salvenfehler werden im Weiteren nicht behandelt: Es wird stets angenommen, dass die Störereignisse für einzelne Bits in einem Wort stochastisch unabhängig voneinander sind.

6. Im Dekodierer wird die empfangene Information wieder in das Alphabet $\alpha(\mathbb{A})$ dekodiert. Dabei werden gewisse Übertragungsfehler erkannt und möglicherweise korrigiert. Hierzu wird im einfachsten Fall eine Abbildung $d : \mathbb{F}_2^\ell \to \mathbb{F}_2^m$ mit der Eigenschaft $d(\mathbb{F}_2^\ell) = \alpha(\mathbb{A})$ genutzt.

   Wir nehmen also ab jetzt auch an, dass sender- und empfängerseitig mit demselben Alphabet $\alpha(\mathbb{A})$ bzw. $\mathbb{A}$ gearbeitet wird.

7. Die binär vorliegende Information wird vom Binärdekonverter in eine für den Empfänger nutzbare Form konvertiert, die nicht notwendig binär oder digital ist.

Die folgende Darstellung liefert ein konkretes, realistisches Beispiel des binären Sender-Empfänger-Szenarios.

Beispiel 2.1 (Bildübertragung von der Raumsonde Mariner 9): Die National Aeronautics and Space Administration (NASA) startete am 30. Mai 1971 die Marsmission Mariner 9 vom Kennedy Space Center in Florida. Mariner 9 ist eine rund 998 kg schwere Sonde, deren Aufgabe es war die Oberfläche des Planeten Mars aus einer Umlaufbahn heraus photographisch zu erfassen, sowie jahreszeitliche Veränderungen der Marsatmosphäre und -oberfläche zu messen. Die Sonde erreichte nach 167 Tagen Flugzeit und einer Flugstrecke von 398 Millionen Kilometern am 14. November 1971 den Mars, wo sie am 30. Dezember 1971 in ihren entgültigen, elliptischen Orbit einschwenkte, in dem sie der Marsoberfläche alle ca. 12 Stunden bis auf 1650 Kilometer nahe kam. Mariner 9 war die erste Sonde, die einen anderen Planeten umkreiste.

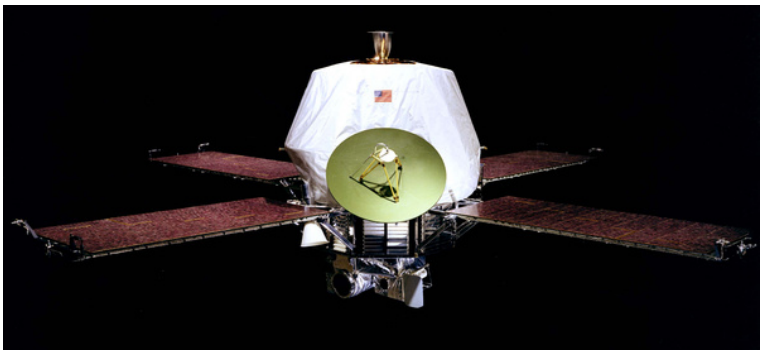


Abbildung 11: Die Raumsonde Mariner 9
(Courtesy NASA/JPL-Caltech)

Mariner 9 sandte bis zu ihrer Abschaltung am 27. Oktober 1972 insgesamt 7329 Schwarz-Weiß-Bilder der Marsoberfläche zur Erde; die Aufnahmen decken über 80% des Marsglobus' ab. Die Aufnahmenerstellung wurde durch einen der größten, jemals auf Mars beobachteten, globalen(!) Sandstürme verzögert; dieser dauerte von Ende September bis Dezember 1971. Der aktuelle Status (November 2022) der Sonde ist unklar: Möglicherweise bewegt sie sich immer noch auf einem Orbit um Mars. Ein Eintritt in die Marsatmosphäre mit nachfolgendem Absturz ist allerdings für das Jahr 2022 prognostiziert worden.

Die Sonde versorgte sich über vier Solarzellen mit insgesamt 500-Watt Leistung mit Energie und sandte ihre Daten mit Hilfe einer Funkanlage

von 20 Watt(!) Leistung. Die Entfernung zwischen Sender und Empfänger veränderte sich dabei je nach Stellung der Planeten Erde und Mars zueinander zwischen etwa 55 und 401 Millionen Kilometer.

Die obigen Angaben zu Mariner 9 stammen von den Missions-Webseiten des NASA Space Science Data Coordinated Archive

`https://nssdc.gsfc.nasa.gov`.

Nun zum Sender-Empfänger-Szenario in diesem Beispiel: Der Sender, also Mariner 9, nahm mit Hilfe zweier Kameras Bilder der Marsoberfläche auf. Die Kameras benutzten zur Erzeugung der Bilder sogenannte Vidicon-Sensoren – siehe Abbildung 12, links.

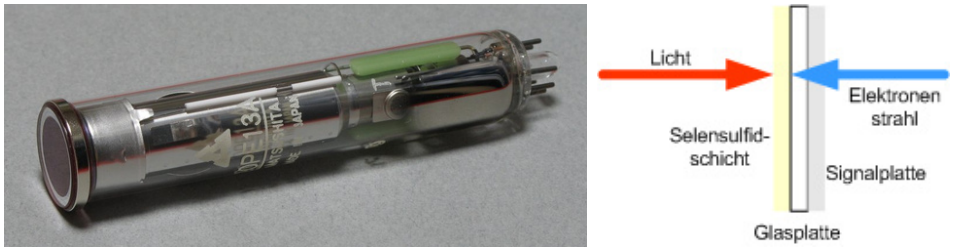


Abbildung 12: Vidicon-Bildaufnahmeröhre (1.7 cm Durchmesser)
(Quelle: Wikipedia, License: CC BY-SA 3.0)

Das zu photographierende Objekt wird auf eine mit Selensulfid beschichtete Glasplatte projiziert, die sich an der Vorderseite der Vidicon-Röhre befindet; in Abbildung 12 ist diese links zu sehen. Gleichzeitig wandert ein von der Röhre erzeugter Elektronenstrahl zeilenweise über die Rückseite der Glasplatte und erzeugt einen elektrischen Strom zwischen der Sulfidschicht und einer dahinter liegenden Signalplatte – siehe Abbildung 12, rechts. Der elektrische Widerstand der Selensulfidschicht an einem bestimmten Punkt hängt von der Stärke des dort auftreffenden Lichts ab, sodass die nach dem Auftreffen des Elektronenstrahls an diesem Punkt gemessene Spannung zwischen Glas- und Signalplatte ein Maß für die Lichtstärke an diesem Bildpunkt ist.

Auf diese Weise erzeugte der Vidicon-Sensor von Mariner 9 Bildaufnahmen, die aus jeweils 832 Bildpunkten pro Bildzeile und aus 700 Bildzeilen bestanden. Für jeden Bildpunkt wurde ein analoger Spannungwert

$U(x, y)$, $x \in \{1, \ldots, 832\}$, $y \in \{1, \ldots, 700\}$, entsprechend einer bestimmten Lichtstärke gemessen. Die Originalinformation ist also eine nicht digitale Funktion

$$U : \{1, \ldots, 832\} \times \{1, \ldots, 700\} \to \mathbb{R},$$

die einer Graustufenaufnahme entspricht.

Die Spannung $U(x, y)$ wurde dann in eine von $64 = 2^6$ Graustufenwerte digitalisiert. Das verwendete Alphabet war also $\mathbb{A} = \mathbb{F}_2^6$; ein Alphabetwechsel α war in diesem Fall nicht notwendig.

Die Graustufenwerte wurden schließlich unter Verwendung eines so genannten Reed-Muller-Kodes (siehe Abschnitt 3.5) kodiert: Jedes Symbol $a \in \mathbb{F}_2^6$ wird dabei in ein Symbol $c(a) \in \mathbb{F}_2^{32}$ kodiert. Aus der ursprünglichen Schwarz-Weiß-Aufnahme entsteht dadurch ein Folge von $832 \cdot 700 = 582\,400$ Kodewörtern mit jeweils 32 Bits. Ein Bild besteht also aus 18 636 800 Bits.

Die Sendeanlage von Mariner 9 konnte etwa 16 000 Bit pro Sekunde übertragen, sodass das Senden eines Bildes etwa 20 Minuten dauerte. Da die Kameras schneller als die Sendeanlage arbeiteten, wurden die Daten in der Sonde auf Band zwischengespeichert.

Der Reed-Muller-Kode konnte auf der Empfängerseite, in diesem Fall das Jet Propulsion Laboratory (JPL) in Kalifornien, mittels Maximum-Likelihood-Dekodierung so dekodiert werden, dass bis zu sieben Übertragungsfehler pro Symbol $c(a)$ korrigiert und ein achter zumindest erkannt wurde.

Nach dem Empfang und der Dekodierung der Daten eines Bildes wurde aus diesen mittels der »Data Reconstruction Camera« EOM 505 der heute noch existierenden Firma Digital Check eine Schwarz-Weiß-Photographie erstellt, die Daten wurden also wieder in ein analoges Format umgewandelt.

Als Beispiel für die von Mariner 9 gelieferten Bilder, die zum Teil eine unerwartet hohe Qualität besaßen, zeigt Abbildung 13 eine Region an der Flanke des erloschenen Schildvulkans Hecates Tholus. Die Aufnahme wurde am 17. Oktober 1972 um 18:24 GMT von der Kamera B (Engwinkelkamera) der Sonde gemacht und zeigt ein Gebiet von ungefähr 100 auf 85 Kilometer Ausdehnung. Sie wurde der Webseite

`http://petermasek.tripod.com/marinerall.html`

von Peter Masek entnommen und ist Teil der »Mariner 9 Imaging Experiment Data Records (EDR)«. Zum Vergleich zeigt Abbildung 13 rechts den gesamten Schildvulkan. Dieses Bild wurde aus Einzelbildern zusammengesetzt, die von der seit dem Jahr 2001 den Mars umkreisenden Sonde Odyssey

aufgenommen wurden. Der in Rede stehende Ausschnitt liegt auf dieser Aufnahme links oberhalb der Bildmitte.

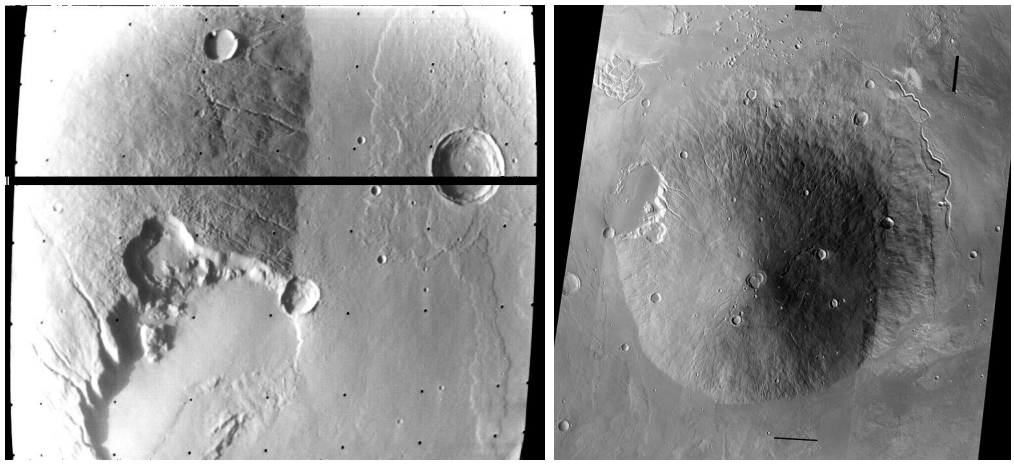


Abbildung 13: Aufnahmen des Schildvulkans Hecates Tholus
Links: Flanke des Schildvulkans (Mariner 9)
(Courtesy NASA Space Science Data Coordinated Archive)
Rechts: Gesamter Vulkan (Mars Odyssey)
(Courtesy NASA/JPL-Caltech)

»Die Menschen sind nicht bereit, sich von Erzählungen über Götter und Riesen trösten zu lassen, und sie sind nicht bereit, ihren Gedanken dort, wo sie über die Dinge des täglichen Lebens hinausgehen, eine Grenze zu ziehen. Damit nicht zufrieden bauen sie Teleskope, Satelliten und Beschleuniger, verbringen sie endlose Stunden am Schreibtisch um die Bedeutung, der von ihnen gewonnenen Daten zu entschlüsseln. Das Bestreben das Universum zu verstehen, hebt das menschliche Leben ein wenig über eine Farce hinaus und verleiht ihm einen Hauch von tragischer Würde.«
Steven Weinberg[2] [Wei] ◇

Wir kommen nun zur mathematischen Definition des Kodierers und des Dekodierers. Dabei vereinfachen wir gleichzeitig das in diesem Abschnitt eingeführte Sender-Empfänger-Szenario, indem wir eine möglicherweise vorhandene Alphabetwechsel $\alpha : \mathbb{A} \to \mathbb{F}_2^m$ und die Kodierungsabbildung $c : \mathbb{F}_2^m \to \mathbb{F}_2^\ell$ durch Verkettung zu einer einzigen Abbildung zusammenfassen. Der mathematisch irrelevante Alphabetwechsel erscheint dadurch in der Betrachtung nicht mehr.

[2] 1933 – 2021, amerikanischer Physiker und Nobelpreisträger

DEFINITION 2.2: *Ein binärer Blockkode der Länge ℓ für das Alphabet $\mathbb{A}$ ist eine injektive Abbildung $c : \mathbb{A} \to \mathbb{F}_2^\ell$.*

Für die Bildmenge $c(\mathbb{A})$ wird in der Regel das Symbol C benutzt. Die Elemente von C werden als Kodewörter (für die Symbole in $\mathbb{A}$) bezeichnet; C selbst nennt man einfach Kode (für $\mathbb{A}$).

Eine (vollständige) Dekodierabbildung für den binären Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ist eine Abbildung $d : \mathbb{F}_2^\ell \to C$ mit der Eigenschaft $d|_C = \mathrm{id}$.

Eine unvollständige Dekodierabbildung für den binären Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ist eine Abbildung $d : D \to \mathbb{A}$, $C \subseteq D$, $D \neq \mathbb{F}_2^\ell$, mit der Eigenschaft $d|_C = \mathrm{id}$.

Dekodierabbildungen können zwei Arten von Mängeln besitzen:

- Bei einem *Dekodierungsversagen* (engl.: decoding failure) kann ein empfangenes Wort nicht in ein Kodewort dekodiert werden. Dies kann nur bei unvollständigen Dekodierabbildungen auftreten, nämlich dann, wenn das übertragene Kodewort x zu einem Wort $y \notin D$ gestört wird.

- Ein *Dekodierungsfehler* (engl.: decoding error) entsteht, wenn für ein gesendetes Kodewort x, das durch Störungen in ein Wort y geändert wurde, $d(y) \neq x$ gilt.

Unvollständige Dekodierabbildungen werden dann verwendet, wenn die Wahrscheinlichkeit eines Dekodierungsfehlers sehr niedrig gehalten werden muss, weil falsche Dekodierungen extreme Konsequenzen haben können.

Das im Abschnitt 1.3 entwickelte stochastische Modell des Sender-Empfänger-Szenarios lässt sich nun soweit detaillieren, dass man damit Güteberechnungen für Kodierer-Dekodierer-Paare (c, d) durchführen kann. Bevor die Details formuliert werden, muss man sich Folgendes klar machen:

- Das im Abschnitt 1.3 mit $\mathbb{A}$ bezeichnete Sendealphabet ist genau genommen nun die Menge der Kodewörter $C \subseteq \mathbb{F}_2^\ell$. Da zwischen $\mathbb{A}$ und C die Bijektion c besteht, entsteht allerdings kein wesentlicher Unterschied zur früheren Beschreibung.

- Das früher mit $\mathbb{B}$ bezeichnete Empfängeralphabet ist nun gleich $\mathbb{F}_2^\ell$, da prinzipiell jedes Wort $y \in \mathbb{F}_2^\ell$ durch Störung aus einem Kodewort $x \in C$ entstehen kann.

- Das Verhalten der Dekodierungsabbildung d muss noch in das stochastische Modell aufgenommen werden.

Nach diesen Vorüberlegungen kommen wir zur Formulierung des konkreten stochastischen Modells für das binäre Sender-Empfänger-Szenario:

- **Senderseite:** Die Wahrscheinlichkeitsverteilung $p_{\mathbb{A}}$ lässt sich mittels des binären Blockkodes $c : \mathbb{A} \to \mathbb{F}_2^\ell$ in eine Wahrscheinlichkeitsverteilung auf $c(\mathbb{A}) = C$ überführen, indem man für jedes Kodewort $x = c(a)$ die gleiche Auftrittswahrscheinlichkeit wie für a setzt. Die entstehende Verteilung wird mit p_C bezeichnet.

- **BSMC:** Die Wahrscheinlichkeit für das Auftreten eines bestimmten Fehlermusters beim Durchgang eines Kodeworts $x \in C$ durch den Übertragungskanal kann mit Hilfe der Binomialverteilung auf $\mathbb{F}_2^\ell$ modelliert werden. Ist nämlich p_0 die Bitfehlerrate des BSMC, so ist

$$b(z) = b((z_1, \ldots, z_\ell)^t) := p_0^{w(z)}(1 - p_0)^{\ell - w(z)} \tag{15}$$

  die Wahrscheinlichkeit dafür, dass das Kodewort x genau an denjenigen Stellen i gestört wird, für die $z_i = 1$ ist.

  Die früher definierten Verteilungen $p_{\mathrm{rc}}(\cdot|x)$ auf $\{x\} \times \mathbb{F}_2^\ell$, die die Wahrscheinlichkeit für den Empfang von $y \in \mathbb{F}_2^\ell$ bei gesendetem $x \in C$ angeben, lassen sich nun mit Hilfe der Verteilung (15) und der Hamming-Metrik konkretisieren:

$$p_{\mathrm{rc}}(y|x) = p_0^{h(x,y)}(1-p_0)^{\ell - h(x,y)} = p_0^{w(x-y)}(1-p_0)^{\ell - w(x-y)} = b(x-y). \tag{16}$$

  Den Vektor $x - y$ nennt man naheliegenderweise den bei der Übertragung aufgetretenen *Fehlervektor*.

  Auch die Produktverteilung auf $C \times \mathbb{F}_2^\ell$ lässt sich jetzt konkret angeben:

$$p_{C \times \mathbb{F}_2^\ell}(x, y) = p_C(x) p_0^{h(x,y)}(1 - p_0)^{\ell - h(x,y)} = p_C(x) b(x - y). \tag{17}$$

- **Empfängerseite:** Die Verteilung p_{rc} auf $\mathbb{F}_2^\ell$ ist die Randverteilung von $p_{C \times \mathbb{F}_2^\ell}$ also

$$p_{\mathrm{rc}}(y) = \sum_{x \in C} p_C(x) p_0^{h(x,y)}(1 - p_0)^{\ell - h(x,y)} = \sum_{x \in C} p_C(x) b(x - y). \tag{18}$$

  An dieser Verteilung ist man allerdings nicht primär interessiert, sondern an derjenigen Verteilung auf C, die sich nach Anwendung des

Dekodierers d ergibt – im Folgenden wird diese mit $p_{c,d}$ bezeichnet, weil sie durch den binären Blockkode c und den Dekodierer d eindeutig festgelegt ist. Wie früher erläutert lässt sich diese Verteilung dann einfach auf das Originalalphabet $\mathbb{A}$ übertragen.

Für die Auftrittswahrscheinlichkeit eines $x' \in C$ auf Empfängerseite erhält man:

$$\begin{aligned} p_{c,d}(x') &= \sum_{y \in \mathbb{F}_2^\ell:\, d(y)=x'} p_{\mathrm{rc}}(y) \\ &= \sum_{y \in \mathbb{F}_2^\ell:\, d(y)=x'} \sum_{x \in C} p_C(x) b(x-y) \\ &= \sum_{x \in C} \sum_{y \in \mathbb{F}_2^\ell:\, d(y)=x'} p_C(x) b(x-y). \end{aligned} \tag{19}$$

Wir wollen nun ein gegebenes Paar $c : \mathbb{A} \to \mathbb{F}_2^\ell$ und $d : D \to \mathbb{A}$ eines binären Blockkodes und einer zugehörigen Dekodierabbildung mit stochastischen Mitteln hinsichtlich ihrer Güte bewerten. Hierzu betrachtet man zunächst das Dekodierungsversagen:

Die Ereignisse »x wird gesendet und nach der Übertragung nicht dekodiert«, also $\{x\} \times \mathbb{F}_2^\ell \setminus D$, sind für verschiedene x disjunkt. Daher ist

$$\begin{aligned} p_{\mathrm{fail}}(c,d) &:= \sum_{x \in C} \sum_{y \notin D} p_{C \times \mathbb{F}_2^\ell}(x,y) \\ &= \sum_{x \in C} \sum_{y \notin D} p_C(x) p_{\mathrm{rc}}(y|x) \\ &= \sum_{x \in C} \sum_{y \notin D} p_C(x) b(x-y) \end{aligned} \tag{20}$$

die Wahrscheinlichkeit für ein Dekodierungsversagen.

Die Ereignisse »x wird gesendet und nach der Übertragung falsch dekodiert«, also $\{x\} \times D \setminus d^{-1}(x)$, sind für verschiedene x disjunkt. Daher ist

$$\begin{aligned} p_{\mathrm{err}}(c,d) &:= \sum_{x \in C} \sum_{y \in D:\, d(y) \neq x} p_{C \times \mathbb{F}_2^\ell}(x,y) \\ &= \sum_{x \in C} \sum_{y \in D:\, d(y) \neq x} p_C(x) p_{\mathrm{rc}}(y|x) \\ &= \sum_{x \in C} \sum_{y \in D:\, d(y) \neq x} p_C(x) b(x-y) \end{aligned} \tag{21}$$

die Wahrscheinlichkeit für einen Dekodierungsfehler.

Da die Ereignisse »Ein Dekodierungsversagen tritt ein.« und »Ein Dekodierungsfehler tritt ein.« disjunkt sind, ist die folgende Definition sinnvoll:

DEFINITION 2.3: *Für einen binären Blockkode c und eine zugehörige Dekodierabbildung d ist die totale Fehlerwahrscheinlichkeit des Paares (c, d) definiert als*

$$p_{\,\mathrm{tot}}(c, d) := p_{\mathrm{fail}}(c, d) + p_{\mathrm{err}}(c, d).$$

BEMERKUNG: Im Fall einer vollständigen Dekodierabbildung d gibt es kein Dekodierungsversagen, weswegen sich die totale Fehlerwahrscheinlichkeit auch so schreiben lässt:

$$p_{\,\mathrm{tot}}(c, d) = 1 - \sum_{x \in C} \sum_{y \in \mathbb{F}_2^\ell :\, d(y) = x} p_C(x) b(x - y). \tag{22}$$

Insgesamt ergibt sich als *ein* theoretisches Ziel der Kodierungstheorie: *Löse das Optimierungsproblem*

$$\operatorname{argmin}(p_{\,\mathrm{tot}}(c, d) :\ c : \mathbb{A} \to \mathbb{F}_2^\ell,\ d : D \to \mathbb{A}) \tag{23}$$

bei gegebener Blocklänge $\ell \in \mathbb{N}$ und gegebenem Alphabet $\mathbb{A}$.
Diese Optimierungsaufgabe lässt sich, obwohl endlich, nicht effektiv lösen, da die Anzahl möglicher Abbildungen c und d zu hoch ist: Berücksichtigt man, dass injektive Abbildung $c : \mathbb{A} \to \mathbb{F}_2^\ell$ und $c' : \mathbb{A} \to \mathbb{F}_2^\ell$ mit demselben Bild C in (23) nicht unterschieden werden müssen, gibt es immer noch

$$r = \binom{2^\ell}{|\mathbb{A}|}$$

verschiedene Kandidaten für c. Eine untere Schranke für die Binomialkoeffizienten ist

$$\left(\frac{n-k+1}{k}\right)^k \le \binom{n}{k},$$

woraus sich

$$r \ge \left(\frac{2^\ell - |\mathbb{A}| + 1}{|\mathbb{A}|}\right)^{|\mathbb{A}|}$$

ergibt. Im Fall des Beispiels 2.1 der Mariner-9-Sonde wären also mehr als

$$\left(\frac{2^{32} - 63}{64}\right)^{64} > 2^{1600} > 10^{481}$$

mögliche Kodierungsabbildungen zu untersuchen. Die Dekodierer sind dabei noch nicht berücksichtigt.

Die totale Fehlerwahrscheinlichkeit $p_{\text{tot}}(c, d)$ kann natürlich auch direkt als Gütemaß zur Beurteilung von konkreten Kodierer-Dekodierer-Paaren genutzt werden. Zwei weitere solche Gütemaße spielen in der Praxis eine wichtige Rolle: Zum ersten der beiden kommt man durch die nun schon mehrfach erwähnte Tatsache, dass die Kodewörter eines »guten« Kodes möglichst großen »Abstand« voneinander haben sollten, damit die Wahrscheinlichkeit einer Störung, die ein Kodewort in ein zweites überführt, gering ist. Man beachte dabei, dass eine solche Störung durch keinen Dekodierer d erkannt werden kann. Dies motiviert die

DEFINITION 2.4: *Die Minimaldistanz des binären Blockkodes* $c : \mathbb{A} \to \mathbb{F}_2^\ell$ *ist definiert als*

$$h_{\min}(c) := \min(h(x, x') : x, x' \in C, x \neq x').$$

Die Minimierung der totalen Fehlerwahrscheinlichkeit ist nicht das einzige praxisrelevante Ziel der Kodierungstheorie. Genauso wichtig ist die pro Kodewort übertragene *relevante* Information, also nicht die Information, die zur Fehlererkennung und -korrektur hinzugefügt wurde, möglichst hoch zu halten. Diese Eigenschaft eines Kodes wird durch folgende Größe quantifiziert:

DEFINITION 2.5: *Die Informationsrate des binären Blockkodes* $c : \mathbb{A} \to \mathbb{F}_2^\ell$ *ist*

$$R(c) := \frac{\log_2(|\mathbb{A}|)}{\ell}.$$

BEMERKUNG: Wegen $|\mathbb{F}_2^\ell| = 2^\ell$ gilt stets $R(c) \leq 1$ und $R(c) = 1$ genau dann, wenn c surjektiv und damit bijektiv ist.

BEZEICHUNG: Ein binärer Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ der Minimaldistanz m wird im Weiteren oft kurz als $(\ell, |\mathbb{A}|, m)$-Kode bezeichnet.

BEISPIEL 2.6: Wir betrachten einen Blockkode für DNS-Sequenzen wie sie vielleicht zwischen verschiedenen Abteilungen eines in der Genetik tätigen Unternehmens ausgetauscht werden. Das Sendealphabet ist also

$$\mathbb{A} = \{A, C, G, T\}$$

und zur Übermittlung von DNS-Sequenzen soll folgender binärer Blockkode $c : \mathbb{A} \to \mathbb{F}_2^4$ der Länge 4 genutzt werden:

$$\left.\begin{array}{rcl} c(A) & = & (0,0,0,0)^t,\ c(C) = (0,1,1,1)^t, \\ c(G) & = & (1,0,0,1)^t,\ c(T) = (1,1,1,0)^t. \end{array}\right\} \tag{24}$$

Eine vollständige Dekodierungabbildung d ist durch die Tabelle 3 gegeben, wobei $y = (y_1, y_2, y_3, y_4)^t \in C$ ist.

