DHBW Mannheim
Studiengang Informatik

Codierungstheorie

Stand: August 2020

Autor:
Reinhold Hübl, Fakultät für Technik, DHBW Mannheim
e-mail:reinhold.huebl@dhbw-mannheim.de

©Fakultät für Technik DHBW Mannheim

Inhaltsverzeichnis

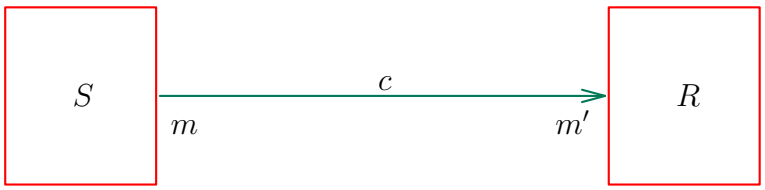
Einleitung

Die Codierungstheorie ist ein Teil der Informationstheorie und beschäftigt sich mit der korrekten Übermittlung von Daten. Ein Beispiel hierfür ist etwa die Speicherung und Übertragung von Musik auf digitalen Datenträgern, etwa auf einer CD. Das Problem hat dabei zwei Aspekte:

1. Musik liegt in Form eines akustischen Signals vor, also als Schallwelle. Hieraus ist eine speicherbares (diskretes) Datum zu erzeugen.

2. Bei der Darstellung von Musik durch Binärdaten entstehen sehr große Mengen an Daten. selbst bei optimaler Speicherung und Übertragung kann nicht sichergestellt werden, dass die Daten in der Tat im Originalzustand wieder ankommen. Trotzdem soll daraus die ursprüngliche Musik zurückgewonnen werden.

Die erste Fragestellung erweist sich als Problem der Integrationstheorie (Signaltheorie), und wird im ersten Abschnitt dieser Veranstaltung (kurz) skizziert. Die zweite Frage wiederum führt zu einem algebraischen Problem, mit dem wir uns in dieser Vorlesung schwerpunktmäßig beschäftigen werden.
Grundsätzlich geht es dabei um die Frage, wie Daten und Nachrichten m von einen Sender S an einen Empfänger R zuverlässig übertragen werden können.
Vorausgesetzt wird dabei, dass der Übertragungskanal c gegeben ist, und das damit zu rechnen ist, dass bei der Übertragung über diesen Kanal Fehler auftreten, sodass also der Empfänger eine Nachricht m' erhält, die nicht identisch ist mit der gesendeten Nachricht m.



Codierungstheorie beschäftigt sich nun mit der Frage, wie aus m' der *Inhalt* von m rekonstruiert werden kann.

Kapitel 1

Signaltheorie und Abtasttheorem

1.1 Kontinuierliche und diskrete Signale

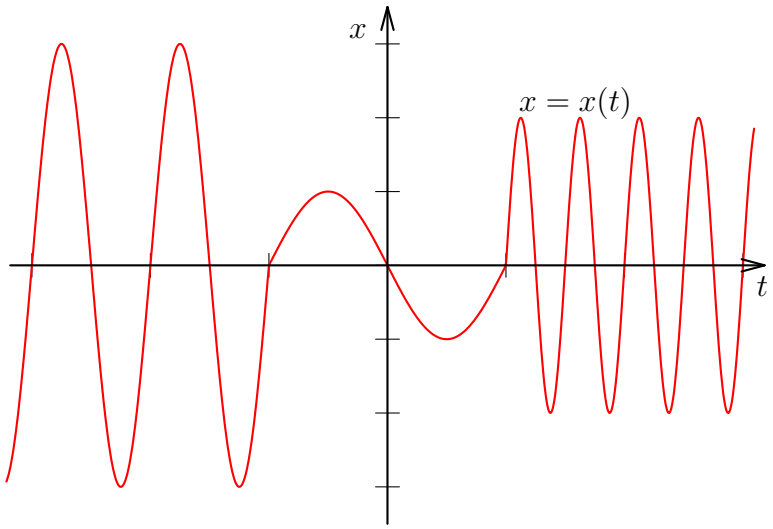
In diesem Abschnitt geht es um die Frage, wie ein kontinuierliches (akustisches) Signal in diskrete Einheiten zu zerlegen ist, damit aus diesen diskreten Werten das ursprüngliche Signal zurückgewonnen werden kann. Die Antwort auf diese Frage liefert das Shannonsche Abtasttheorem.
Das Shannon Abtasttheorem ist ein Resultat der Signaltheorie, das sich mit Beziehungen zwischen kontinuierlichen und diskreten Signalen beschäftigt.
Unter einem **Signal** (Zeitsignal) x versteht man einen physikalische Größe (ohne Einheit) die sich als Funktion der Zeit darstellen lässt, also $x = x(t)$. Beispiele hierfür sind etwa Strom, Feldstärke, Schallwellen, Temperatur etc. Sie liegen in der Regel in Form eines analogen Spannungsverlaufes vor, also als zeit– und wertkontinuierliche Funktion.
Ein zeitkontinuierliches Signal ist also aus mathematischer Sicht nichts anderes als eine Funktion