$w(y)$	y_4	Symbol
0	0	A
1	0	A
2	0	T
3	0	T
1	1	G
2	1	G
3	1	C
4	1	C

Tabelle 3: Vollständige Dekodierung eines Blockkodes der Länge 4

Zur Berechnung der totalen Fehlerwahrscheinlichkeit verwendet man Formel (22), man benötigt also die Distanzen jedes Kodeworts zu jedem Wort. Für das Kodewort $c(A)$ ergibt sich dann – siehe Tabelle 4:

$$\{y \in \mathbb{F}_2^4 :\ d(y) = c(A)\} = \{(0,0,0,0)^t, (0,0,1,0)^t, (0,1,0,0)^t, (1,0,0,0)^t\},$$

also

$$\sum_{y \in \mathbb{F}_2^4:\ d(y) = c(A)} p_0^{h(c(A),y)} (1-p_0)^{4-h(c(A),y)} = (1-p_0)^4 + 3p_0(1-p_0)^3.$$

Für das Kodewort $c(T)$ – siehe Tabelle 4:

$$\{y \in \mathbb{F}_2^4 :\ d(y) = c(T)\} = \{(1,1,1,0)^t, (0,1,1,0)^t, (1,1,0,0)^t, (1,0,1,0)^t\},$$

also

$$\sum_{y \in \mathbb{F}_2^4:\ d(y) = c(T)} p_0^{h(c(T),y)} (1-p_0)^{4-h(c(T),y)} = (1-p_0)^4 + 3p_0(1-p_0)^3.$$

Kodewort	Wort	Distanz	Kodewort	Wort	Distanz
(0,0,0,0)	(0,0,0,0)	0	(1,1,1,0)	(0,0,0,0)	3
(0,0,0,0)	(0,0,0,1)	1	(1,1,1,0)	(0,0,0,1)	4
(0,0,0,0)	(0,0,1,0)	1	(1,1,1,0)	(0,0,1,0)	2
(0,0,0,0)	(0,0,1,1)	2	(1,1,1,0)	(0,0,1,1)	3
(0,0,0,0)	(0,1,0,0)	1	(1,1,1,0)	(0,1,0,0)	2
(0,0,0,0)	(0,1,0,1)	2	(1,1,1,0)	(0,1,0,1)	3
(0,0,0,0)	(0,1,1,0)	2	(1,1,1,0)	(0,1,1,0)	1
(0,0,0,0)	(0,1,1,1)	3	(1,1,1,0)	(0,1,1,1)	2
(0,0,0,0)	(1,0,0,0)	1	(1,1,1,0)	(1,0,0,0)	2
(0,0,0,0)	(1,0,0,1)	2	(1,1,1,0)	(1,0,0,1)	3
(0,0,0,0)	(1,0,1,0)	2	(1,1,1,0)	(1,0,1,0)	1
(0,0,0,0)	(1,0,1,1)	3	(1,1,1,0)	(1,0,1,1)	2
(0,0,0,0)	(1,1,0,0)	2	(1,1,1,0)	(1,1,0,0)	1
(0,0,0,0)	(1,1,0,1)	3	(1,1,1,0)	(1,1,0,1)	2
(0,0,0,0)	(1,1,1,0)	3	(1,1,1,0)	(1,1,1,0)	0
(0,0,0,0)	(1,1,1,1)	4	(1,1,1,0)	(1,1,1,1)	1

Tabelle 4: Distanzen zum Kodewort $c(A)$ (links) und $c(T)$ (rechts)

Für das Kodewort $c(G)$ – siehe Tabelle 5:

$$\{y \in \mathbb{F}_2^4 : \ d(y) = c(G)\} = \{(1,0,0,1)^t, (0,0,0,1)^t, (0,0,1,1)^t, (0,1,0,1)^t\},$$

also

$$\sum_{y \in \mathbb{F}_2^4:\ d(y)=c(G)} p_0^{h(c(T),y)}(1-p_0)^{4-h(c(T),y)} = (1-p_0)^4 + p_0(1-p_0)^3 + 2p_0^2(1-p_0)^2.$$

Für das Kodewort $c(C)$ – siehe Tabelle 5:

$$\{y \in \mathbb{F}_2^4 : \ d(y) = c(C)\} = \{(0,1,1,1)^t, (1,0,1,1)^t, (1,1,0,1)^t, (1,1,1,1)^t\},$$

also

$$\sum_{y \in \mathbb{F}_2^4:\ d(y)=c(C)} p_0^{h(c(T),y)}(1-p_0)^{4-h(c(T),y)} = (1-p_0)^4 + p_0(1-p_0)^3 + 2p_0^2(1-p_0)^2.$$

Zusammenfügen der Einzelwahrscheinlichkeiten unter Verwendung der

Kodewort	Wort	Distanz	Kodewort	Wort	Distanz
(1,0,0,1)	(0,0,0,0)	2	(0,1,1,1)	(0,0,0,0)	3
(1,0,0,1)	(0,0,0,1)	1	(0,1,1,1)	(0,0,0,1)	2
(1,0,0,1)	(0,0,1,0)	3	(0,1,1,1)	(0,0,1,0)	2
(1,0,0,1)	(0,0,1,1)	2	(0,1,1,1)	(0,0,1,1)	1
(1,0,0,1)	(0,1,0,0)	3	(0,1,1,1)	(0,1,0,0)	2
(1,0,0,1)	(0,1,0,1)	2	(0,1,1,1)	(0,1,0,1)	1
(1,0,0,1)	(0,1,1,0)	4	(0,1,1,1)	(0,1,1,0)	1
(1,0,0,1)	(0,1,1,1)	3	(0,1,1,1)	(0,1,1,1)	0
(1,0,0,1)	(1,0,0,0)	1	(0,1,1,1)	(1,0,0,0)	4
(1,0,0,1)	(1,0,0,1)	0	(0,1,1,1)	(1,0,0,1)	3
(1,0,0,1)	(1,0,1,0)	2	(0,1,1,1)	(1,0,1,0)	3
(1,0,0,1)	(1,0,1,1)	1	(0,1,1,1)	(1,0,1,1)	2
(1,0,0,1)	(1,1,0,0)	2	(0,1,1,1)	(1,1,0,0)	3
(1,0,0,1)	(1,1,0,1)	1	(0,1,1,1)	(1,1,0,1)	2
(1,0,0,1)	(1,1,1,0)	3	(0,1,1,1)	(1,1,1,0)	2
(1,0,0,1)	(1,1,1,1)	2	(0,1,1,1)	(1,1,1,1)	1

Tabelle 5: Distanzen zum Kodewort $c(G)$ (links) und $c(C)$ (rechts)

Werte aus Beispiel 1.5 liefert die totale Fehlerwahrscheinlichkeit

$$\begin{aligned} p_{\text{tot}}(c,d) &= 1 - \sum_{a\in\{A,T,G,C\}} p_{\mathbb{A}}(a) \sum_{y\in\mathbb{F}_2^\ell:\, d(y)=c(a)} p_0^{h(c(a),y)}(1-p_0)^{\ell-h(c(a),y)} \\ &= 1 - 0,299\cdot((1-p_0)^4 + 3p_0(1-p_0)^3) \\ &\quad - 0,298\cdot((1-p_0)^4 + 3p_0(1-p_0)^3) \\ &\quad - 0,195\cdot((1-p_0)^4 + p_0(1-p_0)^3 + 2p_0^2(1-p_0)^2) \\ &\quad - 0,201\cdot((1-p_0)^4 + p_0(1-p_0)^3 + 2p_0^2(1-p_0)^2). \end{aligned}$$

Beträgt die Fehlerrate des BSMC zum Beispiel $p_0 = 0.01$, so ergibt sich

$$p_{\text{tot}} \approx 0.025.$$

Die Informationsrate des hier betrachteten binären Blockkodes ist:

$$R(c) = \frac{\log_2(4)}{4} = \frac{1}{2}.$$

Dies entspricht der Intuition: Es werden 2 Bits benötigt um einen Buchstaben des Alphabets vollständig anzugeben, während ein Kodewort 4 Bit lang ist. Folglich sind nur 50% eines Kodeworts informationshaltig in Bezug auf die relevante Information. ◇

2.2 Hadamard-Kodes

In diesem Abschnitt wird eine praxisrelevante Klasse binärer Blockkodes diskutiert, die man aus ganzzahligen Matrizen eines bestimmten Typs gewinnt:

DEFINITION 2.7: *Eine Matrix $H = (h_{ij}) \in \mathbb{Z}^{n \times n}$ heißt Hadamard-Matrix, falls $h_{ij} \in \{-1, 1\}$ und $HH^t = nE$ gilt.*

Zum Beispiel ist

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

eine Hadamard-Matrix.

Abbildung 14: Jacques Hadamard
(Quelle: https://mathshistory.st-andrews.ac.uk/Biographies)

Hadamard-Matrizen sind zu Ehren des französischen Mathematikers und mathematischen Physikers Jacques Salomon Hadamard (1865 – 1963) so benannt, der diese im Bereich der Integralgleichungen einsetzte. Hadamards mathematische Arbeiten besitzen eine enorme Bandbreite: Komplexe Analysis, nichtlineare gewöhnliche Differentialgleichungen, partielle Differentialgleichungen, Differentialgeometrie, Elastizitätslehre, Optik, Hydrodynamik, Stochastik. Als einer seiner herausragendsten Beiträge zur Mathematik zählt der Beweis des Primzahlsatzes: Die Anzahl der Primzahlen kleiner als n wächst asymptotisch wie die Funktion $\frac{n}{\ln(n)}$.

In den Fällen $n = 1$ und $n = 2$ kann man leicht alle Hadamard-Matrizen angeben. Mit Hilfe der folgenden Eigenschaften von Hadamard-Matrizen kann man weitere konstruieren:

FESTSTELLUNG 2.8: *Es sei $H \in \mathbb{Z}^{n\times n}$ eine Hadamard-Matrix.*

1. *Für $i, j \in \{1, \ldots, n\}$, $i \neq j$, gilt: $|\{k : h_{ik} = h_{jk}\}| = |\{k : h_{ik} \neq h_{jk}\}|$. Insbesondere ist im Fall $n > 1$ diese Zahl stets gerade.*

2. *Ersetzt man eine beliebige Zeile oder Spalte in H durch die mit -1 multiplizierte Zeile oder Spalte, so entsteht eine Hadamard-Matrix.*

3. *Die Matrix*
$$H' := \begin{pmatrix} H & H \\ H & -H \end{pmatrix} \in \mathbb{R}^{2n\times 2n}$$
ist eine Hadamard-Matrix.

BEWEIS: Wesentlich für den Beweis der Feststellung ist die Tatsache, dass die Koeffizienten der Matrix HH^t die Skalarprodukte $\langle h_i, h_j\rangle$ sind, wobei h_i die i-te Zeile von H bezeichnet.

1. Nach Voraussetzung gilt $\langle h_i, h_j\rangle = 0$ und für jeden Index k mit $h_{ik} = h_{jk}$ gilt $h_{ik}h_{jk} = 1$. Folglich muss es zu einem solchen k einen Index k' mit der Eigenschaft $h_{ik'}h_{jk'} = -1$ geben. Letzteres ist aber gleichbedeutend mit $h_{ik'} \neq h_{ik'}$.

2. Ersetzt man h_k durch $-h_k$, so werden nur diejenigen Koeffizienten von HH^t beeinflusst, für die Skalarprodukte mit $-h_k$ gebildet werden. Dies sind:

$$\begin{aligned} \langle -h_k, h_j\rangle = -\langle h_k, h_j\rangle = 0 \text{ für } k \neq j, \\ \langle h_i, -h_k\rangle = -\langle h_i, h_k\rangle = 0 \text{ für } k \neq i, \\ \langle -h_k, -h_k\rangle = \langle h_k, h_k\rangle = n. \end{aligned}$$

Ersetzt man die k-te Spalte von H durch ihr Negatives, so werden die Koeffizienten h_{ik} zu $-h_{ik}$ geändert. Der Koeffizient $(H'H'^t)_{ij}$ in der Zeile i und Spalte j der Matrix $H'H'^t$, wobei H' die geänderte Matrix ist, berechnet sich dann zu:

$$(H'H'^t)_{ij} = h_{i1}h_{j1} + h_{i2}h_{j2} + \ldots + (-h_{ik} \cdot -h_{jk}) + \ldots + h_{in}h_{nj} = (HH^t)_{ij}.$$

3. Der Beweis erfolgt durch Nachrechnen. □

Bemerkung: Durch die in Punkt 3 angegebene Konstruktionsmethode kann man Hadamard-Matrizen mit einer beliebigen Zweierpotenz als Zeilenzahl konstruieren. Die rekursiv aus der Matrix $H_1 = (1) \in \mathbb{Z}^1$ entstehenden Matrizen nennt man auch Sylvester-Matrizen[3].

Satz 2.9: *Für jede Hadamard-Matrix $H \in \mathbb{Z}^{n\times n}$ gilt: $n \in \{1, 2\}$ oder n ist durch 4 teilbar.*

Beweis: Es sei H ein Hadamard-Matrix mit $n \geq 3$. Man betrachtet die Teilspalten $(h_{1k}, h_{2k}, h_{3k})^t$ der jeweiligen Koeffizienten der ersten drei Zeilen der Matrix. Indem man gegebenenfalls eine Spalte mit -1 multipliziert – siehe Punkt 2 von Feststellung 2.8, kann man erreichen, dass diese Teilspalten nur folgende Formen haben können:

$$(1, 1, 1)^t,\ (1, 1, -1)^t, (1, -1, 1)^t, (1, -1, -1)^t.$$

Es seien nun i, j, k, ℓ die Anzahlen, in denen diese Formen in allen Spalten von H auftreten. Dann gilt, da H eine Hadamard-Matrix ist,

$$\begin{aligned} i + j - k - l &= 0 \text{ (aus } \langle h_1, h_2\rangle = 0), \\ i - j + k - l &= 0 \text{ (aus } \langle h_1, h_3\rangle = 0), \\ i - j - k + l &= 0 \text{ (aus } \langle h_2, h_3\rangle = 0). \end{aligned}$$

Dies liefert $3i = j + k + l$. Es ist aber auch $i + j + k + l = n$, womit sich $3i = n - i$ also die Behauptung ergibt. □

Der letzte Satz legt die Frage nahe, ob es zu jeder durch 4 teilbaren Zahl n eine Hadamard-Matrix mit n Zeilen gibt. Die Antwort auf diese Frage ist unbekannt. Die so genannte *Hadamard-Paley-Vermutung* besagt, dass die Antwort »Ja« lautet. Nach der Masterarbeit »A Survey of the Hadamard Conjecture« von Eric Tressler (2004, Virginia Polytechnic Institute) war zum Zeitpunkt der Anfertigung der Arbeit $n = 428$ die kleinste natürliche, durch 4 teilbare Zahl zu der keine Hadamard-Matrix bekannt ist.

Binäre Blockkodes aus Hadamard-Matrizen

Aus einer gegebenen Hadamard-Matrix $H \in \mathbb{Z}^{n\times n}$ lassen sich drei verschiedene binäre Blockkodes konstruieren. Dabei *normalisiert* man die Matrix H zunächst: Nach Feststellung 2.8 kann man die Zeilen von H so ersetzen, dass

[3] James Joseph Sylvester: englischer Mathematiker, 1814 – 1897.

die erste Spalte der so gewonnenen Matrix nur 1en enthält. Man kann also annehmen, dass H bereits diese Form besitzt.

Im Folgenden sei $A \in \mathbb{F}_2^{n \times n}$ diejenige Matrix, die man aus H erhält, indem man jede 1 durch $0 \in \mathbb{F}_2$ und jede -1 durch $1 \in \mathbb{F}_2$ ersetzt.

HADAMARD-KODES VOM TYP I

Es sei $C_1 := \{b_1^t, \ldots, b_n^t\} \subseteq \mathbb{F}_2^{n-1}$, wobei b_i die i-te Zeile derjenigen Matrix ist, die durch Entfernen der ersten Spalte aus A – diese enthält nur 0en – entsteht.

FESTSTELLUNG 2.10: *Für den Kode C_1 gilt $h(x, x') = \frac{n}{2}$ für je zwei verschiedene Kodewörter $x, x' \in C_1$. Es handelt sich um einen $(n-1, n, \frac{n}{2})$-Kode der Informationsrate*

$$R(C_1) = \frac{\log_2(n)}{n-1}.$$

BEWEIS: Die Aussage zur Minimaldistanz folgt aus Feststellung 2.8, Punkt 1, wobei zu beachten ist, dass die aus A entfernte erste Spalte nur aus 0en besteht. Alle anderen Aussagen in der Feststellung sind unmittelbar klar. □

BEMERKUNG: Die Informationsrate $R(C_1)$ geht mit wachsendem n gegen 0, was die beeindruckende Minimaldistanz von C_1 relativiert.

HADAMARD-KODES VOM TYP II

DEFINITION 2.11: *Das binäre Komplement eines Worts $y \in \mathbb{F}_2^\ell$ ist das Wort $(1, \ldots, 1)^t - y$.*

BEMERKUNG: Es ist $(1, \ldots, 1)^t - y = (1, \ldots, 1)^t + y$ und für beliebige Wörter $y_1, y_2 \in \mathbb{F}_2^\ell$ gilt

$$h(y_1, y_2) = h((1, \ldots, 1)^t - y_1, (1, \ldots, 1)^t - y_2).$$

Es sei

$$C_2 := C_1 \cup \{(1, \ldots, 1)^t - y : y \in C_1\}.$$

FESTSTELLUNG 2.12: *Die Menge $C_2 \subseteq \mathbb{F}_2^{n-1}$ ist ein $(n-1, 2n, \frac{n}{2}-1)$-Kode der Informationsrate*

$$R(C_2) = \frac{\log_2(n) + 1}{n-1}.$$

BEWEIS: Die Aussage zur Länge des Kodes ist klar.

Da das Bilden des binären Komplements eine injektive Abbildung ist, verdoppelt sich die Anzahl der Kodewörter gegenüber der des Kodes C_1, wenn man nur zeigen kann, dass das binäre Komplement eines Kodeworts $x \in C_1$ nicht selbst in C_1 liegt. Dies wird durch die Bestimmung der Minimaldistanz von C_2 mitgeliefert.

Zur Bestimmung der Minimaldistanz sei $x_1 \in C_1$ und $x_2 = (1, \ldots, 1)^t - x$ für ein $x \in C_1$. Dann gilt $w(x - x_1) = h(x_1, x) = \frac{n}{2}$. Es folgt

$$h(x_2, x_1) = w((1, \ldots, 1)^t - (x - x_1)) = n - 1 - \frac{n}{2} = \frac{n}{2} - 1.$$

Insbesondere ist $x_2 \notin C_1$.

Da die binären Komplemente zweier Wörter aus C_1 wegen der Translationsinvarianz der Hamming-Metrik den Abstand $\frac{n}{2}$ besitzen, ist die Behauptung zur Minimaldistanz von C_2 bewiesen.

Die Aussage zur Informationsrate ist unmittelbar klar. □

HADAMARD-KODES VOM TYP III

FESTSTELLUNG 2.13: *Die Menge $C_3 \subseteq \mathbb{F}_2^n$ der Zeilen der Matrix A und ihrer binären Komplemente, ist ein $(n, 2n, \frac{n}{2})$-Kode. Die Informationsrate dieses Kodes ist*

$$R(C_3) = \frac{\log_2(n) + 1}{n}.$$

BEISPIEL 2.14: Wir bestimmen den Hadamard-Kodes zur Sylvester-Matrix

$$H := \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}.$$

Die oben mit A bezeichnete Matrix ist dann

$$A = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix},$$

woraus sich als Hadamard-Kode vom Typ I die Menge

$$C_1 := \{(0,0,0)^t, (1,0,1)^t, (0,1,1)^t, (1,1,0)^t\}$$

und damit der Hadamard-Kode

$$C_2 := \{(0,0,0)^t, (1,0,1)^t, (0,1,1)^t, (1,1,0)^t, (1,1,1)^t, (0,1,0)^t, (1,0,0)^t, (0,0,1)^t\} = \mathbb{F}_2^3$$

vom Typ II ergeben. Die Minimaldistanz von C_1 ist 2, die von C_2 nur 1. Der Kode C_2 ist hier folglich nutzlos. Der Kode C_1 ist in Abbildung 15 als Teilmenge der Eckenmenge eines Würfels dargestellt.

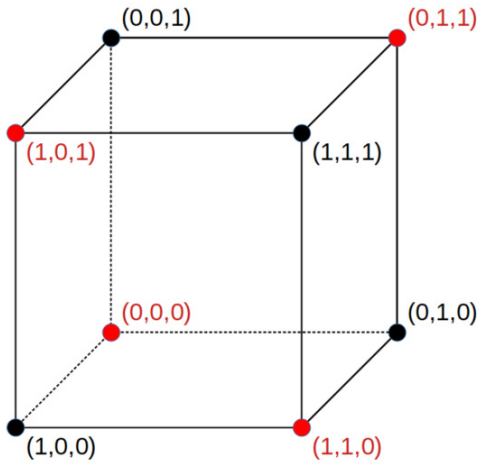


Abbildung 15: Hadamard-Kode $C_1 \subset \mathbb{F}_2^3$ vom Typ I

Der durch die Matrix A definierte Hadamard-Kode vom Typ III ergibt sich zu

$$\begin{aligned} C_2 := \{ \quad & (0,0,0,0)^t, (0,1,0,1)^t, (0,0,1,1)^t, (0,1,1,0)^t, \\ & (1,1,1,1)^t, (1,0,1,0)^t, (1,1,0,0)^t, (1,0,0,1)^t\}. \end{aligned}$$

Er kann als Teilmenge der Eckenmenge eines 4-dimensionalen Würfels (Tesserakts) betrachtet werden. Eine 2-dimensionale Projektion davon ist in Abbildung 16 zu sehen. ◇

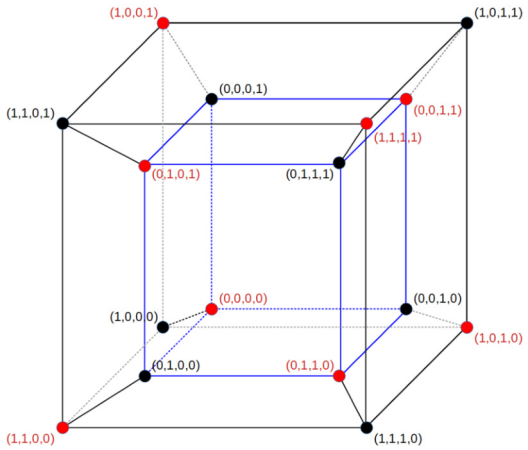


Abbildung 16: Hadamard-Kode $C_3 \subset \mathbb{F}_2^4$ vom Typ III

Beispiel 2.15 (Kodierung von Bitmaps): Zur Digitalisierung von Bildern oder Grafiken werden aktuell mehr als 12 verschiedene Datenformate genutzt. Im Folgenden wird das Bitmap-Format kurz beschrieben und erklärt, wie man einen fehlerkorrigierenden Kode in diesem Rahmen verwendet.

Zur Digitalisierung eines Bildes wird dieses in sogenannte *Pixel* unterteilt, wofür das Bild ein rechteckiges Format besitzen muss. Die rechteckige Bildfläche wird in $b \cdot h$, $b, h \in \mathbb{N}$, gleich große Teilrechtecke zerlegt, wobei in der Bildbreite b dieser Rechtecke nebeneinander und in der Bildhöhe h der Rechtecke übereinander liegen. Um eine hinreichend genaue Reproduktion des Bildes zu gewährleisten, sollte die Zerlegung so fein sein, dass es innerhalb eines Teilrechtecks eine dominierende Farbe gibt. Nur diese wird im Bitmap-Format für das jeweilige Teilrechteck gespeichert.

Zur Digitalisierung von Farben gibt es unterschiedliche Verfahren. Im 24-Bit-RGB-System werden Farben als Mischungen der Grundfarben Rot, Grün und Blau dargestellt. Die Intensität mit der die jeweilige Farbe in der Mischung erscheint kann in 256 Stufen variiert werden, wobei 0 für ein Nichtvorkommen in der Mischung und 255 für die volle Intensität dieser Farbe stehen. Eine im 24-Bit-RGB-System kodierbare Farbe wird also durch Angabe von drei 8-Bit-Worten festgelegt, wobei die Farbintensitäten in der Reihenfolge Rot, Grün und Blau angegeben werden. Die Farbe *cornflowerblue*

hat zum Beispiel die Intensitätswerte

$$R = 1100100,\ G = 10010101,\ B = 11101101.$$

Das 24-Bit Bitmap-Dateiformat (∗.bmp; es gibt genau genommen mehrere solche Formate) besitzt die folgenden Komponenten:

- Eine bmp-Datei beginnt mit einem Header 1, der unter anderem Angaben zur Dateilänge, sowie dem Beginn der eigentlichen Grafikdaten in der Datei enthält.
- Im Header 2 ist unter anderem die Bildbreite und -höhe in Pixel angegeben, sowie die reale Größe eines Pixels.
- Nach dem Header 2 kann eine Farbpalette in Form einer Liste von RGB-Werten angegeben sein. Diese enthält gegebenenfalls alle Farben, die im gespeicherten Bild vorkommen.
- Schließlich folgen die eigentlichen Grafikdaten: Die RGB-Farbwerte der einzelnen Pixel der Grafik erscheinen hier von links nach rechts beginnend von links unten. Dabei werden die Intensitätswerte jeweils in der Reihenfolge Blau, Grün, Rot angegeben. Alternativ können statt der Intensitätswerte auch Indizes dieser Werte in der Farbpalette angegeben sein.

Um die Pixeldaten in einer bmp-Datei fehlerkorrigierend zu kodieren kann man auf mindestens zwei Weisen vorgehen:

1. Man fasst die Farbinformation zu einem Pixel als 24-Bit-Wort auf, muss also einen Kode für das Alphabet $\mathbb{A} = \mathbb{F}_2^{24}$ mit 2^{24} Symbolen verwenden.
2. Man fasst die Farbinformation zu einem Pixel als drei 8-Bit-Worte auf und kodiert jeweils die 8-Bit-Worte. Das zu betrachtende Alphabet ist in diesem Fall $\mathbb{A} = \mathbb{F}_2^8$ mit nur 256 Symbolen.

Im folgenden Beispiel wurde der zweite Weg beschritten, da Graustufenbilder betrachtet werden und für diese die Farbwerte des roten, grünen und blauen Kanals identisch sind. Die Farbwerte der Pixel wurden mit einem Hadamard-Kode

$$c : \mathbb{F}_2^8 \to \mathbb{F}_2^{255}$$

vom Typ I kodiert; die Blocklänge ist also 255 und die Minimaldistanz 128.

Als (vollständige) Dekodierungsabbildung

$$d : \mathbb{F}_2^{255} \to \mathbb{F}_2^8$$

wird die folgende verwendet:

$$d(y) := x \text{ falls } \{x' \in C_1 : h(y, x') \leq h(y, x)\} = \{x\}.$$

Falls mehr als ein Kodewort $x' \in C_1$ minimale Hamming-Distanz zu y aufweits, wählt man $d(y) = x$ so, dass x die erste Zeile in A mit dieser Eigenschaft ist. Diese Festlegung ist programmiertechnisch einfach, jedoch im Kontext sicher nicht die beste Lösung: Besser wäre es in einem solchen Fall bei der Dekodierung auch die Farbwerte der Umgebungspixel zu berücksichtigen.

Beispielhaft wurde mit einem Bildausschnitt von 46 Pixel Breite und 53 Pixel Höhe aus der in Abbildung 13 gezeigten Photographie eine Simulation unter Verwendung des oben eingeführten Kodierer-Dekodierer-Paares durchgeführt. Der Ausschnitt befindet sich links unterhalb des Vulkankraters.

Die Abbildung 17 zeigt das Ergebnis dieser Simulation der Übertragung des oben beschriebenen Bildes über einen BSMC mit $p_0 = 0.35$: Das Originalbild ist links oben zu sehen. Verwendet man keinen fehlerkorrigierenden Kode, so läuft beim Empfänger ein Bild wie rechts oben gezeigt ein. Das Bild rechts unten wird empfangen, wenn man die oben genannte Hadamard-Kodierung nutzt. Statt der ursprünglichen $46 \cdot 53 \cdot 8 = 19\,504$ Bit – man beachte hierbei, dass pro Pixel nur 8 Bit Farbinformation übertragen werden muss, da es sich um ein Graustufenbild handelt – sind bei Hadamard-Kodierung $46 \cdot 53 \cdot 255 = 621\,690$ Bit zu senden. Das Bild links unten zeigt schwarz markiert die im empfangenen Bild fehlerhaften Pixel.

Die Abbildung 18 zeigt analog das Ergebnis einer Simulation an der Leistungsgrenze des Kodes: Hier wurde $p_0 = 0.39$ angenommen. ◇

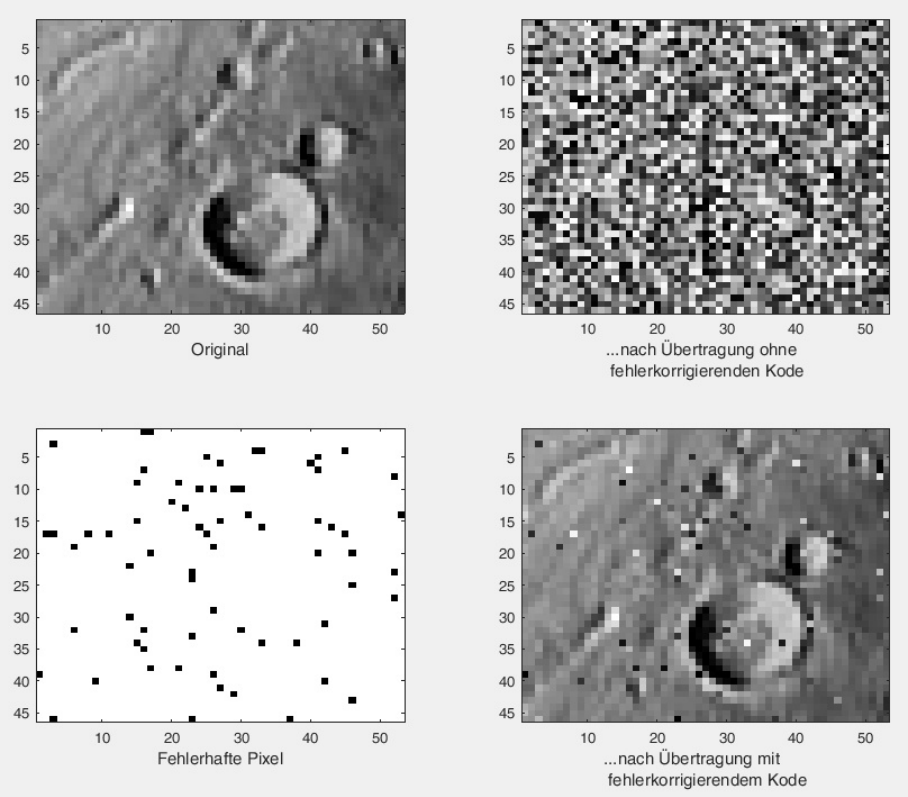


Abbildung 17: Hadamard-Kodierung bei $p_0 = 0.35$

Die Konstruktion von Hadamard-Matrizen nach Paley

Die im Folgenden angegebene Konstruktionsmethode für Hadamard-Matrizen beruht auf zahlentheoretischen Überlegungen und stammt von dem englischen Mathematiker Paley[4].

Definition 2.16: *Es sei $p > 2$ eine Primzahl. Eine Zahl $r \in \{1, \ldots, p-1\}$ heißt quadratischer Rest modulo p, falls es eine Zahl $n \in \mathbb{N}$ mit der Eigenschaft $n^2 = qp + r$, $q \in \mathbb{N}_0$, gibt.*

[4]Raymond Edward Alan Christopher Paley: englischer Mathematiker, 1907 – 1933.