$$x : \mathbb{R} \longrightarrow \mathbb{R}$$

Ein zeit- und wertkontinuierliches Signal ist eine stetige Funktion

$$x : \mathbb{R} \longrightarrow \mathbb{R}$$

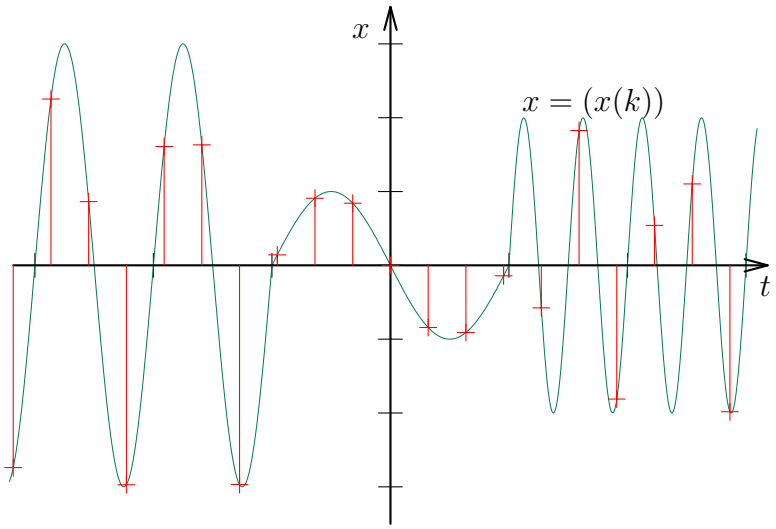
Beispiel 1.1.1. Ein zeit- und wertkontinuierliches Signal kann die folgende Form haben



Im Rahmen der digitalen Signalverarbeitung lassen sich solche kontinuierlichen Funktionen jedoch nicht speichern und verarbeiten. Hierfür ist es erforderlich, mit einzelnen Signalwerten zu arbeiten. Anstelle der Funktion $x = x(t)$ werden also nur ausgewählte Funktionswerte $x(t_0), x(t_1), \ldots$ behandelt, das Signal $x(t)$ wird also zu diversen Zeitpunkten t_k gemessen ("abgetastet"). Dabei wählt man in der Regel konstante Zeitabstände, so dass also $t_{k+1} = t_k + \Delta_t$ mit einem festen Zeitwert Δ_t, und wir schreiben auch

$$x(k) = x(t_k) = x(t_0 + k \cdot \Delta_t) \qquad (k \in \mathbb{Z})$$

Auf diese Art und Weise haben wir also aus dem analogen Signal $x(t)$ ein diskretes Signal $x(k), k \in \mathbb{Z}$ gewonnen. Übrig bleibt ein "gekämmtes Signal"



Wir wollen uns nun mit der folgenden Problemstellung beschäftigen

Problem 1. Unter welchen Voraussetzungen (an das Signal und an die Abtaststellen) kann das Signal $x(t)$ vollständig (also ohne Informationsverlust) aus seiner Diskretisierung $x(k), k \in \mathbb{Z}$ wiederhergestellt werden.

Das ist ganz offensichtlich eine Fragestellung, die von der Art des Signales $x(t)$ und von der Häufigkeit der Abtastung, also von Δ_t abhängt.

1.2 Fouriertransformation

Ein entscheidendes Hilfsmittel bei der Untersuchung von Signalen ist die Fouriertransformation. Dazu betrachten wir ein (analoges) Signal $x(t)$.