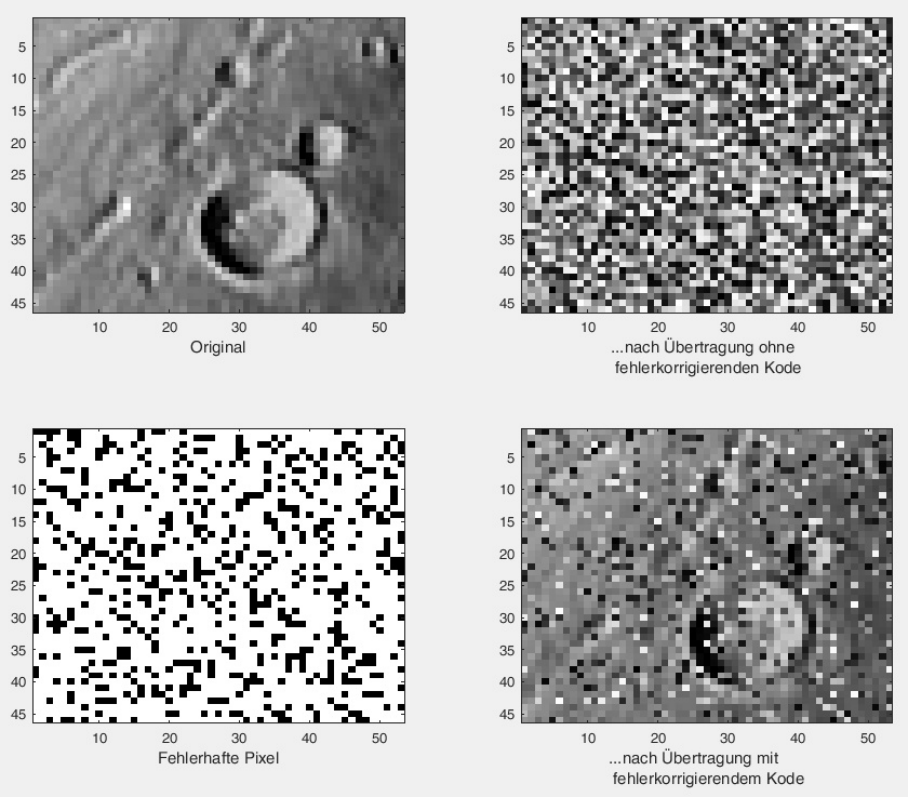


Abbildung 18: Hadamard-Kodierung bei $p_0 = 0.39$

Betrachtet man den Ringhomomorphismus

$$\mathbb{Z} \to \mathbb{F}_p,\ z \mapsto \overline{z},$$

so ist r genau dann ein quadratischer Rest modulo p, wenn $\overline{r}$ ein von 0 verschiedenes Quadrat im Körper $\mathbb{F}_p$ ist, das heißt die Form

$$\overline{r} = \alpha^2,\ \alpha \in \mathbb{F}_p^*$$

besitzt.

FESTSTELLUNG 2.17: *Zu jeder Primzahl $p > 2$ gibt es $\frac{1}{2}(p-1)$ verschiedene quadratische Reste modulo p.*

BEWEIS: Die multiplikative Gruppe $\mathbb{F}_p^*$ ist zyklisch; sei ζ ein Erzeuger. Ein Element $\alpha = \zeta^k$, $k \in \{0, \ldots, p-1\}$, ist ein Quadrat genau dann, wenn k durch 2 teilbar ist. Die Anzahl solcher Exponenten ist $\frac{1}{2}(p-1)$. □

DEFINITION 2.18: *Zu jeder Primzahl $p > 2$ wird die Funktion*

$$\chi_p : \mathbb{Z} \to \{-1, 0, 1\},\ z \mapsto \begin{cases} 1 & \textit{falls } z \notin p\mathbb{Z} \wedge \exists m \in \mathbb{N} \quad p|(m^2 - z), \\ 0 & \textit{falls } p|z, \\ -1 & \textit{sonst.} \end{cases}$$

als Legendre-Symbol [5] *zu p bezeichnet.*

Der Fall $\chi_p(z) = 1$ tritt genau dann ein, wenn gilt: Ist $z = qp + r$ mit $r \in \{1, \ldots, p-1\}$, so ist r ein quadratischer Rest modulo p.

SATZ 2.19: *Das Legendre-Symbol bei p besitzt folgende Eigenschaften:*

1. $\chi_p(z_1 z_2) = \chi_p(z_1)\chi_p(z_2)$.
2. $\sum_{k=0}^{p-1} \chi_p(k) = 0$.
3. $\forall m \in \mathbb{Z} \setminus p\mathbb{Z} \quad \sum_{k=0}^{p-1} \chi_p(k)\chi_p(k+m) = -1$.

BEWEIS: Zu 1.: Falls entweder z_1 oder z_2 durch p teilbar ist, so gilt dies auch für das Produkt $z_1 z_2$, woraus die Behauptung in diesem Fall folgt.

Sind die Zahlen z_1 und z_2 nicht durch p teilbar, so sind $\overline{z_1}, \overline{z_2} \in \mathbb{F}_p^*$. Die Gruppe $\mathbb{F}_p^*$ ist zyklisch; sei γ ein Erzeuger der Gruppe. Jedes $\alpha \in \mathbb{F}_p^*$ besitzt die Form $\alpha = \gamma^m$. Folglich ist α genau dann ein Quadrat in $\mathbb{F}_p^*$, wenn m gerade ist.

Wendet man diese Tatsache auf die Elemente $\overline{z_1} = \gamma^i$ und $\overline{z_2} = \gamma^j$ an, so ergibt sich für das Produkt

$$\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2} = \gamma^{i+j}$$

die Aussage: $\overline{z_1 z_2}$ ist genau dann ein Quadrat, wenn entweder i und j beide gerade oder beide ungerade sind. Dies ist die zu beweisende Aussage.

[5] Adrien-Marie Legendre: französischer Mathematiker, 1752 – 1833.

Zu 2.: Da es nach Feststellung 2.17 genauso viele quadratische Reste wie Nichtreste gibt, ist hier nichts weiter zu beweisen.

Zu 3.: Für $k = 0$ ist $\chi_p(k) = 0$, weswegen man den zugehörigen Summanden nicht beachten muss.

Ist $k \neq 0$, so besitzt die Gleichung

$$\overline{k}x = \overline{m} + \overline{k}$$

in dem Körper $\mathbb{F}_p$ die Lösung $\overline{x_k} = 1 + \frac{\overline{m}}{\overline{k}}$. Da m nicht durch p teilbar ist, ist stets $x_k \neq 1$. Weiter gilt für $k \neq j$:

$$1 + \frac{\overline{m}}{\overline{k}} \neq 1 + \frac{\overline{m}}{\overline{j}}.$$

Folglich nimmt x_k für die verschiedenen Werte von k genau die Werte

$$0, 2, 3, \ldots, p-1$$

an. Es folgt

$$\begin{aligned}
\sum_{k=0}^{p-1} \chi_p(k)\chi_p(k+m) &= \sum_{k=1}^{p-1} \chi_p(k)\chi_p(k+m) \\
&= \sum_{k=1}^{p-1} \chi_p(k)\chi_p(kx_k) \\
&= \sum_{k=1}^{p-1} \chi_p(k)\chi_p(k)\chi_p(x_k) \\
&= \sum_{k=1}^{p-1} \chi_p(x_k) \\
&= \sum_{\ell \in \{0,2,\ldots,p-1\}} \chi_p(\ell) \\
&= -\chi_p(1) = -1,
\end{aligned}$$

wobei man im letzten Schritt die Feststellung 2.17 verwendet. □

Definition 2.20: *Es sei $p > 2$ eine Primzahl. Die Matrix $J \in \mathbb{Z}^{p \times p}$ der Form*

$$J_p = (\chi_p(i-j))_{i,j \in \{0,\ldots,p-1\}}$$

nennt man Jacobsthal-Matrix[6] *zu p.*

[6]Ernst Jacobsthal: deutscher Mathematiker, 1882 – 1965.

Je nach den Eigenschaften der Primzahl p besitzt J_p bestimmte Symmetrieeigenschaften:

LEMMA 2.21: *Besitzt die Primzahl p die Form $4k-1$, so gilt $\chi_p(-1) = -1$ und die Jacobsthal-Matrix J_p ist antisymmetrisch: $J_p = -J_p^t$.*

BEWEIS: Es sei α ein Erzeuger der Gruppe $\mathbb{F}_p^*$. Dann gilt

$$1 = \alpha^{p-1} = (\alpha^{\frac{1}{2}(p-1)})^2,$$

also

$$\alpha^{\frac{1}{2}(p-1)} = -1,$$

denn da α ein Erzeuger von $\mathbb{F}_p^*$ ist, kann nicht $\alpha^{\frac{1}{2}(p-1)} = 1$ gelten. Nun folgt aber aus $p = 4k-1$ die Gleichung $p-1 = 4k-2$, also

$$\alpha^{\frac{1}{2}(p-1)} = \alpha^{2k-1},$$

womit -1 kein Quadrat ist.

Für die Koeffizienten a_{ij} der Jacobsthal-Matrix gilt dann

$$a_{ji} = \chi_p(j-i) = \chi_p((-1)(i-j)) = \chi_p(-1)\chi_p(i-j) = -a_{ij}.$$

□

Nun kommen wir zum Grund für die Betrachtung der oben eingeführten Begriffe:

SATZ 2.22: *Es sei p eine Primzahl mit der Eigenschaft $4|(p+1)$. Dann gelten:*

1. *Die Jacobsthal-Matrix J_p besitzt die Eigenschaften*

$$J_p J_p^t = pE - \mathbf{1}, \quad J_p\mathbf{1} = \mathbf{1}J_p = 0,$$

wobei $\mathbf{1} \in \mathbb{Z}^{p\times p}$ die Matrix ist, deren Koeffizienten alle gleich 1 sind.

2. *Die Matrix*

$$H := \begin{pmatrix} 1 & v^t \\ v & J_p - E \end{pmatrix} \in \mathbb{Z}^{p+1\times p+1},\ v^t = (1,\ldots,1) \in \mathbb{Z}^p,$$

ist eine Hadamard-Matrix (vom Paley-Typ).

BEMERKUNG: Nach dem Dirichlet'schen[7] Primzahlsatz gibt es in jeder Folge $(a+kb)_{k\in\mathbb{N}}$ mit teilerfremden Zahlen $a, b \in \mathbb{Z}$ unendlich viele Primzahlen. Folglich gibt es unendlich viele Primzahlen der Form $p = 4k - 1$.

BEWEIS: Zu 1.: Es seien a_{ij} die Koeffizienten der Matrix $J_p J_p^t$. Dann gilt

$$a_{ii} = \sum_{j=0}^{p-1} \chi_p(i-j)\chi_p(i-j) = p - 1.$$

Weiter hat man für $i \neq j$

$$\begin{aligned} a_{ij} &= \sum_{k=0}^{p-1} \chi_p(i-k)\chi_p(j-k) \\ &= \sum_{k=0}^{p-1} \chi_p(k-i)\chi_p(k-j) \\ &= \sum_{\ell=0}^{p-1} \chi_p(\ell)\chi_p(\ell+(i-j)) \\ &= -1, \end{aligned}$$

nach Satz 2.19. Die verbleibende Behauptung folgt direkt aus Feststellung 2.17.

Zu 2.: Nach den Regeln der Matrixmultiplikation, dem bereits Bewiesenen und Lemma 2.21 ergibt sich:

$$HH^t = \begin{pmatrix} 1 & v^t \\ v & J_p - E \end{pmatrix} \begin{pmatrix} 1 & 0 \\ v & J_p^t - E \end{pmatrix} = (p+1)E$$

□

BEISPIEL 2.23: Wir betrachten die Primzahl $p = 7$. Die quadratischen Reste modulo 7 sind die Zahlen $1 = 1^2$, $4 = 2^2$ und 2; letztere, weil $3^2 = 1 \cdot 7 + 2$

[7] Johann Peter Gustav Lejeune Dirichlet, französischer/deutscher Mathematiker, 1805 – 1859

gilt. Für die Jacobsthal-Matrix J_7 ergibt sich daher:

$$J_7 = \begin{pmatrix} \chi_7(0) & \chi_7(1) & \chi_7(2) & \chi_7(3) & \chi_7(4) & \chi_7(5) & \chi_7(6) \\ -\chi_7(1) & \chi_7(0) & \chi_7(1) & \chi_7(2) & \chi_7(3) & \chi_7(4) & \chi_7(5) \\ -\chi_7(2) & -\chi_7(1) & \chi_7(0) & \chi_7(1) & \chi_7(2) & \chi_7(3) & \chi_7(4) \\ -\chi_7(3) & -\chi_7(2) & -\chi_7(1) & \chi_7(0) & \chi_7(1) & \chi_7(2) & \chi_7(3) \\ -\chi_7(4) & -\chi_7(3) & -\chi_7(2) & -\chi_7(1) & \chi_7(0) & \chi_7(1) & \chi_7(2) \\ -\chi_7(5) & -\chi_7(4) & -\chi_7(3) & -\chi_7(2) & -\chi_7(1) & \chi_7(0) & \chi_7(1) \\ -\chi_7(6) & -\chi_7(5) & -\chi_7(4) & -\chi_7(3) & -\chi_7(2) & -\chi_7(1) & \chi_7(0) \end{pmatrix}$$

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

Die zugehörige Hadamard-Matrix nach Satz 2.22 ergibt sich dann zu

$$H_8 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & 1 & -1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 & 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & -1 & 1 & 1 & -1 & 1 \\ 1 & 1 & -1 & -1 & -1 & 1 & 1 & -1 \\ 1 & -1 & 1 & -1 & -1 & -1 & 1 & 1 \\ 1 & 1 & -1 & 1 & -1 & -1 & -1 & 1 \\ 1 & 1 & 1 & -1 & 1 & -1 & -1 & -1 \end{pmatrix}.$$

$\diamond$

2.3 Maximum-Likelihood-Dekodierung

Mit Hilfe der Hamming-Metrik kann man das Problem der Erkennung und Korrektur von Übertragungsfehlern durch eine geeignete Dekodierungsabbildung d zu einem binären Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ geometrisch betrachten: Wird das Kodewort $x = c(a) \in C$ gesendet, so kann man das empfangene Wort $y \in \mathbb{F}_2^\ell$ eindeutig in der Form

$$y = x + z$$

mit einem $z \in \mathbb{F}_2^\ell$ schreiben, dem (Übertragungs-)Fehlervektor: Für die Komponenten z_i von z gilt genau dann $z_i = 1$, wenn das i-te Bit von x durch einen Übertragungsfehler verändert wurde. Die Wahrscheinlichkeit für das Auftreten des Fehlervektors z in einem BSMC mit Bit-Fehlerwahrscheinlichkeit p_0 ist

$$b(z) = p_0^{w(z)}(1-p_0)^{\ell - w(z)} = p_{\mathrm{rc}}(y|x),$$

siehe (16). Diese Wahrscheinlichkeit sinkt mit steigendem Gewicht von z bei $p_0 < \frac{1}{2}$: Betrachtet man nämlich die Funktion

$$p(t) := p_0^t(1-p_0)^{\ell - t},$$

so gilt

$$p'(t) = (\ln(p_0) - \ln(1-p_0))p_0^t(1-p_0)^{\ell-t},$$

womit p für $p_0 \in (0, \frac{1}{2})$ streng monoton fällt und für $p_0 \in (\frac{1}{2}, 1)$ streng monoton wächst.

Definition 2.24: *Die Dekodierungsabbildung $d : D \to \mathbb{A}$ zu dem binären Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ heißt Maximum-Likelihood-Dekodierung (ML-Dekodierung), falls gilt:*

$$\forall y \in D \quad h(y, d(y)) = \min(h(y,x) : x \in C).$$

Das Wort y wird also so dekodiert, dass die Wahrscheinlichkeit

$$p_{\mathrm{rc}}(y|x) = b(y - d(y))$$

maximal ist.

Bemerkungen:

1. ML-Dekodierungen von c sind im Allgemeinen nicht eindeutig bestimmt, da es mehrere Kodewörter mit minimalem Abstand zu gegebenem y geben kann.

2. In welcher Form man eine ML-Dekodierung effizient implementiert, bleibt an dieser Stelle völlig offen: Es ist klar, dass die Suche nach Elementen mit minimalem Abstand von einem gegebenen Element $y \in \mathbb{F}_2^\ell$ bei großem ℓ eine algorithmische Herausforderung darstellt. Auf Compact Discs wird zum Beispiel ein Kode verwendet, der $(2^8)^{32}$ Wörter zulässt, eine Zahl von der Größenordnung 10^{77}.

Es sei $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein binärer Blockkode und wie stets $C = c(\mathbb{A})$. Für jedes $e \in \{0, \ldots, \ell - 1\}$ liegen außerhalb der Kugel $B[x, e]$, $x \in C$, nur solche Kodewörter $y \in C$, die sich an mindestens $e + 1$ Stellen von x unterscheiden. Ob solche Kodewörter existieren, hängt von ihrer Verteilung im Raum $\mathbb{F}_2^\ell$ ab.

Im Folgenden sei für eine Zahl $\alpha \in \mathbb{R}^{\geq 0}$

$$[\alpha] := \max\{n \in \mathbb{N} : n \leq \alpha\},$$

die so genannte *Gauß-Klammer*.

Es sei c ein binärer Blockkode mit der Eigenschaft $h_{\min}(c) \geq 2e + 1$ für ein $e \in \{0, \ldots, [\frac{\ell}{2}] - 1\}$. Wird ein Kodewort $x \in C$ durch Störung im BSMC in das Wort $y \in \mathbb{F}_2^\ell$ übertragen und ist bekannt, dass y sich an höchstens e Stellen von x unterscheidet, so liegt in der Kugel $B[y, e]$ genau ein $x' \in C$, nämlich x selbst. Denn nach der Dreiecksungleichung gilt für $x, x' \in B[y, e]$ die Ungleichung

$$h(x, x') \leq h(x, y) + h(y, x') \leq 2e.$$

Dies motiviert die

Definition 2.25: *Ein binärer Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ heißt e-fehlerkorrigierend, falls die Ungleichung $h_{\min}(c) \geq 2e+1$ für ein $e \in \{0, \ldots, [\frac{\ell}{2}]-1\}$ vorliegt.*

Wie durch die Namensgebung impliziert gilt nun:

Feststellung 2.26: *Ist ein Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ e-fehlerkorrigierend, so gilt für jede ML-Dekodierung $d : D \to \mathbb{A}$ von c:*

$$\forall x \in C, y \in D \quad h(x, y) \leq e \Rightarrow d(y) = x. \tag{25}$$

Mit anderen Worten: Ein an höchstens e Stellen gestörtes Sendekodewort wird durch eine ML-Dekodierung entweder wiederhergestellt oder es liegt ein Dekodierungsversagen vor. Insbesondere ist die ML-Dekodierung auf der Menge

$$(\bigcup_{x \in C} B[x, e]) \cap D$$

durch c eindeutig bestimmt.

Gilt andererseits für einen Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$, dass jedes an höchstens e Stellen gestörte Sendekodewort durch eine ML-Dekodierung wiederhergestellt wird, so ist $h_{\min}(c) \geq 2e + 1$, das heißt c ist e-fehlerkorrigierend.

Beweis: Nach der Dreiecksungleichung gilt für je zwei verschiedene Kodewörter $x, x' \in C$ eines e-fehlerkorrigierenden Kodes:

$$B[x, e] \cap B[x', e] = \emptyset. \tag{26}$$

Hieraus ergeben sich direkt alle Behauptungen über c.

Werden andererseits bis zu e Fehler in jedem Kodewort $x \in C$ eines Kodes c bei ML-Kodierung korrigiert, so muss für verschiedene $x, x' \in C$ die Gleichung (26) also die Ungleichung $h(x, x') > 2e$ gelten. Folglich ist $h_{\min}(c) \geq 2e + 1$. □

Es stellt sich die Frage, wie man e-fehlerkorrigierende Kodes findet. Prinzipiell handelt es sich um ein endliches Problem: man könnte alle Teilmengen $C \subseteq \mathbb{F}_2^\ell$ der Kardinalität $|\mathbb{A}|$ auf die gewünschte Eigenschaft testen. Dies ist jedoch nicht effizient durchführbar, da es

$$\binom{2^\ell}{|\mathbb{A}|} = \frac{2^\ell!}{|\mathbb{A}|!(2^\ell - |\mathbb{A}|)!}$$

solcher Teilmengen gibt. Hinzu kommt, dass ein praxistaugliches Paar (c, d) folgende, zum Teil konkurrierende Eigenschaften besitzen sollte:

(1) Die Fehlerwahrscheinlichkeit $p_{\text{tot}}(c, d)$ soll klein sein.

(2) Die Informationsrate $R(c)$ soll hoch sein.

(3) Die Minimaldistanz $h_{\min}(c)$ soll groß sein.

(4) Die Dekodierungsabbildung d soll schnell berechenbar sein.

Fehlerkorrigierende Kodes müssen also systematisch konstruiert werden. Hierzu ist die Kenntnis von Abhängigkeiten zwischen verschiedenen durch einen binären Blockkode definierten Größen nützlich. Ein erstes Resultat in dieser Richtung ist:

FESTSTELLUNG 2.27 (Hamming-Schranke): *Für einen binären Blockkode* $c : \mathbb{A} \to \mathbb{F}_2^\ell$ *der Minimaldistanz* m *gilt*

$$|\mathbb{A}| \sum_{i=0}^{[\frac{m-1}{2}]} \binom{\ell}{i} \leq 2^\ell.$$

BEWEIS: Es sei $r := [\frac{m-1}{2}]$. Dann gilt für zwei verschiedene Kodewörter $x, x' \in C$ stets

$$B[x, r] \cap B[x', r] = \emptyset,$$

denn für ein $y \in B[x, r] \cap B[x', r]$ gilt nach der Dreiecksungleichung

$$h(x, x') \leq h(x, y) + h(y, x') \leq 2[\frac{m-1}{2}] \leq m - 1,$$

ein Widerspruch.

Die Aussage folgt nun aus Gleichung (12). □

BEMERKUNG: Wie ihr Beweis zeigt, kann man Feststellung 2.27 auch geometrisch als Kugelpackungsproblems im Raum $\mathbb{F}_2^\ell$ interpretieren.

BEISPIEL 2.28: Wir wenden dieses Resultat an um zu sehen, was man über binäre Blockkodes c sagen kann, die 1-fehlerkorrigierend aber nicht 2-fehlerkorrigierend sind. Es gilt also $m := h_{\min}(c) \in \{3, 4\}$ und damit

$$[\frac{m-1}{2}] = 1,$$

woraus sich die Ungleichung

$$|\mathbb{A}|(1 + \ell) \leq 2^\ell.$$

ergibt.

Will man etwa einfache deutsche Texte senden, so genügt ein Alphabet mit $32 = 2^5$ Buchstaben: 26 Großbuchstaben plus einige Satz- und Sonderzeichen, sowie das Leerzeichen. Man erhält also

$$1 + \ell \leq 2^{\ell-5}.$$

Folglich muss der gesuchte Kode eine Blocklänge $\ell \geq 9$ besitzen. ◇

Beispiel 2.29: Wir betrachten erneut die Situation aus Beispiel 2.6 und wollen einen 1-fehlerkorrigierenden Kode für DNS-Sequenzen finden. Feststellung 2.27 liefert die Ungleichung

$$4(1+\ell) \leq 2^{\ell},$$

die für $\ell \geq 5$ erfüllt ist. Die Existenz eines 1-fehlerkorrigierenden Kodes $c : \{A, C, G, T\} \to \mathbb{F}_2^5$ bedeutet, dass es eine 4-elementige Teilmenge $C \subset \mathbb{F}_2^5$ gibt, in der je zwei Elemente mindestens die Hamming-Distanz 3 besitzen. Sei $C = \{x_1, x_2, x_3, x_4\}$ eine solche Menge, dann besitzt die Translation

$$C - x_1 = \{0, x_2 - x_1, x_3 - x_1, x_4 - x_1\}$$

dieselbe Eigenschaft. Wir können also ohne Einschränkung annehmen, dass $x_1 = 0$ gilt. Es folgt $w(x_i) \geq 3$, $i = 2, 3, 4$. Das einzige Wort $y \in \mathbb{F}_2^5$ vom Gewicht 5 besitzt einen Abstand ≤ 2 von jedem Wort vom Gewicht ≥ 3. Folglich ist $w(x_i) \in \{3, 4\}$, womit es zwei Kodewörter vom gleichen Gewicht 3 oder 4 gibt. Zwei verschiedene Wörter des Gewichts 4 besitzen den Abstand 2. Folglich kann man ohne Einschränkung $w(x_2) = w(x_3) = 3$ annehmen.

Zusammenfassend suchen wir also zwei Wörter x_2, x_3 vom Gewicht 3 mit $h(x_2, x_3) \geq 3$ und ein Wort x_4 vom Gewicht 3 oder 4 mit $h(x_2, x_4) \geq 3$ und $h(x_3, x_4) \geq 3$. Diese Anforderungen werden zum Beispiel von

$$\begin{aligned} x_2 &= (1,1,1,0,0)^t \\ x_3 &= (0,0,1,1,1)^t \\ x_4 &= (1,1,0,1,1)^t \end{aligned}$$

erfüllt. Es gilt dann:

$$h(x_1, x_2) = h(x_1, x_3) = h(x_2, x_4) = h(x_3, x_4) = 3,\ h(x_1, x_4) = h(x_2, x_3) = 4,$$

womit c die Minimaldistanz 3 besitzt.

Wir wollen nun von dem erhaltenen binären Blockkode

$$c : \{A, C, G, T\} \to \mathbb{F}_2^5, c(A) = 0, c(C) = x_2, c(G) = x_3, c(T) = x_4$$

eine ML-Dekodierung bestimmen. Wie sich zeigt, ist diese nicht eindeutig bestimmt: Die Abbildung 19 stellt eine ML-Dekodierung dar. Hierbei gelten:

- Grün gefüllte Kreise sind Kodewörter, alle anderen Wörter sind gelb gefüllt.

- Hellgelb gefüllte Kreise stehen für Wörter, die bei jeder ML-Dekodierung auf die gleiche Weise dekodiert werden. Dunkelgelb gefüllte Kreise dagegen stehen für Wörter, deren Zuordnung bei der Definition der Dekodierungsvorschrift frei festgelegt werden kann.
- Die Farbe der Kreislinie symbolisiert die Dekodierungsvorschrift: Es steht grün für A, violett für C, blau für G und rot für T.
- Kreise mit durchgezogener Kreislinie stehen für Wörter mit Hamming-Distanz ≤ 1 von einem Kodewort.
- Kreise mit durchbrochener Kreislinie stehen für Wörter mit Hamming-Distanz 2 zu mindestens einem Kodewort. Tatsächlich besitzen alle diese Wörter Hamming-Distanz 2 zu mindestens zwei Kodewörter.

Im Beispiel gibt es acht Wörter, welche die Distanz 2 von zwei Kodewörter besitzen:

$$\begin{aligned} K := \{ \quad & (1,0,0,1,0)^t, (1,0,0,0,1)^t, (0,1,0,1,0)^t, (0,1,0,0,1)^t, \\ & (1,0,1,1,0)^t, (1,0,1,0,1)^t, (0,1,1,1,0)^t, (0,1,1,0,1)^t \quad \}. \end{aligned}$$

Falls man beim Dekodieren vorsichtig sein möchte, kann man aus der im Beispiel angegebenen ML-Dekodierung $d : \mathbb{F}_2^5 \to \{A, C, G, T\}$ die unvollständige ML-Dekodierung

$$d|_D : D \to \{A, C, G, T\},\ D := \mathbb{F}_2^5 \setminus K$$

erzeugen. Die Wahrscheinlichkeit dafür, dass ein beliebiges Kodewort $x \in C$ korrekt dekodiert wird, ist dann gleich der Wahrscheinlichkeit dafür, dass x in höchstens einem Bit gestört wird, also

$$(1-p_0)^5 + 5p_0(1-p_0)^4.$$

Denn besitzt der Übertragungsfehler z ein Gewicht $w(z) \geq 2$, so gilt entweder $x + z \notin D$, womit keine Dekodierung stattfindet, oder es gibt genau ein Kodewort x' mit $h(x', y) \leq 1$. Dann wird y zu x' dekodiert, wobei aber $x' \neq x$ gilt.

Folglich ist die totale Fehlerwahrscheinlichkeit (Falschdekodierung und Dekodierungsversagen)

$$p_{\,\mathrm{tot}}(c, d|_D) = 1 - (1-p_0)^5 - 5p_0(1-p_0)^4.$$

$\diamond$

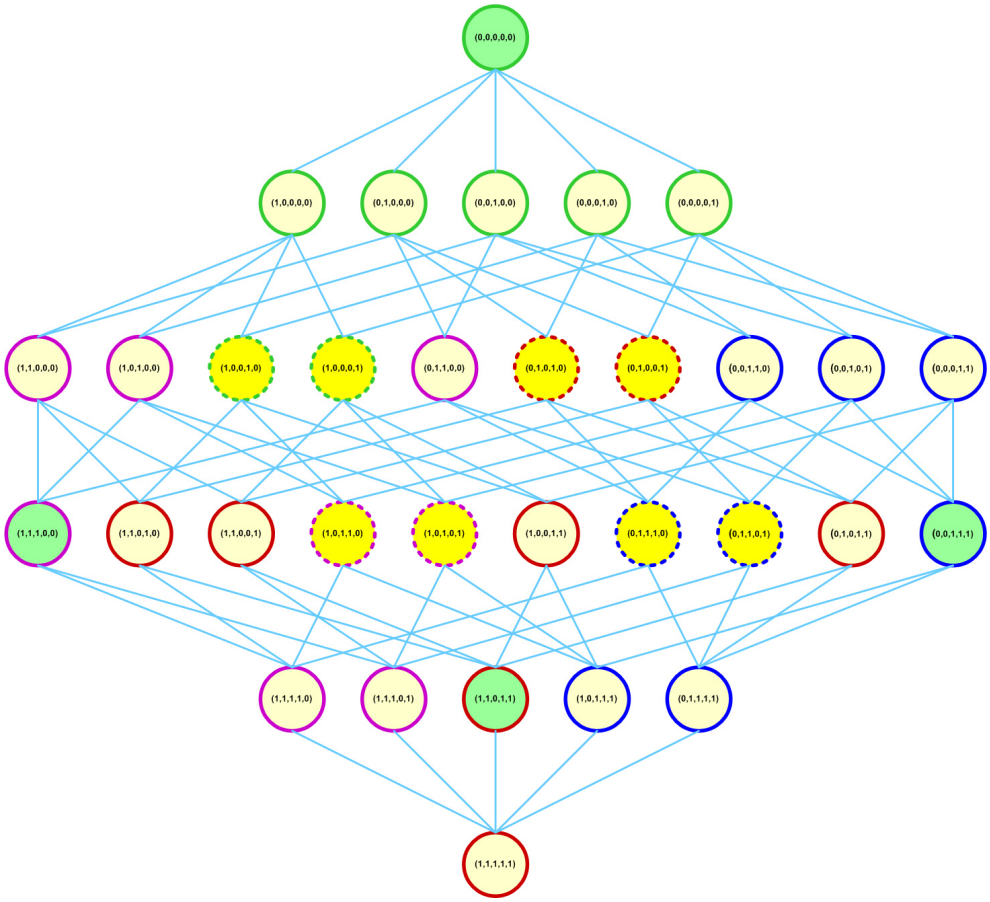


Abbildung 19: ML-Dekodierung von Beispiel 2.29

2.4 Perfekte Kodes

Es ist naheliegend und praxisrelevant nach Kodes zu suchen, für welche die ML-Dekodierung mit Sicherheit eine vorgegebene Maximalzahl e von Fehlern behebt. Solche Kodes nennt man perfekt; die präzise Definition ist:

DEFINITION 2.30: *Ein binärer Blockkode* $c : \mathbb{A} \to \mathbb{F}_2^\ell$ *heißt perfekt, falls es ein* $e \in \{0, 1, \ldots, \ell\}$ *mit der Eigenschaft*

$$\forall y \in \mathbb{F}_2^\ell \quad |B[y, e] \cap C| = 1$$

gibt. Man nennt c *dann auch* e*-perfekt.*

Grundlegende Eigenschaften perfekter Kodes sind im folgenden Satz zusammengefasst.

SATZ 2.31: *Für einen e-perfekten Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ gelten:*

1. *Die ML-Dekodierung ist eindeutig bestimmt; sie ordnet jedem $y \in \mathbb{F}_2^\ell$ das eindeutige Kodewort in der Kugel $B[y, e]$ zu.*
2. *$h_{\min}(c) = 2e + 1$.*
3. *Es gilt die Gleichung*

$$|\mathbb{A}| \sum_{i=0}^{e} \binom{\ell}{i} = 2^\ell. \tag{27}$$

BEWEIS: Zu 1.: Nach Definition einer ML-Dekodierung und der Perfektheit eines Kodes ist dies klar.

Zu 2.: Es seien $x, x' \in C$ zwei verschiedene Kodewörter und $e' := [\frac{h(x,x')}{2}]$. Dann gibt es ein y mit $h(x, y) = e'$ und $e' \leq h(x', y) \leq e' + 1$. Wegen der e-Perfektheit von c gilt dann entweder $h(x, y) = h(x', y) = e'$ und $e' > e$, woraus $h(x, x') = 2e' > 2e$ also $h(x, x') \geq 2e + 1$ folgt. Oder es gilt $h(x', y) = e' + 1$ und damit $h(x, x') = 2e' + 1 > 2e + 1$.

Es seien nun $x \in C$ und $y \in \mathbb{F}_2^\ell$ mit $h(x, y) = e + 1$. Dann gibt es genau ein Kodewort $x' \in B[y, e]$. Es folgt

$$h(x, x') \leq h(x, y) + h(y, x') \leq e + 1 + e = 2e + 1.$$

Zu 3.: Die Kugeln $B[x, e]$ sind nach Voraussetzung paarweise disjunkt und jedes $y \in \mathbb{F}_2^\ell$ liegt in genau einer dieser Kugeln. Die Behauptung folgt nun aus Gleichung (12). □

BEMERKUNG: Das vorliegende Argument zeigt übrigens, dass man Gleichung (27) wie folgt deuten kann: Für einen e-perfekten Kode lässt sich der Raum $\mathbb{F}_2^\ell$ ohne Rest mit Kugeln vom Radius e vollpacken.

KOROLLAR 2.32: *Für einen e-perfekten Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ sind $|\mathbb{A}|$ und $\sum_{i=0}^{e} \binom{\ell}{i}$ Potenzen von 2.*

Als Beispiele perfekter Kodes gibt es zunächst zwei triviale Fälle:

- $|\mathbb{A}| = 2^\ell$ und $e = 0$: Jedes Wort ist ein Kodewort. Eine Fehlerkorrektur ist unmöglich.

- $|\mathbb{A}| = 1$ und $e = \ell$: Jedes Wort wird richtig dekodiert, da es nur ein Kodewort gibt.

Etwas weniger trivial ist die im folgenden Beispiel beschriebene Familie perfekter Kodes:

BEISPIEL 2.33 (WIEDERHOLUNGSKODE): Es sei $\mathbb{A} = \{a_1, a_2\}$, $\ell = 2e+1$ und $c(a_1) = (0, \ldots, 0)^t$, $c(a_2) = (1, \ldots, 1)^t$. Dann liegen in der Kugel $B[0, e]$ alle Wörter $y \in \mathbb{F}_2^\ell$ vom Gewicht $w(y) \leq e$. Besitzt andererseits y ein Gewicht $w(y) > e$, so ist die Anzahl der 0-Bits in y höchstens gleich

$$\ell = 2e + 1 - (e + 1) = e.$$

Folglich ist $h(y, c(a_2)) \leq e$. Insgesamt zeigt dies

$$\mathbb{F}_2^\ell = B[c(a_1), e] \cup B[c(a_2), e],\ B[c(a_1), e] \cap B[c(a_2), e] = \emptyset$$

und damit die e-Perfektheit des Kodes.

Die beschriebenen Kodes heißen Wiederholungskodes, weil man $a_1 = 0$ und $a_2 = 1$ wählen kann und die Kodierung im ℓ-maligen Wiederholen des jeweiligen Symbols besteht. $\diamond$

Satz 2.31 legt nahe alle Zahlen ℓ, e und $|\mathbb{A}|$ zu ermitteln, für die Gleichung (27) gilt. Nur zu solchen Zahlenkombinationen kann es perfekte Kodes geben. Wie man leicht sieht, reduziert sich das Problem darauf alle $e \in \mathbb{N}$ zu finden, für die die Zahl

$$\sum_{i=0}^{e} \binom{\ell}{i}$$

eine Potenz von 2 ist, wobei $e \leq \ell$ gelten muss. Ausgehend von solchen Überlegungen ist es 1971 gelungen den folgenden eigentümlichen Satz zu beweisen:

SATZ 2.34 (A. Tietäväinen, A. Perko, 1971): *Es sei $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein e-perfekter Kode. Dann gibt es für die Zahlen $\ell, e, |\mathbb{A}|$ nur die folgenden Möglichkeiten und zu jeder dieser Möglichkeiten existieren e-perfekte Kodes:*

1. *$\ell \in \mathbb{N}$, $e = 0$ und $|\mathbb{A}| = 2^\ell$,*
2. *$\ell \in \mathbb{N}$, $e = \ell$ und $|\mathbb{A}| = 1$,*

3. $\ell = 2^r - 1$, $e = 1$, $|\mathbb{A}| = 2^{2^r-1-r}$ *für* $r \in \mathbb{N}$, $r \geq 2$,

4. $\ell = 23$, $e = 3$, $|\mathbb{A}| = 2^{12}$,

5. $\ell \in \mathbb{N}$ *ungerade,* $e = \frac{\ell-1}{2}$, $|\mathbb{A}| = 2$.

Ein Beweis dieses Satzes ist jenseits der Möglichkeiten dieser Vorlesung. Die folgenden mit diesem Satz zusammenhängenden Informationen sind aber dennoch interessant:

- $\ell = 90$ und $e = 2$ lösen die Gleichung (27). Man kann aber beweisen, dass es keinen 2-perfekten Kode mit diesen Parametern gibt.
- Kodes mit den unter Punkt 3 angegebenen Parametern werden im nächsten Kapitel konstruiert.
- Ein perfekter Kode mit den unter Punkt 4 angegebenen Parametern wurde von dem Schweizer Mathematiker und Physiker Marcel Golay (1902 – 1989) im Jahr 1949 publiziert. Der Artikel gilt bis heute als wesentlicher Beitrag zur Kodierungstheorie und ist nur knapp eine Seite lang:

  M. J. E. Golay, Notes on Digital Coding, Proc. IRE 37 (1949), p. 657.

  Eine Variante dieses Kodes wurde für die Datenübertragung von der am 5. September 1977 vom Kennedy Space Center gestarteten Raumsonde Voyager 1 genutzt. Die Geschwister-Raumsonden Voyager 1 und 2 gehören zu den erfolgreichsten und beeindruckendsten Raumfahrtprojekten der Menschheit. Die von ihnen im Lauf von Jahrzehnten erfassten Daten haben das Wissen über unser Sonnensystem in ungeahnter Weise erweitert. Beide Sonden sind noch immer in Betrieb; Voyager 1 hat am 25. August 2012 das Sonnensystem verlassen.

Die Bestimmung der totalen Fehlerwahrscheinlichkeit eines perfekten Kodes mit ML-Dekodierung ist besonders einfach:

Satz 2.35: *Für einen e-perfekten Kode c der Länge* ℓ *gilt*

$$p_{\,\mathrm{tot}}(c, d) = 1 - \sum_{k=0}^{e} \binom{\ell}{k} p_0^k (1 - p_0)^{\ell-k},$$

wobei p_0 *die Übertragungsfehlerwahrscheinlichkeit des verwendeten BSMC ist.*

Abbildung 20: Marcel Jules Edouard Golay, September 1960
(Courtesy AIP Emilio Segrè Visual Archives)

Marcel Golay war ab 1962 nach einer Tätigkeit für das United States Army Signal Corps in der Medizintechnik für das Unternehmen PerkinElmer tätig. Er ist unter anderem Erfinder eines Infrarotsensors und des Kapillargaschromatographen.

Für die in der Anwendung interessanten Fälle aus Satz 2.34 ergibt sich also:

- *Fall 3:* $p_{\text{tot}}(c,d) = 1-(1-p_0)^{2^r-1}-(2^r-1)p_0(1-p_0)^{2^r-2}$.
- *Fall 4:*

  $$p_{\text{tot}}(c,d) = 1-(1-p_0)^{23}-23p_0(1-p_0)^{22}-253p_0^2(1-p_0)^{21}-1771p_0^3(1-p_0)^{20}.$$

- *Fall 5:* $p_{\text{tot}}(c,d) = 1-\sum\limits_{k=0}^{\frac{\ell-1}{2}}\binom{\ell}{k}p_0^k(1-p_0)^{\ell-k}$.

Beweis: Wir verwenden die Formel (22)

$$p_{\text{tot}}(c,d) = 1-\sum_{a\in\mathbb{A}}p_{\mathbb{A}}(a)\sum_{y\in\mathbb{F}_2^\ell:\, d(y)=c(a)}p_0^{h(c(a),y)}(1-p_0)^{\ell-h(c(a),y)},$$

wobei d die ML-Dekodierung ist. Es gilt folglich $d(y) = c(a)$ genau dann, wenn $h(c(a),y) \leq e$. Um die totale Fehlerwahrscheinlichkeit zu berechnen, muss also für jedes $k \leq e$ die Anzahl der Wörter y mit $h(c(a),y) = k$ bestimmt werden. Hiervon gibt es $\binom{\ell}{k}$ Stück, da ein solches Wort durch $c(a)$ und die Indizes der k geänderten Komponenten von $c(a)$ festgelegt ist. Es

folgt

$$\sum_{y \in \mathbb{F}_2^\ell \colon d(y)=c(a)} p_0^{h(c(a),y)} (1-p_0)^{\ell - h(c(a),y)} = \sum_{k=0}^{e} \binom{\ell}{k} p_0^k (1-p_0)^{\ell-k},$$

und damit die Behauptung. □

Die Formeln aus Satz 2.35 lassen sich für den Vergleich von Kodes nutzen. Wählt man im Fall 3 beispielsweise $r = 4$, so erhält man einen Kode für Alphabete mit (bis zu) 2^{11} Symbolen und einer Blocklänge von $\ell = 15$. Es kann also interessant sein einen solchen Kode mit einem Kode zum Fall 4 zu vergleichen. In Abbildung 21 sind die totalen Fehlerraten im Intervall $[0, 0.08]$ dargestellt. Man beachte hierbei, dass typische, in der Anwendung vorkommende Bitfehlerraten sehr klein sind. Beispielsweise liegt die Bitfehlerrate von Solid State Disks (SSDs) zwischen 10^{-6} und 10^{-3} (Experimente von Nila Fang, publiziert im November 2015 auf Linkedin). Hierbei ist zu beachten, dass die Bitfehlerrate von SSDs im Lauf ihrer Nutzungszeit zunimmt.

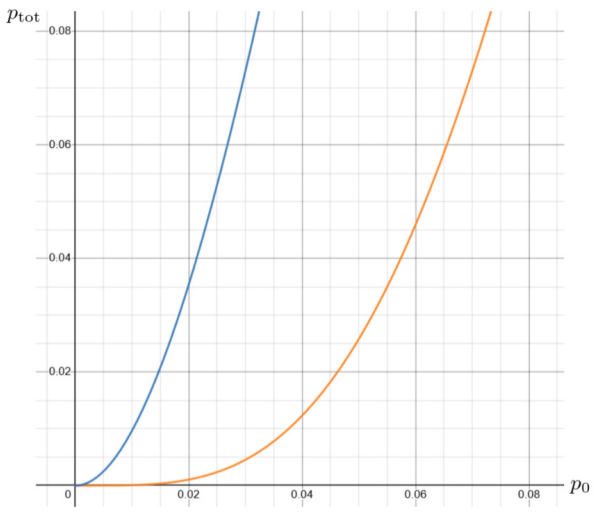


Abbildung 21: Totale Fehlerwahrscheinlichkeiten eines Kodes vom Typ 3 ($r = 4$, blau) und vom Typ 4 (orange)

2.5 Der Satz von Shannon

Die Abbildung 22 zeigt den amerikanische Mathematiker und Elektroingenieur Claude Elwood Shannon (1916 – 2001), dessen Forschungsarbeiten ihm den Titel »Vater der Informationstheorie« einbrachten. Im Jahr 1948 publizierte er die wegweisende Arbeit *A Mathematical Theory of Communication* im *Bell System Technical Journal*, in dem er unter anderem bewies, dass es salopp gesprochen beliebig »gute« binäre Blockkodes gibt. Im vorliegenden Abschnitt wird dieser für die Kodierungstheorie grundlegende Satz formuliert und bewiesen.

Abbildung 22: Claude Elwood Shannon

Links: Einschreibefotografie University of Michigan 1932
(Courtesy Bentley Historical Library)
Rechts: 1985 Verleihung des Kyoto-Preises

THEOREM 2.36 (C.E. Shannon, 1948): *Man betrachte einen BMSC mit Bitfehlerrate* $p_0 < \frac{1}{2}$ *und Kapazität* C*, sowie ein Alphabet* $\mathbb{A}$.

Es seien $\epsilon > 0$ *und* $0 < R < C$.

Dann existieren ein binärer Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ *und eine zugehörige Dekodierungsabbildung* $d : \mathbb{F}_2^\ell \to \mathbb{A}$ *mit den Eigenschaften:*

1. $p_{\text{tot}}(c, d) < \epsilon$,
2. $R(c) > R$.

BEMERKUNG: Der Beweis des Satzs von Shannon ist leider nicht konstruktiv, das heißt er kann nicht als Grundlage für einen Algorithmus zum Ermitteln eines Kodes mit den angebenen Eigenschaften genutzt werden. Tatsächlich ist ein solcher Algorithmus nicht bekannt. Der Beweis zeigt aber, dass sich die Suche nach »guten« Kodes lohnt.

Shannons Existenzbeweis beruht auf stochastischen Betrachtungen. Folgende Tatsachen werden dabei benutzt:

1. Ist $X : \Omega \to \{0, 1, \ldots, \ell\}$ eine binomialverteilte Zufallsvariable zur Wahrscheinlichkeit p_0, so ist ihr Erwartungswert $E(X) = \ell p_0$ und ihre Varianz $V(X) = \ell p_0(1 - p_0)$.

2. Ist X eine reelle Zufallsvariable mit dem Erwartungswert μ und der Varianz σ^2, so gilt die Chebyshev-Ungleichung

$$\forall c > 0 \quad P(|X - \mu| \geq c) \leq \frac{\sigma^2}{c^2}.$$

BEWEIS: *(1) Definition einer Hilfsgröße r*
Man betrachtet die Hamming-Norm w als endliche Zufallsvariable

$$W : \mathbb{F}_2^\ell \to \{0, 1, \ldots, \ell\},\ z \mapsto w(z),$$

wobei auf $\mathbb{F}_2^\ell$ die durch die Bitfehlerrate p_0 definierte Binomialverteilung (15) gegeben ist. Für Erwartungswert und Varianz von W gilt dann

$$E(W) = \sum_{k=0}^{\ell} kp(W = k) = \ell p_0,$$

und

$$V(W) = E((W - E(W))^2) = \ell p_0(1 - p_0).$$

Es sei nun $\epsilon > 0$ vorgegeben. Nach der Ungleichung von Chebyshev gilt

$$\forall k \in \mathbb{N} \quad P(W \geq \ell p_0 + k\sqrt{\ell p_0(1 - p_0)}) \leq \frac{1}{k^2}.$$

Wählt man k als größte ganze Zahl, die kleiner als $\sqrt{\frac{2}{\epsilon}}$ ist, so ergibt sich die im Weiteren benötigte Ungleichung

$$P\left(W \geq \ell p_0 + \sqrt{\frac{2}{\epsilon}\ell p_0(1 - p_0)}\right) \leq \frac{\epsilon}{2}. \tag{28}$$

Wegen $p_0 < \frac{1}{2}$ gibt es ein ℓ_0 mit der Eigenschaft

$$\forall \ell > \ell_0 \quad r := \left\lceil \ell p_0 + \sqrt{\frac{2}{\epsilon} \ell p_0 (1 - p_0)} \right\rceil \leq \frac{\ell}{2}, \tag{29}$$

denn: Für $s := \sqrt{\frac{2}{\epsilon} p_0 (1 - p_0)}$ gibt es ein ℓ_0 mit

$$\forall \ell > \ell_0 \quad s\sqrt{\ell} < (\frac{1}{2} - p_0)\ell,$$

da die Quadratwurzel langsamer als eine lineare Funktion gegen unendlich strebt. Umformen der Ungleichung liefert

$$p_0 \ell + s\sqrt{\ell} < \frac{\ell}{2},$$

also die Behauptung.

(2) Eine Hilfsungleichung

Für jedes r wie unter Punkt (1) definiert gilt die Kardinalitätsabschätzung

$$|B[0, r]| \leq 2^{\ell H(r/\ell)}. \tag{30}$$

Sie ergibt sich so: Nach Gleichung (12) ist

$$|B[0, r]| = \sum_{i=0}^{r} \binom{\ell}{i}.$$

Nun ist aber andererseits $r \leq \frac{\ell}{2}$ (siehe (29)), woraus folgt:

$$\begin{aligned} 1 = (\tfrac{r}{\ell} + (1 - \tfrac{r}{\ell}))^\ell &= \sum_{i=0}^{\ell} \tbinom{\ell}{i} \left(\tfrac{r}{\ell}\right)^i (1 - \tfrac{r}{\ell})^{\ell - i} \\ &= \sum_{i=0}^{\ell} \tbinom{\ell}{i} \left(\tfrac{\frac{r}{\ell}}{1 - \frac{r}{\ell}}\right)^i (1 - \tfrac{r}{\ell})^\ell \\ &\geq \sum_{i=0}^{r} \tbinom{\ell}{i} \left(\tfrac{\frac{r}{\ell}}{1 - \frac{r}{\ell}}\right)^r (1 - \tfrac{r}{\ell})^\ell \\ &= 2^{-\ell(-\frac{r}{\ell}\log_2(\frac{r}{\ell}) - (1 - \frac{r}{\ell})\log_2(1 - \frac{r}{\ell}))} \sum_{i=0}^{r} \tbinom{\ell}{i}, \end{aligned}$$

womit die behauptete Ungleichung bewiesen ist.

(3) Die Dekodierungsabbildung d_c

Für die im Folgenden beschriebene Dekodierungsabbildung ist eine Abschätzung ihrer totalen Fehlerwahrscheinlichkeit gut möglich. Es sei r wie unter (1) definiert und $\mathbb{A} = \{a_1, \ldots, a_m\}$ eine Nummerierung des betrachteten Alphabets. Dann ist jeder Kode c durch die Festlegung $c(a_i) =: x_i \in \mathbb{F}_2^\ell$ eindeutig bestimmt; sei $C := c(\mathbb{A}) = \{x_1, x_2, \ldots, x_m\}$. Als Dekodierungsabbildung definiert man:

$$d_c(y) := \begin{cases} x \text{ falls } B[y,r] \cap C = \{x\}, \\ x_1 \text{ sonst.} \end{cases} \tag{31}$$

(4) Abschätzung der Fehlerwahrscheinlichkeit $p_{\mathrm{tot}}(c, d_c)$

Wir betrachten die Hilfsabbildung

$$f : \mathbb{F}_2^\ell \times \mathbb{F}_2^\ell \to \{0,1\},\ (y,y') \mapsto \begin{cases} 0 & \text{falls } h(y,y') > r, \\ 1 & \text{falls } h(y,y') \leq r. \end{cases}$$

Die Wahrscheinlichkeit für eine fehlerhafte Übertragung eines Kodeworts $x \in C$ lässt sich jetzt wie folgt abschätzen, wobei die in Abschnitt 2.1 eingeführten Bezeichnungen benutzt werden:

$$\begin{aligned} p_{\mathrm{err}}(x) &\leq \sum_{y \in \mathbb{F}_2^\ell} p_{\mathrm{rc}}(y|x)(1 - f(y,x) + \sum_{x' \neq x} f(y,x')) \\ &= \sum_{y \in \mathbb{F}_2^\ell} p_{\mathrm{rc}}(y|x)(1 - f(y,x)) + \sum_{y \in \mathbb{F}_2^\ell} \sum_{x' \neq x} p_{\mathrm{rc}}(y|x) f(y,x'), \end{aligned}$$

da der Term $1 - f(y,x) + \sum\limits_{x' \neq x} f(y,x')$ nicht negativ und genau dann gleich 0 ist, wenn x das einzige Kodewort in $B[y,r]$ ist. Aus der Definition von f und durch Anwendung der Ungleichung (28) ergibt sich

$$\sum_{y \in \mathbb{F}_2^\ell} p_{\mathrm{rc}}(y|x)(1 - f(y,x)) = P(h(y,x) > r) = P(w(y-x) > r) \leq \frac{\epsilon}{2}.$$

Es folgt

$$\begin{aligned} p_{\mathrm{tot}}(c,d) &\leq \sum_{x \in C} p_C(x) \left(\sum_{y \in \mathbb{F}_2^\ell} p_{\mathrm{rc}}(y|x)(1 - f(y,x)) + \sum_{y \in \mathbb{F}_2^\ell} \sum_{x' \neq x} p_{\mathrm{rc}}(y|x) f(y,x') \right) \\ &= \sum_{x \in C} p_C(x) \sum_{y \in \mathbb{F}_2^\ell} p_{\mathrm{rc}}(y|x)(1 - f(y,x)) + \sum_{x \in C} p_C(x) \sum_{y \in \mathbb{F}_2^\ell} \sum_{x' \neq x} p_{\mathrm{rc}}(y|x) f(y,x') \\ &\leq \sum_{x \in C} p_C(x) \tfrac{\epsilon}{2} + \sum_{x \in C} p_C(x) \sum_{y \in \mathbb{F}_2^\ell} \sum_{x' \neq x} p_{\mathrm{rc}}(y|x) f(y,x') \\ &= \tfrac{\epsilon}{2} + \sum_{x \in C} \sum_{y \in \mathbb{F}_2^\ell} \sum_{x' \neq x} p_C(x) p_{\mathrm{rc}}(y|x) f(y,x'). \end{aligned}$$

(5) Mittelung von $p_{\mathrm{tot}}(c, d_c)$ über alle Kodes

Ist (c^*, d^*) ein Kodierer-Dekodierer-Paar der Länge ℓ mit minimaler, totaler Fehlerwahrscheinlichkeit $p_{\mathrm{tot}}(c^*, d^*)$ und ist T irgendeine Menge von Kodierer-Dekodierer-Paaren der Länge ℓ, so gilt offensichtlich

$$p_{\mathrm{tot}}(c^*, d^*) \leq \frac{1}{|T|} \sum_{(c,d)\in T} p_{\mathrm{tot}}(c, d). \tag{32}$$

Wir wenden die Formel (32) auf die Menge

$$T = \{(c, d_c) : c \text{ binärer Blockkode der Länge } \ell\}$$

an:

$$\begin{aligned} p_{\mathrm{tot}}(c^*, d^*) &\leq \tfrac{1}{|T|} \sum_{(c,d_c)\in T} p_{\mathrm{tot}}(c, d_c) \\ &\leq \tfrac{1}{|T|} \sum_{(c,d_c)\in T} \left(\tfrac{\epsilon}{2} + \sum_{x\in C} \sum_{y\in\mathbb{F}_2^\ell} \sum_{x'\neq x} p_C(x) p_{\mathrm{rc}}(y|x) f(y, x') \right) \\ &= \tfrac{\epsilon}{2} + \tfrac{1}{|T|} \sum_{(c,d_c)\in T} \sum_{x\in C} \sum_{y\in\mathbb{F}_2^\ell} \sum_{x'\neq x} p_C(x) p_{\mathrm{rc}}(y|x) f(y, x'). \end{aligned}$$

Um den zweiten Summanden auf der rechten Seite dieser Ungleichung zu berechnen, beachten wir Folgendes: Jedes Paar (c, d_c) ist bei vorgegebener Nummerierung von $\mathbb{A}$ eindeutig bestimmt durch die Festlegung der paarweise verschiedenen Kodewörter $x_i = c(a_i)$ (siehe Schritt (3)), also durch eine Matrix

$$X := (x_1\, x_2\, \cdots\, x_m) \in \mathbb{F}_2^{\ell\times m}$$

mit paarweise verschiedenen Spalten; es sei $M \subset \mathbb{F}_2^{\ell\times m}$ die Menge dieser Matrizen. Wir fassen X als Zufallsvariable auf, wobei auf M die uniforme Verteilung gegeben ist. Bei dieser Auffassung kann man den zweiten Summanden auf der rechten Seite der in Rede stehenden Ungleichung als Erwartungswert deuten:

$$\frac{1}{|T|} \sum_{(c,d_c)\in T} \sum_{i=1}^{m} \sum_{y\in\mathbb{F}_2^\ell} \sum_{x'\neq x_i} p_C(x_i) p_{\mathrm{rc}}(y|x_i) f(y, x') = E(F(X)),$$

wobei

$$F(X) := \sum_{i=1}^{m} \sum_{y\in\mathbb{F}_2^\ell} \sum_{x'\neq x_i} p_C(x_i) p_{\mathrm{rc}}(y|x_i) f(y, x').$$

Die Additivität des Erwartungswerts liefert:

$$\begin{aligned} E(F(X)) &= \sum_{i=1}^{m} \sum_{y \in \mathbb{F}_2^\ell} E\Big(\sum_{x' \neq x_i} p_C(x_i) p_{\mathrm{rc}}(y|x_i) f(y,x') \Big) \\ &= \sum_{i=1}^{m} \sum_{y \in \mathbb{F}_2^\ell} E\Big(\sum_{x' \neq x_i} p_{C \times \mathbb{F}_2^\ell}(x_i,y) f(y,x') \Big). \end{aligned}$$

Nutzung der Annahme uniformer Verteilung von X ergibt für den Erwartungswert

$$\begin{aligned} E\Big(\sum_{x' \neq x_i} p_{C \times \mathbb{F}_2^\ell}(x_i,y) f(y,x') \Big) &= \tfrac{1}{2^\ell} \sum_{x_i \in \mathbb{F}_2^\ell} \sum_{x' \neq x_i} p(x_i,y) f(y,x') \\ &\leq \tfrac{1}{2^\ell} \sum_{x_i \in \mathbb{F}_2^\ell} |B[y,r]| p_{C \times \mathbb{F}_2^\ell}(x_i,y) \\ &\leq \tfrac{|B[0,r]|}{2^\ell} \sum_{x_i \in \mathbb{F}_2^\ell} p_{C \times \mathbb{F}_2^\ell}(x_i,y) \end{aligned}$$

und damit

$$\begin{aligned} E(F(X)) &\leq \sum_{i=1}^{m} \sum_{y \in \mathbb{F}_2^\ell} \tfrac{|B[0,r]|}{2^\ell} \sum_{x_i \in \mathbb{F}_2^\ell} p_{C \times \mathbb{F}_2^\ell}(x_i,y) \\ &= \tfrac{|B[0,r]|}{2^\ell} \sum_{i=1}^{m} \sum_{y \in \mathbb{F}_2^\ell} \sum_{x_i \in \mathbb{F}_2^\ell} p_{C \times \mathbb{F}_2^\ell}(x_i,y) \\ &= m \tfrac{|B[0,r]|}{2^\ell}. \end{aligned}$$

Bringt man nun die Ungleichung (30) ins Spiel so wurde insgesamt

$$p_{\mathrm{tot}}(c^*, d^*) \leq \frac{\epsilon}{2} + \frac{m 2^{\ell H(r/\ell)}}{2^\ell} \tag{33}$$

bewiesen.