Definition 1.2.1. Die Funktion

$$\widehat{x}(\omega) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} x(t) \cdot \cos(\omega t) dt \; - \; \mathrm{i} \cdot \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{+\infty} x(t) \cdot \sin(\omega t) dt$$

heißt die **Fouriertransformierte** oder das **Spektrum** von $x(t)$ (falls dieser Ausdruck existiert).
Wir schreiben auch $X(\omega)$ oder $\mathscr{F}(x)(\omega)$ für $\widehat{x}(\omega)$.

Das uneigentliche Integral ist dabei als Cauchyscher Hauptwert zu sehen, also also

$$\widehat{x}(\omega) := \lim_{R \to \infty} \left(\frac{1}{\sqrt{2\pi}} \int_{-R}^{+R} x(t) \cdot \cos(\omega t) dt \; - \; \mathrm{i} \cdot \frac{1}{\sqrt{2\pi}} \int_{-R}^{+R} x(t) \cdot \sin(\omega t) dt \right)$$

Die Fouriertransformation ist also in der Regel eine Funktion mit Werten in den komplexen Zahlen. Sie ist nicht immer definiert. Das Signal $x(t) = t^2$ etwa besitzt keine Fouriertransformation. Eine hinreichende Bedingung für die Existenz der Fouriertransformation ist, dass $x(t)$ integrierbar ist mit

$$\int_{-\infty}^{\infty} |x(t)| \, dt < \infty$$

Speziell gilt das also, wenn $x(t)$ stetig ist mit $x(t) = 0$ für alle t mit $|t| \geq T_0$ für ein T_0.

Die Fouriertransformation kann auch mit der (komplexen) Exponentialfunktion beschrieben werden,

$$\widehat{x}(\omega) = \frac{1}{\sqrt{2\pi}} \cdot \int_{-\infty}^{\infty} x(t) \cdot e^{-\mathrm{i}\omega t} dt$$

In dieser Form ist sie formal sehr ähnlich zur *Laplace–Transformation*

$$\mathscr{L}(x)(\omega) = \int_{-\infty}^{\infty} x(t) \cdot e^{-\omega t} dt$$

die Ihnen ja bekannt ist.

Bemerkung 1.2.1. Die Fouriertransformierte hat viele interessante Eigenschaften:

1. Ist $x(t)$ (reell) und gerade, so ist $\widehat{x}(\omega)$ gerade und
$$\widehat{x}(\omega) = \frac{2}{\sqrt{2\pi}} \cdot \int_{0}^{\infty} x(t) \cdot \cos(\omega t) dt.$$

2. Ist $x(t)$ (reell) und ungerade, so ist $\widehat{x}(\omega)$ ungerade und
$$\widehat{x}(\omega) = -\frac{2 \cdot \mathrm{i}}{\sqrt{2\pi}} \cdot \int_{0}^{\infty} x(t) \cdot \sin(\omega t) dt.$$

3. Ist $\tau_a x(t)$ die Verschiebung des Signals $x(t)$ um a, also $\tau_a x(t) = x(t-a)$, so ist
$$\widehat{\tau_a x}(\omega) = \widehat{x}(\omega) \cdot e^{-\mathrm{i}\, a\, \omega}.$$

4. Bezeichnet $x_1 * x_2$ das Faltungsprodukt zweier Signale x_1 und x_2, also
$$(x_1 * x_2)(t) = \int_{-\infty}^{\infty} f(s) \cdot g(t-s)\, ds$$
so ist
$$\widehat{x_1 * x_2}(\omega) = \sqrt{2\pi} \cdot \widehat{x_1}(\omega) \cdot \widehat{x_2}(\omega)$$
(falls alle Fouriertransformierten existieren und mindestens ein Signal global beschränkt ist).