(6) Finale

Für die im Schritt (1) eingeführte Größe $s = \sqrt{\frac{2}{\epsilon} p_0 (1-p_0)}$ gilt nach Definition der Hilfsgröße (siehe (1)) $r = [\ell p_0 + s\sqrt{\ell}]$ die Relation $\frac{r}{\ell} \in [p_0, \frac{1}{2}]$ für alle $\ell > \ell_0$. Für die Funktion $\log_2$ gilt in diesem Intervall:

$$\log_2(\frac{r}{\ell}) = \log_2(p_0 + \frac{m}{\sqrt{\ell}} + f(\ell))$$

mit einer Funktion f für die $|f(\ell)| \leq \frac{1}{2\ell}$ gilt. Sei L eine Lipschitzschranke für $\log_2$ in $[p_0, \frac{1}{2}]$, dann gilt

$$\log_2(\frac{r}{\ell}) = \log_2(p_0) + g(\ell),$$

wobei

$$g(\ell) \leq L(\frac{m}{\sqrt{\ell}} + f(\ell)) \leq L(\frac{m}{\sqrt{\ell}} + \frac{1}{2\ell}).$$

Entsprechend ist auch

$$\log_2(1 - \frac{r}{\ell}) = \log_2(1 - p_0) + h(\ell),$$

wobei

$$|h(\ell)| \leq L(\frac{m}{\sqrt{\ell}} + \frac{1}{2\ell}).$$

Es folgt

$$\begin{array}{rcl} H(\frac{r}{\ell}) & = & -\frac{r}{\ell}\log_2(\frac{r}{\ell}) - (1-\frac{r}{\ell})\log_2(1-\frac{r}{\ell}) \\ & = & -(p_0 + \frac{m}{\sqrt{\ell}} + f(\ell))(\log_2(p_0) + g(\ell)) - (1 - p_0 - \frac{m}{\sqrt{\ell}} - f(\ell))(\log_2(1-p_0) + h(\ell)) \\ & = & H(p_0) - (\frac{m}{\sqrt{\ell}} + f(\ell))\log_2(p_0) - (p_0 + \frac{m}{\sqrt{\ell}} + f(\ell))g(\ell) \\ & + & (\frac{m}{\sqrt{\ell}} + f(\ell))\log_2(1-p_0) - (1 - p_0 - \frac{m}{\sqrt{\ell}} - f(\ell))h(\ell) \\ & = & H(p_0) + G(\ell), \end{array}$$

wobei die Funktion G die Eigenschaft

$$G(\ell) \leq M(\frac{m}{\sqrt{\ell}} + \frac{1}{2\ell})$$

mit einem $M > 0$ besitzt. Insgesamt ergibt sich nun:

$$\begin{array}{rcl} \frac{m2^{\ell H(r/\ell)}}{2^\ell} & = & 2^{\ell(H(r/\ell) - 1 + \frac{\log_2(m)}{\ell})} \\ & = & 2^{\ell(H(p_0) + G(\ell) - 1 + R(c))} \\ & = & 2^{\ell(R(c) - C + G(\ell))} \\ & \leq & 2^{\ell(R - C + G(\ell))}. \end{array}$$

Da nach Voraussetzung $R - C < 0$ ist und $\lim\limits_{\ell \to \infty} G(\ell) = 0$ gilt, gibt es $\ell_1 > \ell_0$ (siehe (1) zur Definition von ℓ_0) mit der Eigenschaft

$$\forall \ell > \ell_1 \quad \frac{m2^{\ell H(r/\ell)}}{2^\ell} < \frac{\epsilon}{2}.$$

Die Ungleichung (33) liefert dann wie angestrebt

$$p_{\,\mathrm{tot}}(c^*, d^*) < \epsilon.$$

□

3 Lineare Kodes

In den bisherigen Ausführungen zur Theorie binärer, fehlerkorrigierender Kodes wurde hauptsächlich die metrische Struktur des Hamming-Raums $\mathbb{F}_2^\ell$ genutzt. Wie in Abschnitt 1.4 erläutert ist dieser auch ein $\mathbb{F}_2$-Vektorraum, eine Tatsache, die man für die Konstruktion von Kodes und von Dekodierabbildungen gewinnbringend einsetzen kann.

3.1 Grundlagen

Anstatt in dem Vektorraum $\mathbb{F}_2^\ell$ nach beliebigen Teilmengen C mit aus Sicht der Kodierungstheorie guten Eigenschaften zu suchen, betrachten wir nun nur solche Teilmengen C, die auch Untervektorräume sind. Die Hoffnung dabei ist, dass die Konstruktion und Analyse solcher Teilmengen in Bezug auf die Kodierungstheorie systematischer als im allgemeinen Fall möglich ist.

DEFINITION 3.1: *Ein binärer Blockkode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ heißt linear, falls $c(\mathbb{A}) = C$ ein Untervektorraum von $\mathbb{F}_2^\ell$ ist. Besitzt c in diesem Fall die Minimaldistanz m und C die Dimension k, so spricht man kurz von einem $[\ell, k, m]$-Kode.*

Die Minimaldistanz und die Informationsrate eines linearen Kodes lassen sich einfach berechnen:

FESTSTELLUNG 3.2: *Es sei $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein linearer Kode der Dimension k. Dann gelten*

$$h_{\min}(c) = \min(w(x) : x \in C \setminus 0)$$

und

$$R(c) = \frac{k}{\ell}.$$

BEWEIS: Wegen der Translationsinvarianz $h(x, x') = h(x + y, x' + y)$ der Hamming-Metrik gilt

$$\begin{aligned} \min(h(x, x') : x, x' \in C,\ x \neq x') &= \min(h(x - x', 0) : x, x' \in C,\ x \neq x') \\ &= \min(w(x) : x \in C \setminus 0). \end{aligned}$$

Für die Informationsrate ergibt sich $R(c) = \frac{\log_2 |\mathbb{A}|}{\ell} = \frac{\log_2 |C|}{\ell} = \frac{\log_2(2^k)}{\ell} = \frac{k}{\ell}$. □

Während man bei einem beliebigen binären Blockkode c alle Kodewörter $x \in C$ explizit angeben muss, um mit dem Kode zu arbeiten, genügt es im Fall eines linearen Blockkodes eine Basis $b_1, \ldots, b_k$ des Untervektorraums C anzugeben:

FESTSTELLUNG 3.3: *Für einen linearen Kode c der Länge ℓ besitzt der Vektorraum C der Kodewörter eine Basis $b_1, \ldots, b_k$ mit $k \leq \ell$ Elementen. Jedes Kodewort ist eindeutig in der Form*

$$x = \lambda_1 b_1 + \ldots + \lambda_k b_k,\ \lambda_i \in \mathbb{F}_2$$

darstellbar. Insbesondere gilt $|C| = 2^k$.

BEWEIS: Der Vektorraum $\mathbb{F}_2^\ell$ besitzt die Dimension ℓ, womit nach dem Basisergänzungssatz jeder Untervektorraum höchstens die Dimension ℓ besitzt. Die Kardinalitätsaussage folgt aus der Tatsache, dass man die Koeffizienten λ_i unabhängig voneinander wählen kann und jeweils nur zwei Möglichkeiten dafür hat. □

Jede Wahl einer geordneten Basis $B := (b_1, \ldots, b_k)$ des Kodes C, das heißt für die Basiselemente ist zum Beispiel durch Nummerierung eine Reihenfolge festgelegt, liefert eine lineare Abbildung:

$$T_B :\ \mathbb{F}_2^k \to \mathbb{F}_2^\ell,\ (\lambda_1, \ldots, \lambda_k)^t \mapsto \sum_{i=1}^{k} \lambda_i b_i. \tag{34}$$

Die Abbildung T_B ist injektiv und ihr Bild ist gerade der Kode C. Wählt man jeweils eine Basis von $\mathbb{F}_2^k$ und $\mathbb{F}_2^\ell$, so kann man T_B durch eine Matrix $A \in \mathbb{F}_2^{\ell \times k}$ beschreiben. Am einfachsten wird diese Beschreibung, wenn man in beiden Vektorräumen die Standardeinheitsbasis wählt.

DEFINITION 3.4: *Ist $(b_1, \ldots, b_k)$ eine geordnete Basis des Kodes C, so bezeichnet man die Matrix*

$$G := (b_1\, b_2\, \ldots\, b_k) \in \mathbb{F}_2^{\ell \times k}$$

als Erzeugermatrix von C (engl.: generator matrix). Sie ist die zu der linearen Abbildung (34) bezüglich der Standardeinheitsbasen gehörende Matrix.

Im allgemeinen besitzt ein Kode nicht nur eine Erzeugermatrix. Für jede solche gilt die Gleichung

$$C = \{G \cdot t : t \in \mathbb{F}_2^k\},$$

was die Namensgebung erklärt.

Die lineare Abbildung T_B kann als Parameterdarstellung des Kodes C interpretiert werden. Neben dieser ist eine zweite Darstellung eines Kodes nützlich, nämlich als Lösungsmenge eines homogenen linearen Gleichungssystems bzw. als Kern einer linearen Abbildung.

FESTSTELLUNG 3.5: *Zu einem Kode $C \subseteq \mathbb{F}_2^\ell$ der Dimension k existiert eine Matrix $H \in \mathbb{F}_2^{(\ell-k)\times\ell}$ mit der Eigenschaft*

$$x \in C \Leftrightarrow Hx = 0.$$

Jede solche Matrix besitzt den Rang $\ell - k$.

BEWEIS: Man beweist zunächst die Rangaussage. Hierzu sei $H \in \mathbb{F}_2^{(\ell-k)\times\ell}$ eine Matrix mit der in der Feststellung angegebenen Eigenschaft. Dann besitzt die lineare Abbildung

$$f_H : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell-k},\ y \mapsto Hy \tag{35}$$

den Kern C. Nach der Dimensionsformel gilt also

$$\ell = \dim(\mathbb{F}_2^\ell) = \dim(C) + \dim(f_H(\mathbb{F}_2^\ell)) = k + \dim(f_H(\mathbb{F}_2^\ell)),$$

woraus

$$\dim(f_H(\mathbb{F}_2^\ell)) = \ell - k$$

folgt. Das das Bild von f_H durch die Spalten der Matrix H aufgespannt wird, folgt die Behauptung.

Nun zur Existenz von H: Es sei $b_1, \ldots, b_k$ eine Basis von C. Man ergänzt diese um Vektoren $b_{k+1}, \ldots, b_\ell$ zu einer Basis von $\mathbb{F}_2^\ell$ und definiert eine lineare Abbildung

$$f : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell-k}$$

durch

$$f(b_i) = 0,\ i \in \{1, \ldots, k\},\ f(b_{k+i}) = e_i,\ i \in \{1, \ldots, \ell - k\}.$$

Dann besitzt f den Kern C. Sei $H \in \mathbb{F}_2^{(\ell-k)\times\ell}$ die Koordinatenmatrix von T bezüglich der Standardeinheitsbasen. Dann gilt $C = \{y \in \mathbb{F}_2^\ell : Hy = 0\}$. □

Definition 3.6: *Ist $C \subseteq \mathbb{F}_2^\ell$ ein Kode, so nennt man eine Matrix $H \in \mathbb{F}_2^{(\ell-k)\times\ell}$ mit der Eigenschaft $C = \{y \in \mathbb{F}_2^\ell : Hy = 0\}$ Kontrollmatrix (engl.: parity check matrix) zu C.*

Die Gleichungen des linearen Gleichungssystems $HX = 0$, $X \in \mathbb{F}_2^\ell$ nennt man Kontrollgleichungen von C.

Beispiel 3.7 (Forts. Beispiel 2.33): Der Wiederholungskode

$$C = \{(0, 0, \ldots, 0)^t, (1, 1, \ldots, 1)^t\} \subset \mathbb{F}_2^\ell$$

ist ein linearer Kode der Dimension $k = 1$. Seine einzige Erzeugermatrix ist daher

$$G = (1, 1, \ldots, 1)^t.$$

Eine Kontrollmatrix kann man anhand des Beweises von Feststellung 3.5 bestimmen: Man betrachtet die lineare Abbildung

$$f : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell-1}$$

mit $f((1, 1, \ldots, 1)^t) = 0$ und $f(e_2) = e_1, \ldots, f(e_\ell) = e_{\ell-1}$. Man beachte, dass $\{(1, 1, \ldots, 1)^t, e_2, \ldots, e_\ell\}$ eine Basis von $\mathbb{F}_2^\ell$ bildet. Die Koordinatenmatrix von H bezüglich der Standardeinheitsbasen ist dann:

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

Nur die erste Spalte von H ist erklärungsbedürftig: In $\mathbb{F}_2^\ell$ gilt

$$(1, 1, \ldots, 1)^t = \sum_{i=1}^{\ell} e_i$$

und daher

$$0 = f((1, 1, \ldots, 1)^t) = \sum_{i=1}^{\ell} f(e_i) = f(e_1) + \sum_{i=2}^{\ell} f(e_i) = f(e_1) + (1, 1, \ldots, 1)^t.$$

Die Kontrollgleichungen lauten also

$$\begin{aligned} X_1 + X_2 &= 0 \\ X_1 + X_3 &= 0 \\ \vdots \quad &\vdots \quad \vdots \\ X_1 + X_\ell &= 0. \end{aligned}$$

Sie prüfen, ob $X_1 = X_2 = \ldots = X_\ell$ gilt, eine die Kodewörter charakterisierende Eigenschaft. $\diamond$

Beispiel 3.8 (Forts. Beispiel 2.29): Im Beispiel 2.29 wurde der Kode

$$C = \{(0,0,0,0)^t, (1,1,1,0,0)^t, (0,0,1,1,1)^t, (1,1,0,1,1)^t\} \subset \mathbb{F}_2^5$$

konstruiert. Nachrechnen liefert die Abgeschlossenheit von C bezüglich der Addition in $\mathbb{F}_2^5$, womit C ein Untervektorraum ist. Als Basis kann man die Elemente

$$b_1 = (1,1,1,0,0)^t,\ b_2 = (0,0,1,1,1)^t$$

benutzen, der Kode besitzt also die Dimension $k = 2$ und die Erzeugermatrix

$$G = (b_1\, b_2) \in \mathbb{F}_2^{5\times 2}.$$

Eine Kontrollmatrix bestimmen wir dieses Mal durch Lösen des Gleichungssystems

$$\begin{aligned} Hb_1 &= 0 \\ Hb_2 &= 0 \end{aligned}$$

unter Berücksichtigung der Rangbedingung für H. Ist $H = (h_{ij})$, so ergibt sich:

$$\begin{aligned} h_{11} + h_{12} + h_{13} &= 0 \\ h_{21} + h_{22} + h_{23} &= 0 \\ h_{31} + h_{32} + h_{33} &= 0 \\ h_{13} + h_{14} + h_{15} &= 0 \\ h_{23} + h_{24} + h_{25} &= 0 \\ h_{33} + h_{34} + h_{35} &= 0 \end{aligned}$$

Die Lösungsmenge dieses Gleichungssystems ist also die Menge der Matrizen H der Form

$$\begin{pmatrix} h_{12}+h_{13} & h_{12} & h_{13} & h_{14} & h_{13}+h_{14} \\ h_{22}+h_{23} & h_{22} & h_{23} & h_{24} & h_{23}+h_{24} \\ h_{32}+h_{33} & h_{32} & h_{33} & h_{34} & h_{33}+h_{34} \end{pmatrix}.$$

Die 9 frei wählbaren Koeffizienten müssen im Fall einer Kontrollmatrix so festgelegt werden, dass die entstehende Matrix den Rang 3 besitzt. Hierzu darf keine Zeile nur Null-Bits enthalten. Man wählt also für die erste Zeile zum Beispiel

$$h_{12} = 1, h_{13} = 0, h_{14} = 0.$$

Setzt man in der zweiten Zeile

$$h_{22} = 0, h_{23} = 0, h_{24} = 1,$$

so ist diese von der ersten Zeile verschieden, die beiden sind also linear unabhängig.

Für die dritte Zeile legt man

$$h_{32} = 0, h_{33} = 1, h_{34} = 0$$

fest. Die entstehende Matrix

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

hat dann tatsächlich den Rang 3, ist also eine Kontrollmatrix für C. $\diamond$

Die Vorgehensweise im letzten Beispiel beim Ermitteln einer Kontrollmatrix lässt sich in eine allgemeine Form gießen: Nach Definition sind die Kontrollmatrizen H eines gegebenen linearen Kodes c bzw. C Lösungen der Matrixgleichung

$$X \cdot G = 0, \tag{36}$$

wobei G eine Erzeugermatrix von C und $X \in \mathbb{F}_2^{(\ell-k)\times\ell}$ ist.

FESTSTELLUNG 3.9: *Die Lösungen vom Rang $\ell - k$ der Matrixgleichung (36) sind genau die Kontrollmatrizen des betrachteten Kodes C.*

BEWEIS: Die Implikation $\Leftarrow$ wurde mit Feststellung 3.5 bereits bewiesen, da die Spalten von G Kodewörter sind.

Sei also H eine Lösung von (36) vom Rang $\ell - k$. Dann gilt für ein beliebiges Kodewort $x \in C$:

$$Hx = H(\sum_{i=}^{k} \lambda_i b_i)) = \sum_{i=}^{k} \lambda_i H b_i = 0,$$

also $C \subseteq \mathrm{Kern}(f_H)$ mit $f_H(x) := Hx$. Eine Anwendung der Dimensionsformel liefert andererseits

$$\ell = \dim(\mathrm{Kern}(f_H)) + \dim(f_H(\mathbb{F}_2^\ell)) = \dim(\mathrm{Kern}(f_H)) + \ell - k,$$

da das Bild von f_H von den Spalten von H aufgespannt wird. Es folgt $\dim(\mathrm{Kern}(f_H)) = k$ und damit $\dim \mathrm{Kern}(f_H) = C$. □

Mit Hilfe von Feststellung 3.9 kann man für eine spezielle Klasse von Kodes die Kontrollmatrix ohne Rechnung bestimmen:

DEFINITION 3.10: *Ein linearer Kode c der Dimension k heißt systematisch, falls er eine Erzeugermatrix der Gestalt*

$$G = \begin{pmatrix} E_k \\ P \end{pmatrix} \tag{37}$$

besitzt. In diesem Fall bezeichnet man die Bits $x_1, \ldots, x_k$ jedes Kodeworts $(x_1, \ldots, x_\ell) \in C$ als Informationssymbole und die Bits $x_{k+1}, \ldots, x_\ell$ als Kontrollsysmbole.

BEMERKUNG: Die Namensgebung rührt daher, dass das Wort $(x_1, \ldots, x_k) \in \mathbb{F}_2^k$ das übertragene Symbol eindeutig festlegt, sofern keine Störung aufgetreten ist. Die Bits $x_{k+1}, \ldots, x_\ell$ dienen der Fehlerkorrektur. In einem nicht systematischen Kode ist diese Trennung der Rollen der Bits nicht möglich, die beiden Funktionen sind miteinander verwoben.

Ist c bzw. C ein systematischer Kode, so ist eine Kontrollmatrix durch

$$H = (-P\, E_{\ell-k}) = (P\, E_{\ell-k}) \tag{38}$$

gegeben: Wie man direkt nachrechnet löst H die Matrixgleichung (36) und besitzt offensichtlich den Rang $\ell - k$. Feststellung 3.9 zeigt dann, dass H tatsächlich eine Kontrollmatrix für C ist.

Die zu H gehörenden Kontrollgleichungen für den Kode C lauten

$$\begin{aligned} X_{k+1} &= p_{11}X_1 + p_{12}X_2 + \ldots + p_{1k}X_k \\ X_{k+2} &= p_{21}X_1 + p_{22}X_2 + \ldots + p_{2k}X_k \\ &\vdots \\ X_\ell &= p_{\ell-k\,1}X_1 + p_{\ell-k\,2}X_2 + \ldots + p_{\ell-k\,k}X_k, \end{aligned} \tag{39}$$

wobei $P = (p_{ij})$.

BEISPIEL 3.11: (Golay-Kode) Ein von Marcel Golay im Jahr 1949 publizierter systematischer Kode $C \subset \mathbb{F}_2^{23}$ besitzt die Generatormatrix

$$G := \begin{pmatrix} E_{12} \\ P \end{pmatrix},$$

wobei

$$P := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \in \mathbb{F}_2^{11\times 12};$$

es ist also $\dim(C) = 12$.

Das Kodewort x in der letzten Spalte der Generatormatrix besitzt das Gewicht $w(x) = 7$ und keine Spalte der Generatormatrix besitzt ein kleineres Gewicht, weshalb nach Feststellung 3.2 für die Minimaldistanz $h_{\min}(C) \leq 7$ gilt. Tatsächlich gilt $h_{\min}(C) = 7$, was aber nicht einfach zu erkennen ist.

Für die Zahlen $\ell = 23$, $e = 3$, $|C| = 2^{12}$ gilt die Gleichung (27), weshalb C ein 3-perfekter Kode ist – Fall 4 in Satz 2.34. ◇

3.2 Kodes und lineare Abbildungen

Eine Möglichkeit zur systematischen Konstruktion fehlerkorrigierender Kodes besteht darin einen bereits bekannten Kode zu modifizieren. Im Fall eines linearen Kodes kann man hierzu lineare Abbildungen nutzen. Da man jedoch auch eine Aussage über die Minimaldistanz des modifizierten Kodes machen möchte, ist das metrische Verhalten einer linearen Abbildung mit ins Auge zu fassen. Den in der vorliegenden Situation relevanten Aspekt dieses Verhaltens kann man wie folgt quantifizieren:

DEFINITION 3.12: *Ist $f : X \to Y$ eine Abbildung zwischen zwei metrischen Räumen (X, d_X) und (Y, d_Y), so definiert man die Kontraktion von f als*

$$C(f) := \sup\left(\frac{d_X(x_1, x_2)}{d_Y(f(x_1), f(x_2))} : x_1, x_2 \in X, f(x_1) \neq f(x_2)\right).$$

BEMERKUNGEN:

1. Nach Definition gilt stets die Ungleichung

$$d_X(x_1, x_2) \leq C(f) d_Y(f(x_1), f(x_2)).$$

2. Im Fall $X = \mathbb{F}_2^\ell$ und $Y = \mathbb{F}_2^{\ell'}$ versehen mit den jeweiligen Hamming-Metriken ergibt sich

$$C(f) := \max\left(\frac{h(x_1, x_2)}{h(f(x_1), f(x_2))} : x_1, x_2 \in \mathbb{F}_2^\ell, f(x_1) \neq f(x_2)\right).$$

3. Ist f zusätzlich linear, so erhält man

$$C(f) := \max\left(\frac{w(x)}{w(f(x))} : x \in \mathbb{F}_2^\ell, f(x) \neq 0\right).$$

FESTSTELLUNG 3.13: *Ist $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein linearer Kode der Dimension k und $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell'}$ eine injektive, lineare Abbildung, so ist $T \circ c$ ein linearer Kode der Dimension k. Für seine Minimaldistanz gilt*

$$h_{\min}(T \circ c) \geq \frac{1}{C(T)} h_{\min}(c).$$

Ist T eine Isometrie, so gilt $h_{\min}(T \circ c) = h_{\min}(c)$.

BEWEIS: Das Bild $T(C)$ des Untervektorraums $C = c(\mathbb{A})$ ist wegen der Linearität von T ein Untervektorraum von $\mathbb{F}_2^{\ell'}$ und besitzt wegen der Injektivität von T dieselbe Dimension wie C.

Für jedes $x \in C$ gilt nach Bemerkung 3 zur Definition der Kontraktion die Ungleichung $w(x) \leq C(T) w(T(x))$, woraus die Behauptung direkt folgt, da $T(C)$ die Menge der Kodewörter von $T \circ c$ ist.

Die Behauptung im Fall einer Isometrie T ist offensichtlich. □

Beispiel 3.14: Ist $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein beliebiger linearer Kode, so kann mit Hilfe der linearen Abbildung

$$T : \mathbb{F}_2^\ell \to \mathbb{F}_2^{2\ell},\ y \mapsto \begin{pmatrix} y \\ y \end{pmatrix}$$

die Blocklänge verdoppelt werden. Es gilt $w(T(y)) = 2w(y)$ und daher $C(T) = \frac{1}{2}$. Für die Minimaldistanz von $T \circ c$ folgt $h_{\min}(T \circ c) = 2h_{\min}(c)$. $\diamond$

Beispiel 3.15: Wir betrachten wieder einen beliebigen linearen Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$, sowie eine lineare Abbildung

$$f : \mathbb{F}_2^\ell \to \mathbb{F}_2;$$

jede solche Abbildung besitzt die Gestalt

$$f(y_1, \ldots, y_\ell) = \sum_{i=1}^{\ell} a_i y_i$$

mit gewissen $a_1, \ldots, a_\ell \in \mathbb{F}_2$. Mit Hilfe von f definiert man die Abbildung

$$T : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell+1},\ (y_1, \ldots, y_\ell)^t \mapsto (y_1, \ldots, y_\ell, f(y_1, \ldots, y_\ell));$$

sie ist offensichtlich linear und injektiv. Weiter gilt

$$w(T(y_1, \ldots, y_\ell)) \geq w(y_1, \ldots, y_\ell),$$

also $C(T) \leq 1$ und daher

$$h_{\min}(T \circ c) \geq h_{\min}(c). \tag{40}$$

Ein Spezialfall ist das »adding an overall parity check«: Hier wählt man

$$f(y_1, \ldots, y_\ell) = \sum_{i=1}^{\ell} y_i,$$

das heißt an ein Kodewort mit geradem Gewicht wird ein Null-Bit angehängt, an ein solches mit ungeradem Gewicht ein Eins-Bit. Die Kodewörter $x' \in T(C)$ des Kodes $T \circ c$ besitzen daher alle gerades Gewicht. Da dann auch die Minimaldistanz $h_{\min}(T \circ c)$ gerade sein muss, erhält man aus der Ungleichung

(40): *Ist c ein Kode mit ungerader Minimaldistanz, so liefert das »adding an overall parity check« einen Kode mit der Minimaldistanz*

$$h_{\min}(T \circ c) = h_{\min}(c) + 1.$$

Der Kode

$$C = \{(0,0,0,0,0)^t, (1,1,1,0,0)^t, (0,0,1,1,1)^t, (1,1,0,1,1)^t\}$$

aus Beispiel 2.29 besitzt die Minimaldistanz 3. »Adding an overall parity check« liefert hier den Kode

$$C' = \{(0,0,0,0,0,0)^t, (1,1,1,0,0,1)^t, (0,0,1,1,1,1)^t, (1,1,0,1,1,0)^t\} \subset \mathbb{F}_2^6$$

der Minimaldistanz 4. $\diamond$

Feststellung 3.13 zeigt, dass sich mittels linearer Abbildungen $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell'}$, die die Hamming-Distanz invariant lassen, aus einem gegebenen Kode c neue mit derselben Minimaldistanz gewinnen lassen. Ist $\ell = \ell'$, so besitzt $T \circ c$ auch dieselbe Informationsrate wie c. Die genauere Betrachtung dieses Sachverhalts liefert ein besseres Verständnis linearer Kodes, ist aber für die praktische Anwendung weniger wichtig.

Satz 3.16: *Eine lineare Abbildung $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^{\ell'}$ ist genau dann eine Isometrie, wenn T injektiv und das Bild $T(e_i)$ jedes Standardeinheitsvektors $e_i \in \mathbb{F}_2^\ell$ ein Standardeinheitsvektor von $\mathbb{F}_2^{\ell'}$ ist.*

Insbesondere gibt es zu jeder linearen Isometrie $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ eine Permutation $\sigma \in S_\ell$ mit der Eigenschaft

$$\forall (y_1, \ldots, y_\ell)^t \in \mathbb{F}_2^\ell \quad T((y_1, y_2, \ldots, y_\ell)^t) = (y_{\sigma(1)}, y_{\sigma(2)}, \ldots, y_{\sigma(\ell)})^t.$$

Beweis: Es sei T eine lineare Isometrie. Dann gilt für jeden Standardeinheitsvektor $e_i \in \mathbb{F}_2^\ell$:

$$1 = w(e_i) = h(0, e_i) = h(T(0), T(e_i)) = h(0, T(e_i)) = w(T(e_i)),$$

womit $T(e_i)$ ein Standardeinheitsvektor sein muss. Jede Isometrie ist injektiv.

Sei andererseits T eine injektive Abbildung, die Standardeinheitsvektoren auf Standardeinheitsvektoren abbildet. Dann sind $T(e_1), T(e_2), \ldots, T(e_\ell)$

paarweise verschiedene Standardeinheitsvektoren. Besitzt $y \in \mathbb{F}_2^\ell$ das Gewicht $w(y) = w$, so besitzt y die Form

$$y = e_{i_1} + e_{i_2} + \ldots + e_{i_w},$$

woraus

$$T(y) = T(e_{i_1}) + T(e_{i_2}) + \ldots + T(e_{i_w})$$

folgt. Da die Bilder $T(e_{i_j})$ Standardeinheitsvektoren sind, folgt $w(T(y)) = w$, das heißt T ist gewichterhaltend. Da die Hamming-Metrik translationsinvariant ist, folgt hieraus, dass T isometrisch ist. Der Rest der Behauptungen ist nun klar. □

Ist $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ eine lineare Isometrie und $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein linearer Kode, so stimmt der lineare Kode $T \circ c$ in allen Eigenschaften mit c überein, die sich mittels der Hamming-Metrik oder linearer Algebra oder einer Kombination von beiden ausdrücken lassen. Dies motiviert die

DEFINITION 3.17: *Zwei lineare Kodes $c : \mathbb{A} \to \mathbb{F}_2^\ell$ und $c' : \mathbb{A} \to \mathbb{F}_2^\ell$ heißen äquivalent, falls $c' = T \circ c$ mit einer Isometrie $T : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell$ gilt.*

Mit Hilfe dieses Äquivalenzbegriffs lassen sich lineare Kodes klassifizieren:

SATZ 3.18: *Jeder lineare Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ist zu einem systematischen Kode aquivalent.*

BEWEIS: Es sei G eine Erzeugermatrix des Kodes c. Mit Hilfe des Gauß-Verfahrens lässt sich die Matrix G^t in eine Matrix der Gestalt $(E_k\, Q)$ überführen. Das Gauß-Verfahren arbeitet dabei bekanntlich mit elementaren Zeilenoperationen – im vorliegenden Fall des Körpers $\mathbb{F}_2$ sind dies nur Vertauschungen zweier Zeilen und das Addieren einer Zeile zu einer anderen, sowie Spaltenvertauschungen. Alle diese Operationen kann man durch Multiplikation von G^t mit bestimmten Matrizen von links (für die Zeilenoperationen) und von rechts (für die Spaltenoperationen) bewirken. Da die Operationen umkehrbar sind, sind diese Matrizen invertierbar. Zusammenfassend existieren also invertierbare Matrizen $Z \in \mathbb{F}_2^{k \times k}$, $S \in \mathbb{F}_2^{\ell \times \ell}$ derart, dass die Gleichung

$$ZG^tS = (E_k\, Q)$$

gilt. Es folgt

$$S^tGZ^t = \begin{pmatrix} E_k \\ Q^t \end{pmatrix}.$$

Die lineare Abbildung

$$T : \mathbb{F}_2^\ell \to \mathbb{F}_2^\ell,\ y \mapsto S^t y$$

ist invertierbar und bildet Standardeinheitsvektoren auf solche ab, da die Matrix S die im Gauß-Verfahren notwendigen Spaltenvertauschungen bewirkt. Nach Satz 3.16 ist T also eine lineare Isometrie und damit $c' := T \circ c$ ein zu c äquivalenter Kode.

Der Kode c' besitzt die Erzeugermatrix $S^t G Z^t$, ist also systematisch: Die Spalten der Matrix GZ^t sind Linearkombinationen der Spalten von G und da Z^t invertierbar ist, besitzt GZ^t denselben Rang wie G. Es folgt: Die Spalten $a_1, \ldots, a_k$ von GZ^t bilden eine Basis von C. Die Spalten der Matrix $S^t G Z^t$ sind dann gerade die Vektoren

$$S^t a_k = T(a_k).$$

Da T invertierbar ist und nach Definition des Kodes c' bilden diese eine Basis von $C' = T(C)$, womit in der Tat $S^t G Z^t$ eine Erzeugermatrix von c' ist. □

Beispiel 3.19 (Forts. Beispiel 3.8): Wie in Beispiel 3.8 gezeigt ist

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

die Transponierte einer Erzeugermatrix des dort betrachteten Kodes c. Eine Vertauschung der zweiten und dritten Spalte liefert die Matrix

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Addieren der zweiten zur ersten Zeile ergibt

$$\begin{pmatrix} 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{pmatrix},$$

womit die gewünschte Form erreicht ist. Der zu C äquivalente, systematische Kode ist also

$$C' = \{(0,0,0,0,0)^t, (1,0,1,1,1)^t, (0,1,0,1,1)^t, (1,1,1,0,0)^t\}.$$

◇

Beispiel 3.20: Dieses Beispiel zeigt, dass man Kodes auch aus Kernen linearer Abbildungen gewinnen kann. Wir betrachten die lineare Abbildung

$$\begin{array}{rcl} f : \mathbb{F}_2^6 & \to & \mathbb{F}_2^3 \\ (y_1, y_2, y_3, y_4, y_5, y_6)^t & \mapsto & (y_1 + y_2 + y_3, y_3 + y_4 + y_5, y_5 + y_6 + y_1)^t. \end{array}$$

Es gilt $f(e_1) = (1, 0, 1)^t$, $f(e_2) = (1, 0, 0)^t$ und $f(e_3) = (1, 1, 0)^t$. Da diese drei Vektoren eine Erzeugendensystem von $\mathbb{F}_2^3$ bilden, ist f surjektiv und der Kern $C := \mathrm{Ker}\,(f)$ besitzt nach der Dimensionsformel für lineare Abbildungen die Dimension 3. Durch Probieren findet man eine Basis von C und damit eine Generatormatrix:

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

Die restlichen 4 Elemente des Kodes lassen sich nun zu

$$(1, 0, 1, 0, 1, 0)^t, (0, 1, 1, 1, 0, 0)^t, (1, 1, 0, 1, 1, 0)^t, (0, 0, 0, 1, 1, 1)^t$$

berechnen. Für die Minimaldistanz des Kodes gilt also $h_{\min}(C) = 3$, das heißt der Kode ist 1-fehlerkorrigierend.

Kontrollgleichungen für C lassen sich mit Hilfe der Tatsache ermitteln, dass C der Kern von f ist. Ein Element $(y_1, y_2, y_3, y_4, y_5, y_6)^t$ ist genau dann ein Kodewort, wenn die Gleichungen

$$\begin{array}{rcl} y_1 + y_2 + y_3 & = & 0 \\ y_3 + y_4 + y_5 & = & 0 \\ y_5 + y_6 + y_1 & = & 0 \end{array}$$

gelten, eine Kontrollmatrix ist folglich

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

Wir bestimmen auch einen zu C äquivalenten Kode durch Anwenden des Gauß-Verfahrens auf die Matrix

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

Addition der ersten zur dritten Zeile liefert

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

und nachfolgende Addition der zweiten zur dritten Zeile

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Addition der zweiten zur ersten Zeile ergibt

$$\begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Schließlich vertauscht man die dritte und vierte Spalte und erhält

$$(G')^t := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}. \tag{41}$$

Der zu C äquivalente Kode ist damit

$$\begin{aligned} C' := \{ \quad & (0,0,0,0,0,0)^t, (1,0,0,1,1,0)^t, (0,1,0,1,1,1)^t, (0,0,1,0,1,1)^t \\ & (1,1,0,0,0,1)^t, (1,0,1,1,0,1)^t, (0,1,1,1,0,0)^t, (1,1,1,0,1,0)^t\} \end{aligned}$$

Man beachte die gleiche Anzahl von Kodewörten mit gegebenem Gewicht: Beide Kodes besitzen vier Kodewörter vom Gewicht 3 und drei Kodewörter vom Gewicht 4. Dies ist eine direkte Folge der Tatsache, dass die Kodewörter von C durch eine Isometrie bijektiv auf die Kodewörter von C' abgebildet werden.

Um die Minimaldistanz auf 4 zu erhöhen kann man ein »adding an overall parity check« mit C oder C' durchführen. Im Fall von C' ergibt sich der Kode

$$\begin{aligned} C'' := \{ \quad & (0,0,0,0,0,0,0)^t, (1,0,0,1,1,0,1)^t, (0,1,0,1,1,1,0)^t, (0,0,1,0,1,1,1)^t \\ & (1,1,0,0,0,1,1)^t, (1,0,1,1,0,1,0)^t, (0,1,1,1,0,0,1)^t, (1,1,1,0,1,0,0)^t\} \end{aligned}$$

Eine Kontrollmatrix für C'' lässt sich durch folgende Überlegung bestimmen: Da die ersten 6 Komponenten eines Kodeworts $x'' \in C'' \subset \mathbb{F}_2^7$ dieselben wie

im ursprüngleichen Kodewort $x' \in C'$ sind, sind die Kontrollgleichungen für C'' dieselben wie für C' erweitert um die Gleichung

$$X_7 = X_1 + X_2 + X_3 + X_4 + X_5 + X_6,$$

womit sich als Kontrollmatrix für C'' die Matrix

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

ergibt. Alternativ kann man auch so vorgehen: Die Matrix G' aus Gleichung (41) ist die Erzeugermatrix des Kodes C'. Aus ihr lässt sich eine Erzeugermatrix von C'' durch Anfügen der »overall parity bits« als letzte Zeile gewinnen:

$$(G'')^t := \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

Folglich ist auch C'' ein systematischer Kode und eine Kontrollmatrix ist

$$H''_2 := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{pmatrix},$$

wobei man die Formel (38) verwendet. ◇

3.3 Syndrom-Dekodierung

Im Fall eines linearen Kodes $c : \mathbb{A} \to \mathbb{F}_2^\ell$ kann man die Maximum-Likelihood-Dekodierung deutlich effizienter als im allgemeinen Fall durchführen. Ein entsprechender Algorithmus wird in diesem Abschnitt formuliert. Dabei spielt der Begriff der Nebenklasse in einem Vektorraum eine zentrale Rolle.

DEFINITION 3.21: *Es sei V ein Vektorraum über einem Körper K und $U \subseteq V$ ein Untervektorraum von V. Eine Teilmenge der Form*

$$v + U := \{v + u : u \in U\}$$

bezeichnet man als Nebenklasse von V modulo U und das Element v als Repräsentanten der Nebenklasse $v + U$.

Die Menge aller Nebenklassen von V modulo U wird mit dem Symbol V/U bezeichnet.

Eine Teilmenge $R \subseteq V$ heißt Repräsentantensystem von V/U falls die Abbildung

$$R \to V/U,\ v \mapsto v + U$$

bijektiv ist.

BEMERKUNG: Im Fall $K = \mathbb{R}$ können Untervektorräume U des Vektorraums $\mathbb{R}^\ell$ geometrisch je nach Dimension als Ursprungsgeraden, Ursprungsebenen usw. aufgefasst werden. Die Nebenklassen $v+U$ können dann als um v verschobene Ursprungsgeraden, Ursprungsebenen usw. interpretiert werden.

Einige elementare Eigenschaften von Nebenklassen sind im Folgenden zusammengefasst:

FESTSTELLUNG 3.22: *Es sei V ein Vektorraum über dem Körper K und $U \subseteq V$ ein Untervektorraum von V.*

1. $\forall v, v' \in V \quad v + U = v' + U \Leftrightarrow v - v' \in U$.
2. $\forall v, v' \in V \quad v + U \neq v' + U \Rightarrow v + U \cap v' + U = \emptyset$.
3. *Für jedes Repräsentantensystem R von V/U gilt* $V = \bigcup_{v \in R} v + U$.

BEWEIS: 1.: Aus $v + U = v' + U$ folgt $v \in v' + U$, da $v = v + 0 \in v + U$. Folglich gilt $v = v' + u$ mit einem $u \in U$. Es ergibt sich $v - v' = u \in U$ wie behauptet.

Ist andererseits $v - v' \in U$, so gilt $v = v' + u$ mit einem $u \in U$. Für jedes $w \in v + U$ gilt dann $w = v + u' = v' + u + u' \in v' + U$, da $u + u' \in U$. Also liegt die Inklusion $v + U \subseteq v' + U$ vor. Für jedes $w' \in v' + U$ gilt andererseits $w' = v' + u' = v - u + u' \in v + U$, da $u' - u \in U$. Damit gilt auch die Inklusion $v' + U \subseteq v + U$ und die Behauptung ist bewiesen.

2. Es sei $w \in v + U \cap v' + U$. Dann gilt $w = v + u = v' + u'$ für gewisse $u, u' \in U$. Folglich ist $v - v' = u' - u \in U$, womit nach Punkt 1 $v + U = v' + U$ gilt.

3. Da stets $v \in v + U$ gilt, hat man trivialerweise $V = \bigcup_{v \in V} v + U$. Nach Definition eines Repräsentantensystems gibt es zu jeder Nebenklasse $v + U$ ein $v' \in R$ mit $v' + U = v + U$, was die Behauptung beweist. □

Im Fall des endlichen Vektorraums $\mathbb{F}_2^\ell$ sind alle Nebenklassen endliche Mengen und man hat die folgenden zusätzlichen Informationen:

FESTSTELLUNG 3.23: *Es sei C ein Untervektorraum von $\mathbb{F}_2^\ell$. Dann gelten die Gleichungen*

$$\forall z \in \mathbb{F}_2^\ell \quad |z + C| = |C|,$$

und

$$|\mathbb{F}_2^\ell / C| = \frac{2^\ell}{|C|} = 2^{\ell - \dim(C)}.$$

BEWEIS: Für jedes $z \in \mathbb{F}_2^\ell$ ist die Translationsabbildung

$$\mathbb{F}_2^\ell \to \mathbb{F}_2^\ell,\ y \mapsto y + z$$

bijektiv. Hieraus folgt die erste Gleichung. Die zweite Gleichung ergibt sich nun aus Punkt 3 von Feststellung 3.22. □

BEISPIEL 3.24 (Forts. Beispiel 2.29): Für den linearen Kode

$$C = \{(0,0,0,0,0)^t, (1,1,1,0,0)^t, (0,0,1,1,1)^t, (1,1,0,1,1)^t\} \subset \mathbb{F}_2^5$$

ergeben sich neben C selbst sieben Nebenklassen von $\mathbb{F}_2^5$ modulo C:

$$\begin{array}{rcl}
(1,0,0,0,0)^t + C & = & \{(1,0,0,0,0)^t, (0,1,1,0,0)^t, (1,0,1,1,1)^t, (0,1,0,1,1)^t\} \\
(0,1,0,0,0)^t + C & = & \{(0,1,0,0,0)^t, (1,0,1,0,0)^t, (0,1,1,1,1)^t, (1,0,0,1,1)^t\} \\
(0,0,1,0,0)^t + C & = & \{(0,0,1,0,0)^t, (1,1,0,0,0)^t, (0,0,0,1,1)^t, (1,1,1,1,1)^t\} \\
(0,0,0,1,0)^t + C & = & \{(0,0,0,1,0)^t, (1,1,1,1,0)^t, (0,0,1,0,1)^t, (1,1,0,0,1)^t\} \\
(0,0,0,0,1)^t + C & = & \{(0,0,0,0,1)^t, (1,1,1,0,1)^t, (0,0,1,1,0)^t, (1,1,0,1,0)^t\} \\
(0,1,0,0,1)^t + C & = & \{(0,1,0,0,1)^t, (1,0,1,0,1)^t, (0,1,1,1,0)^t, (1,0,0,1,0)^t\} \\
(0,1,0,1,0)^t + C & = & \{(0,1,0,1,0)^t, (1,0,1,1,0)^t, (0,1,1,0,1)^t, (1,0,0,0,1)^t\}.
\end{array}$$

◇

Ist C die Menge der Kodewörter eines linearen Kodes c, so kann die Nebenklasse $z + C$ zu einem $z \in \mathbb{F}_2^\ell$ gedeutet werden als Menge der mit dem Fehler z gestörten Kodewörter. Im Rahmen der Maximum-Likelihood-Dekodierung interessant ist nun die Tatsache, dass es in $z + C$ stets ein Element z_0 mit minimalem Gewicht unter allen Elementen von $z + C$ gibt. Nach Feststellung 3.22 gilt

$$z + C = z_0 + C,$$

das heißt die Menge der gestörten Kodewörter $z + C$ kann durch eine Minimalstörung z_0 erzeugt werden. Dies motiviert die nächste Definition:

Definition 3.25: *Es sei C die Menge der Kodewörter eines linearen Kodes $c : \mathbb{A} \to \mathbb{F}_2^\ell$. Ein Element $z_0 \in z + C$ einer Nebenklasse $z + C$ heißt Nebenklassenführer von $z + C$, falls*

$$w(z_0) = \min(w(z + x) : x \in C)$$

gilt.

Beispiel 3.26 (Forts. Beispiel 3.24): Die Nebenklassenführer in Beispiel 3.24 sind die folgenden:

$$\begin{array}{rcl} C & : & (0,0,0,0,0)^t \\ (1,0,0,0,0)^t + C & : & (1,0,0,0,0)^t \\ (0,1,0,0,0)^t + C & : & (0,1,0,0,0)^t \\ (0,0,1,0,0)^t + C & : & (0,0,1,0,0)^t \\ (0,0,0,1,0)^t + C & : & (0,0,0,1,0)^t \\ (0,0,0,0,1)^t + C & : & (0,0,0,0,1)^t \\ (0,1,0,0,1)^t + C & : & (0,1,0,0,1)^t, (1,0,0,1,0)^t \\ (0,1,0,1,0)^t + C & : & (0,1,0,1,0)^t, (1,0,0,0,1)^t. \end{array}$$

Insbesondere zeigt dieses Beispiel, dass eine Nebenklasse mehrere Nebenklassenführer besitzen kann. ◇

Mit Hilfe der Nebenklassenführer kann ein Algorithmus zur ML-Dekodierung formuliert werden, der deutlich effizienter ist als eine systematische Suche im Raum $\mathbb{F}_2^\ell$.

SATZ 3.27 (ALGORITHMUS ZUR SYNDROM-DEKODIERUNG): *Für einen linearen Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ der Dimension k kann eine ML-Dekodierung nach folgendem Verfahren erfolgen:*

1. ***Initialisierung:***
   - *Bestimme eine Kontrollmatrix $H \in \mathbb{F}_2^{(\ell-k)\times\ell}$ zu c.*
   - *Bestimme zu jeder Nebenklasse $z + C \in \mathbb{F}_2^\ell/C$ einen Nebenklassenführer.*
     Seien $z_1, z_2, \ldots, z_{2^{\ell-k}}$ die dann vorliegenden Nebenklassenführer.
   - *Berechne die sogenannten Syndrome $Hz_1, \ldots, Hz_{2^{\ell-k}} \in \mathbb{F}_2^{\ell-k}$.*
2. ***Dekodierung:*** *Sei $y \in \mathbb{F}_2^\ell$ ein empfangenes Wort.*
   - *Berechne das Syndrom $Hy \in \mathbb{F}_2^{\ell-k}$.*
   - *Bestimme $i \in \{1, \ldots, 2^{\ell-k}\}$ mit $Hy = Hz_i$.*
   - *Dekodiere y zu $y - z_i$.*

BEWEIS: Es ist nur zu zeigen, dass die beschriebene Dekodierungsabbildung tatsächlich eine ML-Dekodierung von c, das heißt das $y - z_i$ ein Kodewort mit minimaler Hamming-Distanz zu y ist.

Zunächst gilt: Die angegebene Dekodierungabbildung ist vollständig.

Denn nach Definition bilden die Nebenklassenführer ein Repräsentantensystem der Menge $\mathbb{F}_2^\ell/C$, es gibt also zu gegebenem y ein eindeutig bestimmtes z_i mit $y \in z_i + C$. Damit gilt $y = z_i + x$ mit $x \in C$, also $Hy = H(z_i + x) = Hz_i + Hx = Hz_i$, womit y zu $x = y - z_i$ dekodiert wird.

Sei nun $x \in C$ ein Kodewort mit minimalem Abstand zu $y \in z_i + C$, dann gilt:

$$\begin{aligned} w(y-x) = h(y,x) &= \min(h(y,x') : x' \in C) \\ &= \min(h(y,x') : x' \in C) \\ &= \min(w(y-x') : x' \in C) \\ &= \min(w(z) : z \in y + C) \\ &= \min(w(z) : z \in z_i + C). \end{aligned}$$

Folglich ist $y - x$ ein Nebenklassenführer von $z_i + C$, womit

$$h(y,x) = w(y-x) = w(y-z_i)$$

gilt und die Dekodierungsabbildung tatsächlich eine ML-Dekodierung ist. □

BEISPIEL 3.28: Wir kehren zum Beispiel 3.8 zurück und sammeln zunächst die bereits bekannte Information: Der betrachtete Kode ist

$$C = \{(0,0,0,0,0)^t, (1,1,1,0,0)^t, (0,0,1,1,1)^t, (1,1,0,1,1)^t\} \subset \mathbb{F}_2^5$$

und besitzt die Kontrollmatrix

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

Aus der in Beispiel 3.24 erstellten Liste wählt man die Nebenklassenführer

$$\begin{array}{ll} z_1 = (0,0,0,0,0)^t, & z_5 = (0,0,0,1,0)^t \\ z_2 = (1,0,0,0,0)^t, & z_6 = (0,0,0,0,1)^t \\ z_3 = (0,1,0,0,0)^t, & z_7 = (0,1,0,0,1)^t \\ z_4 = (0,0,1,0,0)^t, & z_8 = (0,1,0,1,0)^t. \end{array}$$

Damit ergeben sich die folgenden Syndrome:

$$\begin{array}{ll} Hz_1 = (0,0,0)^t, & Hz_5 = (0,1,0)^t \\ Hz_2 = (1,0,1)^t, & Hz_6 = (0,1,1)^t \\ Hz_3 = (1,0,0)^t, & Hz_7 = (1,1,1)^t \\ Hz_4 = (0,0,1)^t, & Hz_8 = (1,1,0)^t. \end{array}$$

Angenommen das Wort $y = (1,0,1,1,0)^t$ wurde empfangen. Sein Syndrom ist

$$Hy = (1,1,0)^t = Hz_8,$$

womit y zu

$$y - z_8 = (1,0,1,1,0)^t - (0,1,0,1,0)^t = (1,1,1,0,0)^t$$

dekodiert wird. $\diamond$

3.4 Hamming-Kodes

Ein praxistauglicher Kode sollte mindestens 1-fehlerkorrigierend sein. Daher wird im Folgenden zunächst untersucht, wie man lineare, 1-fehlerkorrigierende Kodes konstruieren kann. Das Ergebnis führt zu einer Familie praxisrelevanter linearer, 1-fehlerkorrigierender, perfekter Kodes.

Sei $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein linearer, 1-fehlerkorrigierender Kode der Dimension $k := \dim(C)$ und $r := \ell - k$. Weiter sei $H \in \mathbb{F}_2^{r \times \ell}$ eine Kontrollmatrix von c. Man beobachtet zunächst, dass H keine Nullspalte besitzen kann: Wäre nämlich die i-te Spalte gleich 0 und $x \in C \setminus \{0\}$, so erhielte man

$$H(x + e_i) = Hx + He_i = 0$$

und folglich $x + e_i \in C$. Da für die Minimaldistanz von c die Ungleichung $h_{\min}(c) \geq 3$ gilt, ist dies unmöglich.

Die Matrix H kann auch keine zwei gleichen Spalten besitzen: Wären nämlich die i-te und j-te Spalte gleich, so erhielte man für $x \in C$:

$$H(x + e_i + e_j) = Hx + He_i + He_j = 2He_i = 0,$$

also $x + e_i + e_j \in C$, was wegen $h(x, x + e_i + e_j) = 2$ wiederum unmöglich ist.

Wir haben also notwendige Bedingungen dafür gefunden, dass ein linearer Kode 1-fehlerkorrigierend ist. Sie sind sogar hinreichend:

Satz 3.29: *Ein linearer Kode $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ist genau dann 1-fehlerkorrigierend, wenn eine Kontrollmatrix H mit paarweise verschiedenen Spalten und ohne Nullspalte existiert. Die beiden zuletzt genannten Eigenschaften gelten dann für jede Kontrollmatrix von c.*

Beweis: Es wurde bereits gezeigt, dass jede Kontrollmatrix eines linearen, 1-fehlerkorrigierenden Kodes die genannten Eigenschaften besitzt. Es ist daher nur noch die (interessantere) Implikation $\Leftarrow$, das heißt $h_{\min}(c) \geq 3$, zu beweisen.

Es sei H eine Kontrollmatrix von c. Weiter sei $x \in C$ und für das Wort y gelte $h(x, y) = 1$, dann besitzt y die Form $y = x + e_i$ für ein $i \in \{1, \ldots, \ell\}$. Da H nach Voraussetzung keine Nullspalte besitzt, ist

$$Hy = H(x + e_i) = Hx + He_i = He_i \neq 0,$$

also $y \notin C$. Folglich ist $h_{\min}(c) \geq 2$.

Für zwei Kodewörter $x, x' \in C$ mit $h(x, x') = 2$ gilt $x' = x + e_i + e_j$ mit $i \neq j$. Es folgt

$$He_i = H(x + e_i) = H(x' + e_j) = He_j.$$

Da H paarweise verschiedene Spalten besitzt, kann dieser Fall nicht eintreten und die Behauptung ist bewiesen. □

Satz 3.29 liefert eine Bauanleitung für 1-fehlerkorrigierende Kodes der Blocklänge ℓ und Dimension k:

1. Man wähle eine Matrix $H \in \mathbb{F}_2^{\ell-k\times\ell}$ vom Rang $\ell - k$ mit paarweise verschiedenen Spalten und ohne Nullspalte.

2. Man ermittle eine Lösung $X = G$ vom Rang k der Matrixgleichung $HX = 0$.

Der von den Spalten der Matrix G erzeugte Unterraum $C \subseteq \mathbb{F}_2^\ell$ ist dann 1-fehlerkorrigierend. Weder der erste noch der zweite Schritt dieser Bauanleitung sind bei gegebenen ℓ und k notwendigerweise durchführbar.

Beispiel 3.30: Der Versuch einen 1-fehlerkorrigierenden Kode $C \subset \mathbb{F}_2^5$ der Dimension $k = 3$ zu konstruieren, scheitert am ersten Schritt der Bauanleitung, da die gesuchte Matrix H fünf verschiedene Spalten aus dem Raum $\mathbb{F}_2^2$ besitzen müsste; dieser besitzt aber nur vier verschiedene Elemente.

Betrachtet man dagegen den Fall $\ell = 6$, so kann eine Matrix mit den gesuchten Eigenschaften angegeben werden:

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

Die Spalten der im Schritt 2 gesuchten Matrix G liegen nach Definition im Kern der linearen Abbildung

$$f_H : \mathbb{F}_2^6 \to \mathbb{F}_2^3,\ y \mapsto Hy.$$

Da f_H nach Konstruktion surjektiv ist, folgt aus der Dimensionsformel für lineare Abbildungen $\dim(\mathrm{Ker}\,(f_H)) = 3$, es gibt also tatschlich drei linear unabhängige Lösungen der Gleichung $Hy = 0$, womit man $C = \mathrm{Ker}\,(f_H)$ erhält und eine Matrix G vom Rang 3 gerade jede Erzeugermatrix von C

ist. Schreibt man $Hy = 0$ in Koordinaten aus, erhält man das lineare Gleichungssystem

$$\begin{aligned} y_1 + y_4 + y_5 &= 0 \\ y_2 + y_4 + y_6 &= 0 \\ y_3 + y_5 + y_6 &= 0 \end{aligned}$$

mit der Lösungsmenge

$$C = \{ \begin{pmatrix} y_4 + y_5 \\ y_4 + y_6 \\ y_5 + y_6 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} : y_4, y_5, y_6 \in \mathbb{F}_2 \}.$$

Anhand dieser Parameterdarstellung des Kodes C sieht man leicht, dass für die Kodewörter $x = (x_1, x_2, x_3, x_4, x_5, x_6)^t \in C$ die folgende Gewichtsverteilung vorliegt:

- $w((x_4, x_5, x_6)) = 1 \Rightarrow w(x) = 3$ (drei Kodewörter),
- $w((x_4, x_5, x_6)) = 2 \Rightarrow w(x) = 4$ (drei Kodewörter),
- $w((x_4, x_5, x_6)) = 3 \Rightarrow w(x) = 3$ (ein Kodewort).

$\diamond$

Wir verschärfen nun die Anforderungen an die betrachteten Kodes und fordern anstelle der 1-Fehlerkorrektur sogar die 1-Perfektheit. Ist $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein solcher Kode, so gilt nach Satz 2.31 die Gleichung

$$2^\ell = |\mathbb{A}|(1 + \ell) = 2^k(1 + \ell).$$

Folglich ist $1 + \ell = 2^r$, woraus sich

$$2^{2^r - 1} = 2^{k+r}$$

und damit

$$k = \dim(C) = 2^r - r - 1$$

ergibt. Man vergleiche dies mit Fall 3 des Satzes 2.34.

SATZ 3.31: *(R.W.Hamming) Zu jeder Zahl $r \in \mathbb{N}$ existiert ein linearer, 1-perfekter Kode der Blocklänge $2^r - 1$ und der Dimension $2^r - r - 1$.*

Genauer: Ist $H \in \mathbb{F}_2^{r \times 2^r - 1}$ eine Matrix mit paarweise verschiedenen Spalten, von denen keine gleich 0 ist, so ist jeder lineare Kode, für den H eine Kontrollmatrix ist, 1-perfekt.

BEMERKUNG: Lineare, 1-perfekte Kodes werden nach ihrem Entdecker als *Hamming-Kodes* bezeichnet.

BEWEIS: Es sei $H \in \mathbb{F}_2^{r \times 2^r - 1}$ eine Matrix wie im Satz angegeben. Dann bestehen die Spalten von H aus einer Permutation der Elemente von $\mathbb{F}_2^r \setminus \{0\}$.

Existiert überhaupt ein linearer Kode c für den H eine Kontrollmatrix ist, so ist dieser nach Satz 3.29 1-fehlerkorrigierend und es gilt die Gleichung

$$|\mathbb{A}|(\ell + 1) = 2^{2^r - r - 1} 2^r = 2^\ell.$$

Jede Kugel $B[x, 1]$ um ein Kodewort enthält $\ell + 1$ Elemente und, da c 1-fehlerkorrigierend ist, außer x kein weiteres Kodewort. Folglich besagt die obige Gleichung, dass jedes $y \in \mathbb{F}_2^\ell$ in genau einer Kugel $B[x, 1]$ liegt und c folglich 1-perfekt ist.

Um die Existenz eines linearen Kodes c mit H als Kontrollmatrix zu beweisen, genügt es zu zeigen, dass die Matrixgleichung $HX = 0$ eine Lösung G vom Rang $k = 2^r - r - 1$ besitzt.

Man nimmt zunächst an, dass die Matrix H die Form

$$H = (E_r \; P)$$

besitzt, wobei E_r die $r \times r$-Einheitsmatrix und $P \in \mathbb{F}_2^{r \times k}$ ist. Schreibt man dann das gesuchte G in der Form

$$G = \begin{pmatrix} G_r \\ G' \end{pmatrix},$$

mit $G_r \in \mathbb{F}_2^{r \times k}$ und $G' \in \mathbb{F}_2^{k \times k}$, so sieht man, dass man die Koeffizienten von G' beliebig vorgeben und daraus die Koeffizienten von G_r berechnen kann. Insbesondere kann man für G' eine invertierbare Matrix vorgeben, womit die Behauptung im vorliegenden Fall gezeigt ist.

Im allgemeinen Fall gibt es eine Matrix $Q \in \mathbb{F}_2^{2^r - 1 \times 2^r - 1}$ die eine Permutation der Spalten von H so bewirkt, dass $HQ = (E_r \; P)$ gilt. Die Matrix Q ist invertierbar. Man kann also die Matrixgleichung

$$(HQ)Y = 0$$

betrachten, die nach dem bereits Bewiesenen eine Lösung $Y = G_1$ mit linear unabhängigen Spalten besitzt. Dann sind auch die Spalten der Matrix $G := QG_1$ linear unabhängig und G löst die Gleichung $HX = 0$. □

BEISPIEL 3.32 ([7, 4]-HAMMING-KODE): Betrachtet man die Aussage von Satz 3.31 für $r = 3$, so ergibt sich $\ell = 2^r - 1 = 7$ und $k = 2^r - r - 1 = 4$. Eine Kontrollmatrix H des gesuchten Kodes muss $r = 3$ Zeilen haben und in den Spalten stehen alle von 0 verschiedenen Elemente von $\mathbb{F}_2^3$. Man kann also zum Beispiel die Kontrollmatrix

$$H := \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 \end{pmatrix} =: (E_3\ P)$$

vorgeben. Wie früher gezeigt, ist eine Erzeugermatrix zu einer solchen Kontrollmatrix durch

$$G = \begin{pmatrix} P \\ E_4 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Ausgeschrieben sind die 16 Elemente des Kodes also:

$$\begin{aligned} 0 &= (0,0,0,0,0,0,0)^t \\ x_1 &= (0,1,1,1,0,0,0)^t \quad , \\ x_2 &= (1,0,1,0,1,0,0)^t \quad , \\ x_3 &= (1,1,0,0,0,1,0)^t \quad , \\ x_4 &= (1,1,1,0,0,0,1)^t \quad , \end{aligned} \qquad \begin{aligned} x_1 + x_2 &= (1,1,0,1,1,0,0)^t \\ x_1 + x_3 &= (1,0,1,1,0,1,0)^t \\ x_1 + x_4 &= (1,0,0,1,0,0,1)^t \\ x_2 + x_3 &= (0,1,1,0,1,1,0)^t \\ x_2 + x_4 &= (0,1,0,0,1,0,1)^t \\ x_3 + x_4 &= (0,0,1,0,0,1,1)^t \\ x_1 + x_2 + x_3 &= (0,0,0,1,1,1,0)^t \\ x_1 + x_2 + x_4 &= (0,0,1,1,1,0,1)^t \\ x_1 + x_3 + x_4 &= (0,1,0,1,0,1,1)^t \\ x_2 + x_3 + x_4 &= (1,0,0,0,1,1,1)^t \\ x_1 + x_2 + x_3 + x_4 &= (1,1,1,1,1,1,1)^t. \end{aligned}$$

Der Kode besitzt demnach 7 Kodewörter vom Gewicht 3, 7 Kodewörter vom Gewicht 4 und ein Kodewort vom Gewicht 7. ◇

Die Syndrom-Dekodierung von Hamming-Kodes ist besonders einfach, was zu den Stärken dieser Kodes zählt: Jedes Wort $y \in \mathbb{F}_2^{2^r-1}$ liegt in genau einer Kugel $B[x,1]$, das heißt es gilt $y = x + e_i$ mit einem Element e_i der Standardbasis (13). Es gilt also $y + C = e_i + C$ und $Hy = He_i$. Dies zeigt, dass man die Elemente der Standardbasis als Nebenklassenführer benutzen kann und die Syndrom-Dekodierung dann wie folgt abläuft:

1. **Initialisierung:** Bestimme eine Kontrollmatrix $H \in \mathbb{F}_2^{r \times \ell}$.
2. **Dekodierung:** Sei $y \in \mathbb{F}_2^{\ell}$ ein empfangenes Wort.
   - Berechne das Syndrom $Hy \in \mathbb{F}_2^r$.
   - Ist $Hy = 0$, dekodiere y zu y.
   - Ist $Hy \neq 0$, bestimme $i \in \{1, \ldots, 2^r - 1\}$ mit $Hy = He_i$.
   - Dekodiere y zu $y - e_i$.

Nach Satz 2.35 gilt für die totale Fehlerwahrscheinlichkeit eines Hamming-Kodes bei ML-/Syndrom-Dekodierung:

$$p_{\text{tot}}(c,d) = 1 - (1-p_0)^{2^r-1} - (2^r-1)p_0(1-p_0)^{2^r-2}.$$

Dies offenbart eine Schwäche der Hamming-Kodes: Betrachtet man die in der Gleichung für $p_{\text{tot}}(c,d)$ auftretende Funktion

$$f(t) := (1-p_0)^{2^t-1} + (2^t-1)p_0(1-p_0)^{2^t-2}$$

für $t \geq 1$, so gilt

$$f(t) = (1-p_0)^{2^t-2}(1-p_0+(2^t-1)p_0) = (1-p_0)^{2^t-2}(1+(2^t-2)p_0),$$

und daher für $p_0 \in (0,1)$

$$\lim_{t\to\infty} f(t) = 0.$$

Hieraus ergibt sich unmittelbar

$$\lim_{r\to\infty} p_{\text{tot}}(c,d) = 1,$$

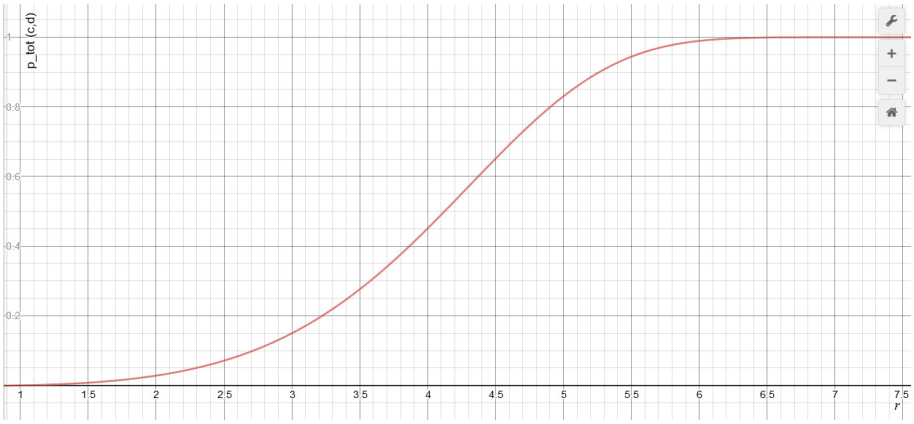


Abbildung 23: Totale Fehlerwahrscheinlichkeit von Hamming-Kodes in Abhängigkeit vom Parameter r bei einer Bitfehlerrate von $p_0 = 0.1$

das heißt mit zunehmendem Parameter r verlieren Hamming-Kodes ihre Güte in Bezug auf die Fehlklassifikationswahrscheinlichkeit bei fester Bitfehlerrate p_0. Die Abbildung 23 zeigt die Situation für den Fall $p_0 = 0.1$.

Im folgenden Beispiel wird eine Kodekonstruktion verwendet, die es verdient unabhängig vom Beispiel formuliert zu werden:

FESTSTELLUNG 3.33: *Es seien* $c_1 : \mathbb{A}_1 \to \mathbb{F}_2^\ell$ *und* $c_2 : \mathbb{A}_2 \to \mathbb{F}_2^\ell$ *lineare Kodes mit dere Eigenschaft* $C_1 \cap C_2 = 0$, $C_i := c_i(\mathbb{A}_i)$. *Dann ist*

$$c : \mathbb{A}_1 \times \mathbb{A}_2 \to \mathbb{F}_2^\ell,\ (a_1, a_2) \mapsto c_1(a_1) + c_2(a_2)$$

ein linearer Kode mit den Kodewörtern $C = C_1 \oplus C_2$.

BEWEIS: Die Summe zweier Untervektorräume eines Vektorraums ist selbst ein Untervektorraum. Im vorliegenden Fall ist nach Annahme die Summe sogar direkt: Die Darstellung $x_1 + x_2$ eines Elements $x \in C_1 + C_2$ ist eindeutig. Daher gilt $|C_1 + C_2| = |C_1|\,|C_2|$, womit die Abbildung c die Menge $\mathbb{A}_1 \times \mathbb{A}_2$ bijektiv auf C abbildet. □

Beispiel 3.34 (USB-Sticks): **U**niversal-**S**erial-**B**us-Sticks (im engeren Sinn) dienen der Massenspeicherung von Daten in binär digitalisiertem Format. Zur Speicherung werden so genannte Flash-**E**lectrically-**E**rasable-**P**rogrammable-**R**ead-**O**nly-**M**emory-Bausteine verwendet, die bei niedrigem Energieaufwand die nichtflüchtige, allerdings auch vergleichsweise langsame Speicherung der Daten ermöglichen. Flash-EEPROMs gibt es in zwei Bauarten, NOR- und NAND-Flashes, die sich in der Art des Zugriffs auf die Daten unterscheiden. In beiden Fällen werden die einzelnen Bits jeweils in einem Feldeffekttransistor gespeichert. Speicherung und Lesezugriff auf die gespeicherten Bits können bei einem NAND-Baustein nur gruppenweise erfolgen, das heißt es müssen stets simultan ganze Gruppen, so genannte Pages, von Speicherzellen beschrieben oder gelesen werden. Eine typische Page-Größe ist 4 KB also $1024 \cdot 4 = 4096$ Bit. Bei NOR-Bausteinen dagegen erfolgt der Zugriff pro Speicherzelle.

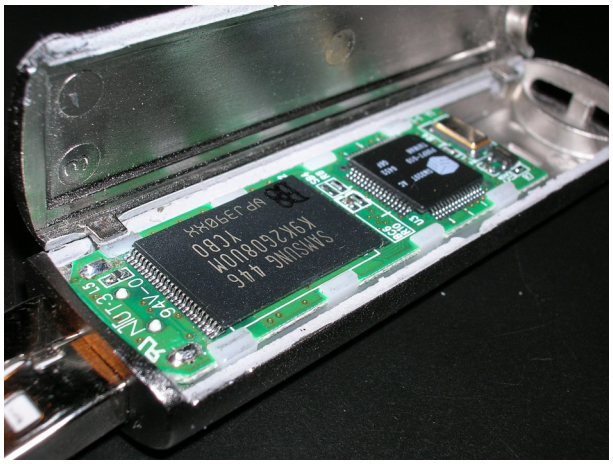


Abbildung 24: USB-Stick: links: Flash-EEPROM, rechts: Microcontroller
(Quelle: Nrbelex, CC BY-SA 3.0,
`https://commons.wikimedia.org/w/index.php?curid=179956`)

Feldeffekttransistoren unterliegen einem durch die Schreib-Lesezugriffe verursachten Abnutzungsprozess, der schließlich nach größenordnungsmäßig 30 000 Lese-Schreib-Zyklen zur Zerstörung der Transistorstruktur führt. Um dem durch den Abnutzungsprozess verursachten fehlerhaften Speichern oder Lesen von Bits entgegenzuwirken werden unter anderem fehlerkorrigierende Kodes verwendet. Die Kodierung und Dekodierung wird dabei von einem

sogenannten Microcontroller übernommen, der in den USB-Stick eingebaut ist.

Der im folgenden beschriebene binäre Blockkode ist der Technical Note TN-29-08 »Hamming Codes for NAND Flash Memory Devices« (2005) des Unternehmens Micron Technology, einem Hersteller von Halbleiterbausteinen, entnommen.

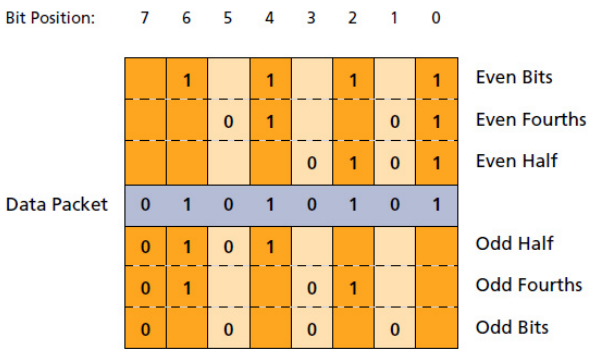


Abbildung 25: Berechnung der Kontrollsymbole für ein 8-Bit-Datenpaket

Wir betrachten Datenpakete von 8 Bit Länge (*Bytes*), also Elemente von $\mathbb{F}_2^8$. Jedem solchen Element ordnet man wie in Abbildung 25 sechs zusätzliche Bits zu. Schreibt man diese Zuordnung als Abbildung, so ergibt sich der Kode

$$
\begin{array}{rcl}
c : \mathbb{F}_2^8 & \to & \mathbb{F}_2^{14} \\
\begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} & \mapsto & \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_5 + x_6 + x_7 + x_8 \\ x_3 + x_4 + x_7 + x_8 \\ x_2 + x_4 + x_6 + x_8 \\ x_1 + x_2 + x_3 + x_4 \\ x_1 + x_2 + x_5 + x_6 \\ x_1 + x_3 + x_5 + x_7 \end{pmatrix}.
\end{array}
$$

Da die Koordinatenabbildungen von c linear in den Koordinaten x_i sind, ist c eine lineare Abbildung. Folglich ist das Bild $C := c(\mathbb{F}_2^8)$ ein Untervektorraum von $\mathbb{F}_2^{14}$.Wegen der ersten acht Koordinatenabbildungen ist c injektiv ist und damit ein linearer Kode. Eine Basis des Untervektorraums C erhält man, indem man die Bilder der Basis $e_1, \ldots, e_8$ von $\mathbb{F}_2^8$ berechnet. Eine Erzeugermatrix von c erhält man dann, indem man diese Bilder als Spalten einer Matrix auffasst. So ergibt sich die Erzeugermatrix

$$G := \begin{pmatrix} E_8 \\ P \end{pmatrix},$$

wobei

$$P := \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix};$$

es handelt sich bei c also insbesondere um einen systematischen Kode. Damit können wir nach Formel (38) eine Kontrollmatrix von c angeben:

$$H = (P\ E_6).$$

Man beachte, dass die Spalten von H paarweise verschieden sind und keine davon eine Nullspalte ist. Nach Satz 3.29 ist c also 1-fehlerkorrigierend, kann jedoch kein Hamming-Kode sein, da das Dimensionspaar $(14, 8)$ nicht von der Form $(2^r - 1, 2^r - 1 - r)$ ist. Der Kode c ist jedoch aus zwei Hamming-Kodes der Dimension 4 und Blocklänge 7 zusammengesetzt. Um dies zu sehen, betrachtet man die beiden Untervektorräume

$$U_1 := \mathbb{F}_2 e_1 + \mathbb{F}_2 e_2 + \mathbb{F}_2 e_3 + \mathbb{F}_2 e_4,\ U_2 := \mathbb{F}_2 e_5 + \mathbb{F}_2 e_6 + \mathbb{F}_2 e_7 + \mathbb{F}_2 e_8$$

des $\mathbb{F}_2^8$. Es gilt $\mathbb{F}_2^8 = U_1 \oplus U_2$ und die beiden Abbildungen

$$\begin{array}{rcl} c_1 : U_1 & \to & \mathbb{F}_2^7 \\ \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{pmatrix} & \mapsto & \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_1 + x_2 + x_3 + x_4 \\ x_1 + x_2 \\ x_1 + x_3 \end{pmatrix}. \end{array}$$

und

$$c_2 : U_2 \rightarrow \mathbb{F}_2^7$$

$$\begin{pmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \end{pmatrix} \mapsto \begin{pmatrix} x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_5 + x_6 + x_7 + x_8 \\ x_5 + x_6 \\ x_5 + x_7 \end{pmatrix}.$$

sind Hamming-Kodes: Die Kontrollmatrizen besitzen die in Satz 3.29 geforderten Eigenschaften, beide Kodes sind also 1-fehlerkorrigierend. Die Blocklänge und die Dimension der Kodes entsprechen den Anforderungen an einen Hamming-Kode. Der Beweis von Satz 3.31 zeigt dann, dass es sich tatsächlich um Hamming-Kodes handelt.

Wir betrachten nun die Abbildung

$$\rho : \mathbb{F}_2^7 \times \mathbb{F}_2^7 \rightarrow \mathbb{F}_2^{14}$$

$$\left(\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \end{pmatrix}, \begin{pmatrix} y'_1 \\ y'_2 \\ y'_3 \\ y'_4 \\ y'_5 \\ y'_6 \\ y'_7 \end{pmatrix} \right) \mapsto \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y'_1 \\ y'_2 \\ y'_3 \\ y'_4 \\ y'_5 \\ y_5 - y_6 + y'_5 - y'_6 \\ y_6 + y'_6 \\ y_5 \\ y'_6 \\ y_5 \end{pmatrix}$$

Die Abbildung ρ ist bijektiv und linear. Daher ist die Abbildung

$$U_1 \oplus U_2 \rightarrow \mathbb{F}_2^{14},\ x \mapsto \rho(c_1(u_1), c_2(u_2))$$

nach Feststellung 3.13 ein linearer Kode; er ist gerade so konstruiert, dass er mit dem Kode c übereinstimmt.

NAND Flashes schreiben und lesen Daten nicht byte-weise sondern page-weise, wobei eine page aus 512 Bytes also 4096 Bits besteht. Das gerade beschriebene Prinzip lässt sich auf diesen Fall ausdehnen und führt zum hinzufügen von weiteren 24 Bits für die Fehlerkorrektur. Dadurch entsteht ein linearer Kode

$$c : \mathbb{F}_2^{4096} \to \mathbb{F}_2^{4120},$$

der zusammen mit einem ML-Dekodierungsalgorithmus in den Kontroller des Bausteins implementiert ist. In Abbildung 26 ist diese Erweiterung des Prinzips für den einfacheren Fall von nur 8 Byte also 64 Bit dargestellt. ◇

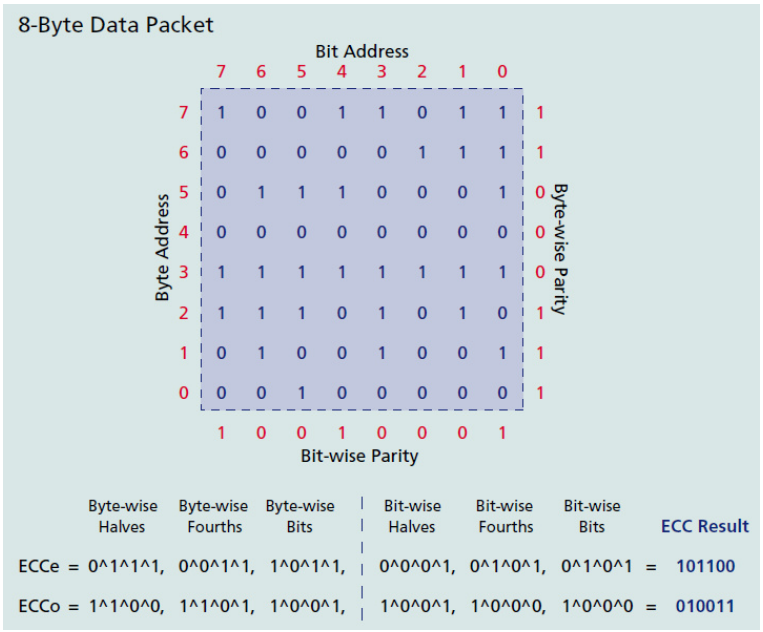


Abbildung 26: Berechnung der Kontrollsymbole für ein 8-Byte-Datenpaket

3.5 Reed-Muller-Kodes

Es ist eine naheliegende Idee zwei oder mehrere binäre Blockkodes zu »kombinieren«, um einen Blockkode etwa für ein umfangreicheres Alphabet als das der Ausgangskodes zu erzeugen. Die im Folgenden vorgestellte Methode zur rekursiven Erzeugung von binären Blockkodes stammt von dem amerikanischen Mathematiker und Ingenieur Morris Plotkin (1914 – 1990, die Angaben sind unsicher). Dessen beruflicher Lebenslauf kann nach Einschätzung des Autors des vorliegenden Skripts durchaus stellvertretend für den vieler Ingenieure und Mathematiker der damaligen Zeit gesehen werden. Einen Eindruck gibt der folgende Auszug aus den *IEEE Transactions on Reliability and Quality Control* aus dem Jahr 1965:

Morris Plotkin,(S'43 - A'45 - M'55 - SM'55), previously employed full time with AUERBACH Corporation and now a research staff member with the University of Pennsylvania, continues to provide consultation services to mathematicians, physicists, and systems engineers who are responsible for quantitatively analyzing systems and making preliminary feasibility design studies. He directed an error study on the digital computations in the SWALLOW navigation computer, in the course of which he developed original methods for the study of a precise, complex control system. He developed mathematical specifications in the BMEWS system on the extraction of signals from noise. As part of the system formulation phase of DATACOM (message switching system), he analyzed a number of critical queuing situations. In another area of activity, Mr. Plotkin developed methods of computing reliability of complex systems.

For eight years Mr. Plotkin was associated with the Naval Air Development Center at Johnsville, Pa. He directed the first simulation performed on TYPHOON., the first modern large-scale analog computer. Many of the basic techniques now standard practice in the operation of analog computers were originated or developed by Mr. Plotkin. He performed and directed the mathematical formulation of problems in missile guidance, aircraft performance, nuclear shielding, techniques for improving radar performance, and propagation of sound in water. He performed statistical analyses, including the design of a large program for sampling aircraft loading and the analysis of sufficiency of sample size in the Monte Carlo programs.

In the field of man-machine performance analysis, Mr. Plotkin established a unique flight simlation facility using a centrifuge large enough to carry a man and an analog computer. This system computes the simulated aircraft performance from the pilot's control actions and then operates the centrifuge to duplicate the actual flight maneuvers.

Prior to joining NADC, Mr. Plotkin was a research staff member of the Moore School of Electrical Engineering, University of Pennsylvania, for four years. His interests were in two fields: analytical work on military defense systems and theoretical work in connection with digital computers. In the latter category, he has received wide attention for some basic results on the minimum amount of redundancy required for error-correcting codes.

Mr. Plotkin received his B.S. degree in Electrical Engineering in 1934, his M.A. degree in Mathematics in 1951, and his M.S. degree in Electrical Engineering in 1952 from

the University of Pennsylvania. Mr. Plotkin is a member of Sigma Xi and the American Mathematical Society.

ARMS LAB WORKS ON DEVELOPMENT OF FEED MECHANISM FOR AIRCRAFT TURRET GUNS

AAL Military aircraft were built with one purpose in mind —to fight. As the aircraft improves and advances, so must the ordnance systems which are its weapons. With the advent of jet aircraft into the fleet, the need for research into advanced armament became critical. Since no commercial facilities for this kind of study existed, it was necessary for the Navy to undertake comprehensive studies in the field. The Aircraft Armament Laboratory of NADC was established in 1946 to meet this particular problem.

The AAL started in 1946 as a research and development laboratory. Later its function was changed to development only. But through the changes its mission has remained relatively constant. That mission is so broad that it encompasses practically every facet of design, test and evaluation of every kind of projectile.

The AAL, presently under the direction of Cdr. Hamilton O. Hauck, is responsible for the development, design, alteration, construction, installation, flight testing and actual range firing of all naval air guns, missiles and rockets. Above all, theirs is the task of peering into the future to design and develop entirely new systems of naval air ordnance, to adapt new developments to naval warfare; in short, to do everything to keep the armament program ahead of the high speed development of modern jet aircraft.

The AAL works with scientists, with the Bureau of Aeronautics and with ordnance and airframe contractors. The problems it studies are not limited to the development of armament alone, but also with fitting the lethal hardware into the weapons system for tactical use.

Gun mounting, for instance, is a new problem with each new aircraft that is added to the Navy's arsenal. Guns must be located where their weight will not effect the flight characteristics on the aircraft. Explosive gases must be properly vented. Lubricants must be developed that will permit the guns to operate at extremes of temperature. Bomb and rocket release and detonation devices must be foolproof. These and myriad other related problem areas are under constant and careful study by the AAL.

ACL Until a few years ago, scientists were hindered in their search for new knowledge by the fact that it was virtually physically impossible to make all of the computations necessary to prove or disprove theories evolved from then known facts. They were overcome by sheer arithmetic. They solved their own problem by developing giant computers, impossible before the advent of the electronic age.

The Naval Air Development Center was no exception. In the summer of 1950, the NADC formed its Analytical and Computer Laboratory. This new facility, now under Cdr. I. K. Blough's direction, went into business in a big way with the largest electronic analogue computer in existence,—*Typhoon*, so named, no doubt, because it is ready to cope with a veritable tidal wave of numbers.

Electronic Computers, sometime miscalled "Brains", are of two varieties—digital and analogue. The digital computer is, in effect, a gigantic adding machine, solving the problems fed to it by an astronical number of additions, many of which are retained, for use at the exact moment they are required, in what is usually called an electronic memory. The analogue computer is infinitely more complex;

ANALOGUE COMPUTER "TYPHOON" SOLVES AERODYNAMIC AND ENGINEERING PROBLEMS

Abbildung 27: Artikel zum TYPHOON Analog Computer, *Naval Aviation News*, November 1955

set up to solve difficult differential equations in an infinitesimal fraction of time that would be required for the pencil and paper method.

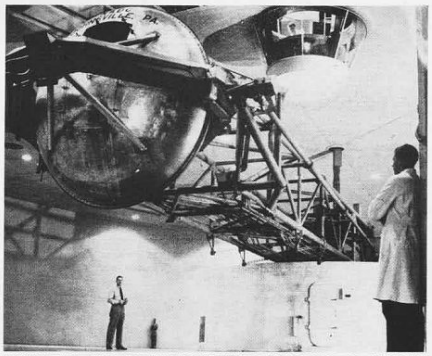
Typhoon, built by RCA for the Navy, makes airplanes fly and missiles shoot them down long before the first order is placed for the first sheet of aluminum for the first prototype model. The ACL, working with industry, saves millions and millions of dollars in proving that the gleam in the eye of the scientist can or cannot be turned into a practical piece of hardware that will add to the arsenal of the Navy's weapons.

Here is how a typical problem might work. A guided missile contractor has an idea or a requirement from the Navy that will accomplish a specific mission in the destruction of enemy aircraft that might possibly attack our forces. The scientists who conceived the basic design of such a missile reduce all of the projected data about the missile to a series of (to the layman) completely unintelligible formulae. Listed in sequence along the edge of a huge sheet of paper, these mathematical equations represent everything that is planned for the projectile—speed, power plant, wingspan, length, drag, length of time in flight, and a hundred other details of aerodynamics.

Personnel of the Analytical Computer Lab translate these formulae into electronic circuits that can be fed into the *Typhoon*. It may take six weeks to two months to relate the mathematics to electrical circuits. When this has been done the electronic circuits are fed into *Typhoon*. This probably will take another six weeks. Each circuit must be tested individually to work out the particular formula that it represents.

The characteristics of the missile are in the machine. The flight pattern of the plane it is pursuing is in, the flight time of the missile is set at, let us say, one minute. The big moment has arrived. The missile is about to fly — electronically. The switch is thrown and one minute later the results of the flight are graphically displayed on paper.

By simulating flight conditions *Typhoon* can fly a missile or an aircraft on many flights at the merest fraction of the cost of one test flight.



LARGEST HUMAN CENTRIFUGE INVESTIGATES HUMAN BARRIER, EFFECT OF "G" FORCES

AMAL Man overcame the so-called Sonic Barrier in 1947 when the first plane buffeted its way through the speed of sound and the first human raced into the unknown and became super-sonic. We are now making our first assault upon what has come to be known as the heat barrier—the speed at which friction of atmosphere will make now known metals unsuitable for aircraft and missile construction.

But there has been developing along with the advanced speeds of aircraft another kind of barrier, less discussed but no less important—the Human Barrier. Since the inception of the science of aeronautics, man has had to accept environments in which his body was not created to exist. He has risen to altitudes far beyond the tolerances of the flexible human system. He has invented the artificial aids that he needs to maintain life and consciousness and alertness. Now with the inception of really high speed flight the problem of high acceleration or "G" forces looms larger than ever.

Rapid changes of direction in an aircraft subject the human body, designed to operate under the influence of its own weight or the pull of one "G", to forces beyond the capacity of the body to withstand without damage. The injurious effect of acceleration is the product of the amount of "G's" and the length of time they are exerted on the man. Now we need to know how much a pilot can stand. For how long? In what position—sitting, standing, prone or supine?

In 1949 there was added to the facilities of the Naval Air Development Center the Aviation Medical Acceleration Laboratory. Here personnel of the Navy's Medical Corps conduct investigations with the use of a human centrifuge to define the limits of human tolerance to acceleration. Their interest runs also to the effects of high "G" forces applied to various parts of the body.

The centrifuge at AMAL, the world's largest, can produce forces up to 40 "G"—forty times the weight of the man who is being tested. The cockpit or gondola of the centrifuge in which the subject is placed is at the end of a 50-foot arm which is rotated by a giant 4,000-hp electric motor. Volunteers are whirled in a variety of positions at speeds that will produce the desired acceleration while the scientists study the effect of the "G's" on their bodies. The work of AMAL now under Capt. H. G. Shepler, will guide future aircraft, pilot equipment and safety device design.

Abbildung 28: Artikel zum TYPHOON Analog Computer, *Naval Aviation News*, November 1955

DEFINITION 3.35 (Plotkin-Konstruktion, 1960): *Es seien* $c_1 : \mathbb{A}_1 \to \mathbb{F}_2^\ell$ *und* $c_2 : \mathbb{A}_2 \to \mathbb{F}_2^\ell$ *zwei binäre Blockkodes. Dann definiert man den binären Blockkode* $c_1|c_2$ *als die Abbildung*

$$c_1|c_2 : \mathbb{A}_1 \times \mathbb{A}_2 \to \mathbb{F}_2^{2\ell},\ (a_1, a_2) \mapsto (c_1(a_1), c_1(a_1) + c_2(a_2))^t.$$

Damit die obige Definition sinnvoll ist, ist sicherzustellen, dass $c_1|c_2$ injektiv ist: Nimmt man $(c_1|c_2)(a_1, a_2) = (c_1|c_2)(b_1, b_2)$ an, so folgt nach Definition zunächst $c_1(a_1) = c_1(b_1)$, also wegen der Injektivität von c_1 die Gleichheit $a_1 = b_1$. Weiter hat man $c_1(a_1) + c_2(a_2) = c_1(b_1) + c_2(b_2)$, also nach dem bereits Gefolgerten $c_1(a_1) + c_2(a_2) = c_1(a_1) + c_2(b_2)$, woraus $c_2(a_2) = c_2(b_2)$ folgt. Die Injektivität von c_2 liefert dann $b_1 = b_2$.

FESTSTELLUNG 3.36: *Der binäre Blockkode* $c_1|c_2$ *besitzt die folgenden Eigenschaften:*

1. $h_{\min}(c_1|c_2) = \min(2h_{\min}(c_1), h_{\min}(c_2))$.
2. *Sind* c_i *lineare Kodes der Dimension* k_i*, so ist* $c_1|c_2$ *ein linearer Kode der Dimension* $k_1 + k_2$.
3. *Sind* G_i *Erzeugermatrizen von* c_i*, so ist die Matrix*

$$\begin{pmatrix} G_1 & 0 \\ G_1 & G_2 \end{pmatrix}$$

eine Erzeugermatrix von $c_1|c_2$.

BEWEIS: Zu 1.: Es seien $x := (x_1, x_1 + x_2)$ und $y := (y_1, y_1 + y_2)$ verschiedene Kodewörter von $c_1|c_2$. Dann gilt

$$\begin{aligned} h(x, y) &= h(x_1, y_1) + h(x_1 + x_2, y_1 + y_2) \\ &\geq h(x_1, y_1) + h(x_1 + x_2, x_1 + y_2) - h(y_1 + y_2, x_1 + y_2) \\ &= h(x_1, y_1) + h(x_2, y_2) - h(y_1, x_1) \\ &= h(x_2, y_2), \end{aligned}$$

wobei man in der zweiten Zeile die Dreiecksungleichung

$$h(x_1 + x_2, x_1 + y_2) \leq h(x_1 + x_2, y_1 + y_2) + h(y_1 + y_2, x_1 + y_2)$$

benutzt. Weiter hat man im Fall $x_1 = y_1 = 0$ die Gleichung $h(x, y) = h(x_2, y_2)$, sowie im Fall $x_2 = y_2$ die Gleichung $h(x, y) = 2h(x_1, y_1)$. Hieraus folgt die Behauptung.

Zu 2.: Nach Definition sind die Kodewörter von $c_1|c_2$ genau die Wörter der Form $(x_1, x_1 + x_2)$, wobei x_i Kodewörter von c_i sind. Die Summe zweier Wörter dieser Gestalt besitzt wiederum diesselbe Gestalt, womit $c_1|c_2$ linear ist.

Es gilt weiter die Gleichung

$$(x_1, x_1 + x_2) = (x_1, x_1) + (0, x_2),$$

wobei beide Summanden auf der rechten Seite Kodewörter von $c_1|c_2$ sind. Es seien $b_{1,1}, \ldots, b_{1,k_1}$ und $b_{2,1}, \ldots, b_{2,k_2}$ Basen der Kodes C_1 und C_2. Die Kodewörter der Form (x_1, x_1) lassen sich offensichtlich eindeutig als Linearkombination der Kodewörter $(b_{1,i}, b_{1,i})$ schreiben. Die Kodewörter der Form $(0, x_2)$ lassen sich ebenso offensichtlich eindeutig als Linearkombination der Kodewörter $(0, b_{2,i})$ schreiben. Folglich ist die Menge

$$\{(b_{1,i}, b_{1,i}) : i = 1, \ldots, k_1\} \cup \{(0, b_{2,i}) : i = 1, \ldots, k_2\}$$

eine Basis des Kodes $c_1|c_2$.

Zu 3.: Folgt direkt aus Punkt 2. □

Im Weiteren betrachten wir (fast) ausschließlich Alphabete der Form $\mathbb{A} = \mathbb{F}_2^n$, $n \in \mathbb{N}$. Wir stellen uns also wieder auf den Standpunkt, das ein aus dem Anwendungskontext stammendes Alphabet $\mathbb{A}$ bereits durch einen Alphabetwechsel in binäre Form gebracht wurde.

Aus technischen Gründen ist es nützlich die *trivialen Kodes*

$$\{0\} \to \mathbb{F}_2^\ell, 0 \mapsto (0, \ldots, 0)^t$$

einzuführen. Sie werden mit 0_ℓ oder auch einfach mit 0 bezeichnet.

Ist $c : \mathbb{A} \to \mathbb{F}_2^\ell$ ein binärer Blockkode, so kann man das Alphabet $\mathbb{A} \times \{0\}$ mit $\mathbb{A}$ identifizieren. Die Plotkin-Konstruktion $c|0_\ell$ liefert in diesem Sinn den Kode:

$$\mathbb{A} \to \mathbb{F}_2^{2\ell},\ a \mapsto (c(a), c(a))^t.$$

Im Folgenden wird $c|0_\ell$ immer in diesem Sinn verstanden.

Definition 3.37: *Die rekursiv durch*

$$\forall m \in \mathbb{N}_0 \quad R(m, m) := (\mathrm{id} : \mathbb{F}_2^{2^m} \to \mathbb{F}_2^{2^m}),$$

$$\forall m \in \mathbb{N} \quad R(0, m) := R(0, m-1)|0,$$

$$\forall m \in \mathbb{N}, r \in \{1, \ldots, m-1\} \quad R(r, m) := R(r, m-1)|R(r-1, m-1).$$

definierte Familie von Kodes nennt man Reed-Muller-Kodes (RM-Kodes).

Bemerkungen:

1. Die wesentliche Rekursion in der Definition der RM-Kodes ist die für $R(r,m)$, $r \neq m$, $r \neq 0$. Die Kodes $R(0,m)$ lassen sich leicht angeben: Es ist $R(0,0) = (\mathrm{id} : \mathbb{F}_2^1 \to \mathbb{F}_2^1)$, daher ist entsprechend der Bemerkung 2 zur Plotkin-Konstruktion

   $$R(0,1) : \mathbb{F}_2 \to \mathbb{F}_2^2,\ y \mapsto (y,y)^t.$$

   Hieraus ergibt sich

   $$R(0,2) : \mathbb{F}_2 \to \mathbb{F}_2^4,\ y \mapsto (y,y,y,y)^t$$

   und allgemein

   $$R(0,m) : \mathbb{F}_2 \to \mathbb{F}_2^{2^m},\ y \mapsto (y,y,\ldots,y)^t.$$

2. RM-Kodes werden in der sogenannten Deep Space Kommunikation zwischen Raumsonden untereinander und mit Empfangsstationen auf der Erde eingesetzt. Sie sind außerdem »Verwandte« der *polaren Kodes*, die im 5-G-Standard des Mobilfunknetzes eingesetzt werden.

Die Kodes $R(r,m)$ wurden im Jahr 1953 von David Eugene Muller definiert beziehungsweise entdeckt.

Abbildung 29: David Eugene Muller: 22. Mai 1959 und 15. Juli 2004

Die links zu sehende Fotografie des amerikanischen Mathematikers und Computerwissenschaftlers David Muller (1924 – 2008) stammt aus dem Archiv der University of Illinois, auf das man über die Webseite

https://archives.library.illinois.edu

zugreifen kann. David Muller arbeitete sowohl in der Computertechnik als auch in der Kodierungs- und Gruppentheorie. Die Aufnahme rechts stammt aus einem von mehreren Interviews, das David Muller zu verschiedenen Themen gab. Sie finden sich auf der Webseite

http://library.cshl.edu/oralhistory/

der Oral History Collection des Cold Spring Harbor Laboratory. Beide Eltern von David Muller waren Wissenschaftler: seine Mutter Jessie Jacobs Muller Offermann war Mathematikerin, sein Vater Hermann Joseph Muller Genetiker, der im Jahr 1946 einen Nobelpreis für Forschungen zu Mutationen, die durch Röntgenstrahlung erzeugt werden, erhielt. Bedingt durch die Arbeit des Vaters lebte David Muller zeitweise in Berlin (zur Zeit der Machtergreifung durch die Nationalsozialisten) und in Leningrad.

Satz 3.38: *Die Kodes $R(r,m)$ sind lineare Kodes der Blocklänge $\ell = 2^m$, besitzen die Dimension*

$$k = \sum_{i=0}^{r} \binom{m}{i},$$

sowie die Minimaldistanz

$$h_{\min}(R(r,m)) = 2^{m-r}.$$

Bemerkung: Man beachte, dass man durch geeignete Wahl des Parameters r bei fester Blocklänge ℓ die Minimaldistanz eines RM-Kodes in gewissem Rahmen vorgeben kann. Diese Möglichkeit bestand bei den bisher betrachteten Kodes nicht.

Beweis: Die Aussage zur Dimension folgt in den Fällen $r = m$ und $r = 0$ direkt aus der Definition beziehungsweise der Bemerkung dazu. Das gleiche gilt für die Aussage über die Minimaldistanz.

Die Aussage zur Dimension im Fall $0 < r < m$ wird durch vollständige Induktion nach $r + m$ bewiesen: Der Induktionsanfang liegt bei $r + m = 3$, in welchem Fall $r = 1$ und $m = 2$ ist. Nach Definition ist dann

$$R(1,2) = R(1,1)|R(0,1),$$

wobei $\dim R(1,1) = 2$ und $\dim R(0,1) = 1$ gilt. Nach Feststellung 3.36 ergibt sich

$$\dim R(1,2) = 3 = \binom{2}{0} + \binom{2}{1}.$$

Für den Induktionsschritt nutzt man die Pascal'sche Identität

$$\binom{m-1}{i-1} + \binom{m-1}{i} = \binom{m}{i}.$$

Es gilt nämlich nach Definition und Feststellung 3.36

$$\dim R(r,m) = \dim R(r,m-1) + \dim R(r-1,m-1).$$

Nach Induktionsannahme folgt also

$$\begin{aligned} \dim R(r,m-1) + \dim R(r-1,m-1) &= \sum_{i=0}^{r} \tbinom{m-1}{i} + \sum_{i=0}^{r-1} \tbinom{m-1}{i} \\ &= \tbinom{m-1}{0} + \sum_{i=1}^{r} \tbinom{m}{i} \\ &= \sum_{i=0}^{r} \tbinom{m}{i}. \end{aligned}$$

Nun zu den Minimaldistanzen: Im Fall $r+m=3$ liefert Feststellung 3.36

$$h_{\min}(R(1,2)) = \min(2h_{\min}(R(1,1)), h_{\min}(R(0,1))) = \min(2,2).$$

Der Induktionsschritt liefert unter Verwendung derselben Formel

$$\begin{aligned} h_{\min}(R(r,m)) &= \min(2h_{\min}(R(r,m-1)), h_{\min}(R(r-1,m-1))) \\ &= \min(2 \cdot 2^{m-1-r}, 2^{m-r}) = 2^{m-r}. \end{aligned}$$

□

Beispiel 3.39: Wir kehren zurück zum Beispiel 2.1 der Übertragung von Graustufenbildern von der Sonde Mariner 9 zur Erde. Hierbei wurde der RM-Kode

$$R(1,5) : \mathbb{F}_2^6 \to \mathbb{F}_2^{32}$$

benutzt. Er besitzt die Minimaldistanz $h_{\min}(R(1,5)) = 16$. Entsprechend der rekursiven Definition gilt

$$\begin{aligned} R(1,5) &= R(1,4)|R(0,4) \\ &= (R(1,3)|R(0,3))|R(0,4) \\ &= ((R(1,2)|R(0,2))|R(0,3))|R(0,4) \\ &= (((R(1,1)|R(0,1))|R(0,2))|R(0,3))|R(0,4). \end{aligned}$$

Es ist $R(1,1) = (\mathrm{id} : \mathbb{F}_2^2 \to \mathbb{F}_2^2)$ und $R(0,1) = (\mathbb{F}_2 \to \mathbb{F}_2^2, y \mapsto (y,y)^t)$, woraus sich

$$R(1,1)|R(0,1) = (\mathbb{F}_2^2 \times \mathbb{F}_2 \to \mathbb{F}_2^4, ((y_1,y_2)^t, y_3) \mapsto (y_1, y_2, y_1+y_3, y_2+y_3)^t$$

ergibt. Für den Kode $(R(1,1)|R(0,1))|R(0,2$ erhält man dann:

$$\begin{array}{rcl} (\mathbb{F}_2^2 \times \mathbb{F}_2) \times \mathbb{F}_2 & \to & \mathbb{F}_2^8 \\ (((y_1,y_2)^t, y_3), y_4) & \mapsto & \begin{pmatrix} y_1 \\ y_2 \\ y_1+y_3 \\ y_2+y_3 \\ y_1+y_4 \\ y_2+y_4 \\ y_1+y_3+y_4 \\ y_2+y_3+y_4 \end{pmatrix}. \end{array}$$

Dies liefert für den Kode $((R(1,1)|R(0,1))|R(0,2))|R(0,3)$:

$$\begin{array}{rcl} (\mathbb{F}_2^2 \times \mathbb{F}_2 \times \mathbb{F}_2) \times \mathbb{F}_2 & \to & \mathbb{F}_2^{16} \\ (((y_1,y_2)^t, y_3, y_4), y_5) & \mapsto & \begin{pmatrix} y_1 \\ y_2 \\ y_1+y_3 \\ y_2+y_3 \\ y_1+y_4 \\ y_2+y_4 \\ y_1+y_3+y_4 \\ y_2+y_3+y_4 \\ y_1+y_5 \\ y_2+y_5 \\ y_1+y_3+y_5 \\ y_2+y_3+y_5 \\ y_1+y_4+y_5 \\ y_2+y_4+y_5 \\ y_1+y_3+y_4+y_5 \\ y_2+y_3+y_4+y_5 \end{pmatrix}. \end{array}$$

Schließlich kann man die Abbildungsvorschrift für $R(1,5)$ angeben:

$$
\begin{array}{rcl}
R(1,5) : \mathbb{F}_2^6 & \to & \mathbb{F}_2^{32} \\
\begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \end{pmatrix} & \mapsto & \begin{pmatrix}
y_1 \\ y_2 \\ y_1+y_3 \\ y_2+y_3 \\ y_1+y_4 \\ y_2+y_4 \\ y_1+y_3+y_4 \\ y_2+y_3+y_4 \\ y_1+y_5 \\ y_2+y_5 \\ y_1+y_3+y_5 \\ y_2+y_3+y_5 \\ y_1+y_4+y_5 \\ y_2+y_4+y_5 \\ y_1+y_3+y_4+y_5 \\ y_2+y_3+y_4+y_5 \\ y_1+y_6 \\ y_2+y_6 \\ y_1+y_3+y_6 \\ y_2+y_3+y_6 \\ y_1+y_4+y_6 \\ y_2+y_4+y_6 \\ y_1+y_3+y_4+y_6 \\ y_2+y_3+y_4+y_6 \\ y_1+y_5+y_6 \\ y_2+y_5+y_6 \\ y_1+y_3+y_5+y_6 \\ y_2+y_3+y_5+y_6 \\ y_1+y_4+y_5+y_6 \\ y_2+y_4+y_5+y_6 \\ y_1+y_3+y_4+y_5+y_6 \\ y_2+y_3+y_4+y_5+y_6
\end{pmatrix}.
\end{array}
$$

$\diamond$

Prinzipiell können RM-Kodes als lineare Kodes mit Hilfe einer Kontrollmatrix dekodiert werden. Dies ist jedoch nicht immer der effizienteste Algo-

rithmus zur ML-Dekodierung. Im Fall der Mariner-Sonde wurde der Kode $R(1,5)$ auch deswegen gewählt, weil es zu seiner ML-Dekodierung schnellere Algorithmen als den Weg über eine Kontrollmatrix gibt. Eine solche Methode wurde von dem amerikanischen Mathematiker und Ingenieur Irving Stoy Reed während seiner Tätigkeit am Massachusetts Institute of Technolgy im Jahr 1953 entwickelt. Im Folgenden wird eine weitere schnelle Methode zur Dekodierung vorgestellt.

Abbildung 30: Irving Stoy Reed
(Quelle links: Nachruf Sol Golomb von M. Ballon, D. Druhora, 2016, Viterbi School of Engineering)
(Quelle rechts: Nachruf Irving Reed von K. Dunham, 2012, Viterbi School of Engineering)

Die linke Aufnahme aus dem Jahr 1963 zeigt den amerikanischen Mathematiker und Ingenieur Irving Stoy Reed (1923 – 2012) zusammen mit Kollegen der Viterbi School of Engineering der University of South Carolina. Sie zeigt laut den dortigen Angaben von links nach rechts Alfred C. Ingersoll (amerikanischer Ingenieur, 1920 – 1999), Solomon Golomb (amerikanischer Mathematiker und Ingenieur, 1932 – 2016), Irving Reed, Nasser E. Nahi (iranischer Mathematiker, 1933 – 1978) und Zohrab Kaprielian (armenischer Ingenieur).
Irving Reed war als Student an der Entwicklung eines der ersten Digitalcomputer, des Magnetic Drum Digital Differential Analyzer (MADDIDA), der in der Luftraumkontrolle eingesetzt wurde, beteiligt. Er beschäftigte sich später mit der Entwicklung von Programmiersprachen, der Theorie von Radarsystemen und der Kodierungstheorie. Was letztere angeht gehört er zu den Mathematikern, die früh die praktische Bedeutung der Theorie endlicher Körper erkannten.

Effiziente ML-Dekodierung der Kodes $R(1,m)$

Man führt zunächst Abbildungen ein, die bereits im Abschnitt 2.2 eine Rolle gespielt haben: Die Abbildung

$$\phi : \mathbb{F}_2 \to \{-1,1\},\ 0 \mapsto 1, 1 \mapsto -1 \tag{42}$$

ist ein Isomorphismus von Gruppen, wenn man $\mathbb{F}_2$ mit der Addition und $\{-1,1\}$ mit der Multiplikation versieht. Dieser liefert die bijektiven Abbildungen

$$\begin{array}{rcl} \phi_{m\times n} : \mathbb{F}_2^{m\times n} & \to & \{-1,1\}^{m\times n} \subset \mathbb{R}^{m\times n} \\ A = (a_{ij})_{i\in\{1,\ldots,m\},j\in\{1,\ldots,n\}} & \mapsto & \widehat{A} := (\phi(a_{ij}))_{i\in\{1,\ldots,m\},j\in\{1,\ldots,n\}}. \end{array}$$

Eine ML-Dekodierung eines Worts $y \in \mathbb{F}_2^\ell$ in ein Kodewort $x_0 \in C$, erfüllt die Bedingung

$$h(y,x_0) = \min(h(y,x) : x \in C).$$

Diese Bedingung lässt sich mit Hilfe von $\phi_{\ell\times 1}$ umformulieren:

Feststellung 3.40: *Die Gleichung $h(y,x_0) = \min(h(y,x) : x \in C)$ ist äquivalent zu der Gleichung*

$$\langle \widehat{y}, \widehat{x_0} \rangle = \max(\langle \widehat{y}, \widehat{x} \rangle : x \in C),$$

wobei $\langle \cdot,\cdot \rangle$ das Standardskalarprodukt bezeichnet.

Beweis: Das Skalarprodukt

$$\langle \widehat{y}, \widehat{x} \rangle = \sum_{i=1}^{\ell} \widehat{y}_i \widehat{x}_i$$

ist umso größer, je mehr Koordinaten von $\widehat{x}$ und $\widehat{y}$ gleich sind, da diese nur die Werte -1 und 1 annehmen können. □

Die obige Umformulierung der ML-Dekodierung führt in Verbindung mit den folgenden Eigenschaften der Kodes $R(1,m)$ zu einem effizienten Dekodierungsalgorithmus. Man beginnt mit der Tatsache, dass jedes Kodewort $x \in \mathbb{F}_2^{2^m}$ von $R(1,m) = R(1,m-1)|R(0,m-1)$ die Form

$$x = \begin{pmatrix} x_1 \\ x_1 + \lambda \begin{pmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \end{pmatrix},\ \lambda \in \mathbb{F}_2, \tag{43}$$

besitzt, wobei $x_1 \in \mathbb{F}_2^{2^{m-1}}$ ein Kodewort von $R(1, m-1)$ ist.

SATZ 3.41: *Die RM-Kodes $R(1,m)$, $m \geq 2$, besitzen die Eigenschaften:*

1. *Für Kodewörter x, x' mit der Eigenschaft $x - x' \notin \{0, (1, \ldots, 1)^t\}$ gilt $h(x, x') = 2^{m-1}$.*

2. *Es seien $x_1, \ldots, x_{2^m}$ diejenigen Kodewörter von $R(1,m)$, deren erste Komponente gleich 0 ist.*

   Die Nummerierung der Kodewörter sei so gewählt, dass sie die Reihenfolge wiedergibt, in der diese Kodewörter nach folgender Rekursion erzeugt werden:

   $x_1, \ldots, x_{2^{m-1}}$ seien die Kodewörter von $R(1,m)$, die sich durch Anwenden der Formel (43) mit $\lambda = 0$ auf alle Kodewörter $x'_1, \ldots, x'_{2^{m-1}}$ von $R(1, m-1)$ mit erster Komponente gleich 0 ergeben.

   $x_{2^{m-1}+1}, \ldots, x_{2^{m-1}}$ seien die Kodewörter von $R(1,m)$, die sich durch Anwenden der Formel (43) mit $\lambda = 1$ auf alle Kodewörter $x'_1, \ldots, x'_{2^{m-1}}$ von $R(1, m-1)$ mit erster Komponente gleich 0 ergeben.

   Hierbei seien die Kodewörter $x'_1, \ldots, x'_{2^{m-1}}$ entsprechend der Rekursionsvorschrift nummeriert.

   Dann ist die Matrix

$$H := (\widehat{x_1}\, \widehat{x_2} \ldots \widehat{x_{2^m}}) \in \{-1, 1\}^{2^m \times 2^m}$$

   eine Hadamard-Matrix vom Sylvestertyp.

BEMERKUNG: Man beachte, dass es zu jeder Potenz 2^m genau eine Hadamard-Matrix vom Sylvestertyp gibt, diese also unabhängig(!) vom Kode $R(1,m)$ berechnet werden kann.

BEWEIS: Zu 1.: Es genügt für jedes Kodewort $x \notin \{0, (1, \ldots, 1)^t\}$ die Gleichung

$$w(x) = 2^{m-1}$$

zu beweisen. Hierzu benutzt man die Gleichung (43) um einen Beweis durch vollständige Induktion zu führen.

Induktionsanfang bei $m = 2$: In diesem Fall ist $x_1 = (0,0)^t$ und $\lambda = 1$, in welchem Fall die Aussage stimmt, oder es ist $x_1 \in \{(1,0)^t, (0,1)^t\}$ und λ beliebig, in welchem Fall die Aussage ebenfalls stimmt,.oder es ist $x_1 = (1,1)^t$ und $\lambda = 1$, was ebenfalls zu einer korrekten Aussage führt.

Induktionsschluss: Ist $x_1 = 0$, so muss nach Annahme $\lambda = 0$ gelten, womit die Aussage stimmt.

Ist $x_1 \neq 0$ und $x_1 \neq (1, \ldots, 1)^t$, so ist nach Induktionsannahme $w(x_1) = 2^{m-2}$ und damit auch die Anzahl der 1en in x_1 gleich 2^{m-2}. Im Fall $\lambda = 0$ ist die Aussage dann richtig. Im Fall $\lambda = 1$ folgt

$$w(x_1 + (1, \ldots, 1)^t) = 2^{m-2}$$

und damit ebenfalls die Aussage.

Ist $x_1 = (1, \ldots, 1)^t$, so muss nach Annahme $\lambda = 1$ gelten, womit die Aussage korrekt ist.

Zu 2.: Die Matrix $A := (x_1\, x_2\, \ldots\, x_{2^m})$ besitzt nach Konstruktion folgende Blockstruktur

$$\begin{array}{rcl} A & = & \begin{pmatrix} x'_1 & x'_2 & \cdots & x'_{2^{m-1}} & x'_1 & x'_2 & \cdots & x'_{2^{m-1}} \\ x'_1 & x'_2 & \cdots & x'_{2^{m-1}} & x'_1 + (1,\ldots,1)^t & x'_2 + (1,\ldots,1)^t & \cdots & x'_{2^{m-1}} + (1,\ldots,1)^t \end{pmatrix} \\ & =: & \begin{pmatrix} A' & A' \\ A' & B \end{pmatrix}. \end{array}$$

Nun gilt für ein beliebiges Wort $y \in \mathbb{F}_2^\ell$ die Gleichung

$$y + \widehat{(1, \ldots, 1)}^t = (-1)\widehat{y}. \tag{44}$$

Es folgt

$$H = \widehat{A} = \begin{pmatrix} \widehat{A'} & \widehat{A'} \\ \widehat{A'} & -\widehat{A'} \end{pmatrix},$$

womit H der Rekursionsformel für Hadamard-Matrizen vom Sylvestertyp genügt. Um die Behauptung zu beweisen, muss also nur noch die korrekte Initialisierung der Rekursion bei $m = 2$ geprüft werden: Die Kodewörter mit erster Komponente gleich 0 in $R(1,1)$ sind $(0,0)^t$ und $(0,1)^t$ was in dieser Reihenfolge zur Matrix

$$\widehat{A'} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

führt, wie gewünscht. □

Wir können jetzt eine effiziente ML-Dekodierung für die Kodes $R(1,m)$, $m \geq 2$, formulieren:

SATZ 3.42: *Die folgende Prozedur liefert eine ML-Dekodierung für den Kode $R(1,m)$, $m \geq 2$:*

1. ***Initialisierung:*** *Berechne die Sylvestermatrix $H \in \{-1,1\}^{2^m \times 2^m}$.*
2. ***Dekodierung:*** *Sei $y \in \mathbb{F}_2^{2^m}$ ein empfangenes Wort.*
   (a) *Berechne $\widehat{y}^t H =: (z_1, z_2, \ldots, z_{2^m}) \in \mathbb{Z}^{2^m}$ und bestimme k so, dass*
   $$|z_k| = \max(|z_i| : i = 1, \ldots, 2^m).$$
   (b) *Ist $z_k > 0$, dekodiere y zu $\phi^{-1}_{2^m \times 1}(h_k)$, wobei h_k die k-te Zeile von H ist.*
   (c) *Ist $z_k < 0$, dekodiere y zu $\phi^{-1}_{2^m \times 1}(h_k) + (1, \ldots, 1)^t$, wobei h_k die k-te Zeile von H ist.*

BEWEIS: Zunächst: Der angegebene Algorithmus liefert stets ein Ergebnis, da der Fall $z_k = 0$ nicht auftritt. Die Gleichung $\langle h_k, \widehat{y} \rangle = 0$ legt nämlich in der vorliegenden Situation den Vektor h_k bis auf ein Vielfaches von -1 eindeutig fest. Andererseits ist keine Spalte der Sylvestermatrix das -1-fache einer anderen.

Nach Feststellung 3.40 ist ein Kodewort x zu finden, für welches das Skalarprodukt $\langle \widehat{y}, \widehat{x} \rangle$ maximal wird. Nach Punkt 2 von Satz 3.41 stehen in den Zeilen von H die Vektoren $\widehat{x'}$, wobei x' alle Kodewörter durchläuft, deren erste Komponente gleich 0 ist.

Stets ist $(1, \ldots, 1)^t$ ein Kodewort wie man durch eine simple Induktion mit Hilfe von Gleichung (43) beweist. Addiert man zu allen Kodewörten, deren erste Komponente gleich 0 ist, das Kodewort $(1, \ldots, 1)^t$, so erhält man alle Kodewörter, deren erste Komponente gleich 1 ist.

Schließlich gilt die Gleichung (44).

Zusammengenommen ergibt sich, dass die Werte $\pm z_k$, $k = 1, \ldots, 2^m$, genau die Werte der Skalarprodukte $\langle \widehat{y}, \widehat{x} \rangle$ sind, wobei x *alle* Kodewörter durchläuft, woraus sich die Behauptung ergibt. □

Literatur

[C-T] T.M. Cover, J.A. Thomas, Elements of Information Theory, Wiley 2006.

[Lue] W. Lütkebohmert, Codierungstheorie, Vieweg 2003.

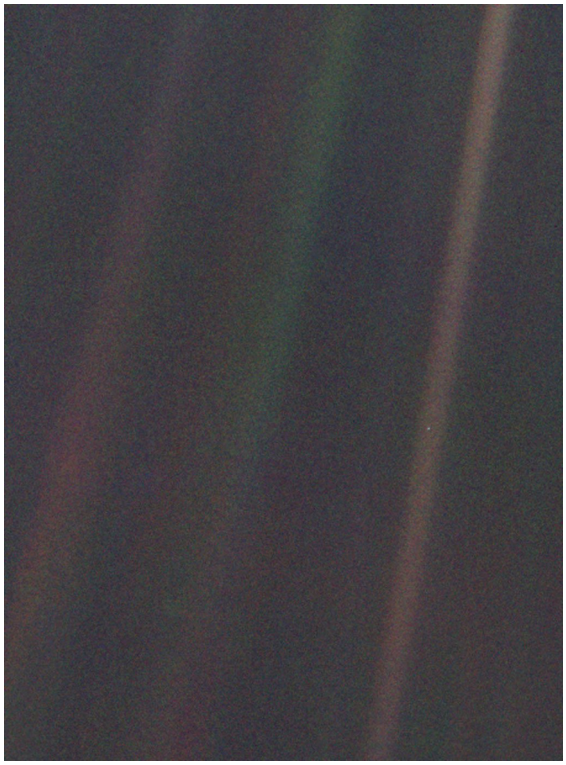
[Mac] F. J. MacWilliams, The Theory of Error-Correcting Codes, North Holland 1988.

[P-S] J. G. Proakis, M. Salehi, Communication Systems Engineering, Prentice Hall, 2002.

[Sag] C. Sagan, Pale Blue Dot: A Vision of the Human Future in Space, Random House USA Inc., 1997.

[Wei] S. Weinberg, Die ersten drei Minuten, Deutscher Taschenbuch Verlag GmbH & Co. KG., München 1980.

[vL] J.H. van Lint, Coding Theory, Lecture Notes in Mathematics 201, Springer Verlag 1971.



Pale Blue Dot – die Erde
Fotografie der Sonde Voyager 1 vom 14. Februar 1990
Entfernung Sonde – Erde: 6.4 Milliarden Kilometer / 5.9 Lichtstunden
(Courtesy NASA/JPL-Caltech)

≫We succeeded in taking that picture, and, if you look at it, you see a dot. That's here. That's home. That's us. On it, everyone you ever heard of, every human being who ever lived, lived out their lives. The aggregate of all our joys and sufferings, thousands of confident religions, ideologies and economic doctrines, every hunter and forager, every hero and coward, every creator and destroyer of civilizations, every king and peasant, every young couple in love, every hopeful child, every mother and father, every inventor and explorer, every teacher of morals, every corrupt politician, every superstar, every supreme leader, every saint and sinner in the history of our species, lived there on a mote of dust, suspended in a sunbeam.≪

Carl Sagan [8] [Sag]

[8] Carl Edward Sagan, amerikanischer Astronom, Astrophysiker, Exobiologe und Schriftsteller, 1934 – 1996