5. Ist das Signal $x(t)$ differenzierbar und existiert auch die Fouriertransformierte von $x'(t)$, so gilt

$$\widehat{x'}(\omega) = \mathrm{i} \cdot \omega \cdot \widehat{x}(\omega)$$

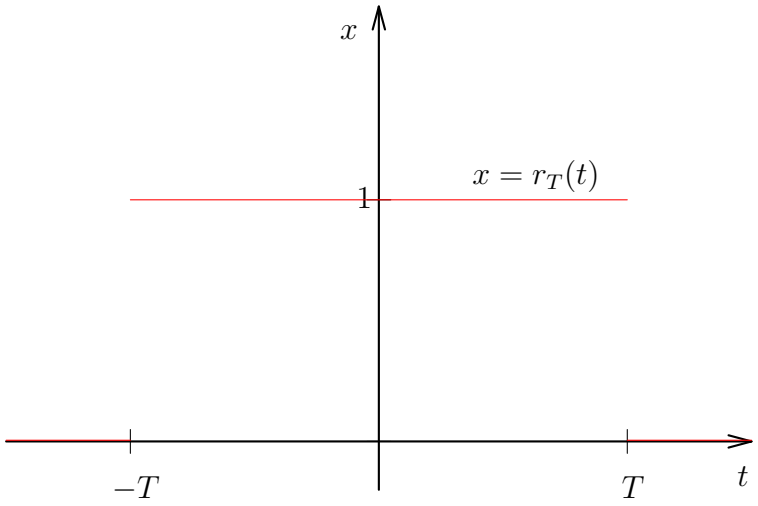
6. Existiert für $-\mathrm{i} \cdot t \cdot x(t)$ die Fouriertransformierte, so gilt

$$\widehat{(-\mathrm{i} \cdot t \cdot x)}(\omega) = \widehat{x}'(\omega).$$

Beispiel 1.2.1. Der Rechtecksimpuls $r_T(t)$ mit

$$r_T(t) = \begin{cases} 1 & \text{für } t \in [-T, T] \\ 0 & \text{sonst} \end{cases}$$

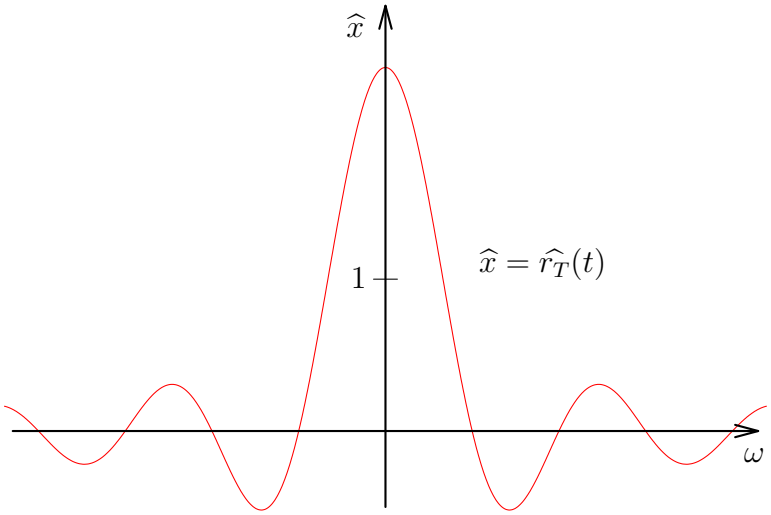
der durch folgendes Bild dargestellt wird



hat Fouriertransformierte

$$\widehat{r_T}(\omega) = \frac{2T}{\sqrt{2\pi}} \frac{\sin(\omega T)}{\omega T}$$

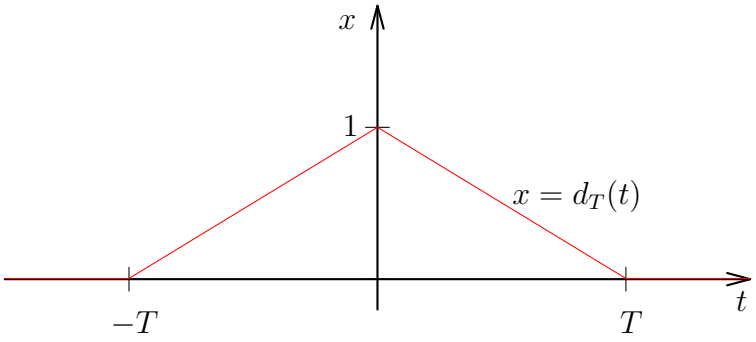
also graphisch



Beispiel 1.2.2. Der Dreiecksimpuls $d_T(t)$ mit

$$d_T(t) = \begin{cases} \frac{1}{T}(T+t) & \text{für } t \in [-T, 0] \\ \frac{1}{T}(T-t) & \text{für } t \in [0, T] \\ 0 & \text{sonst} \end{cases}$$

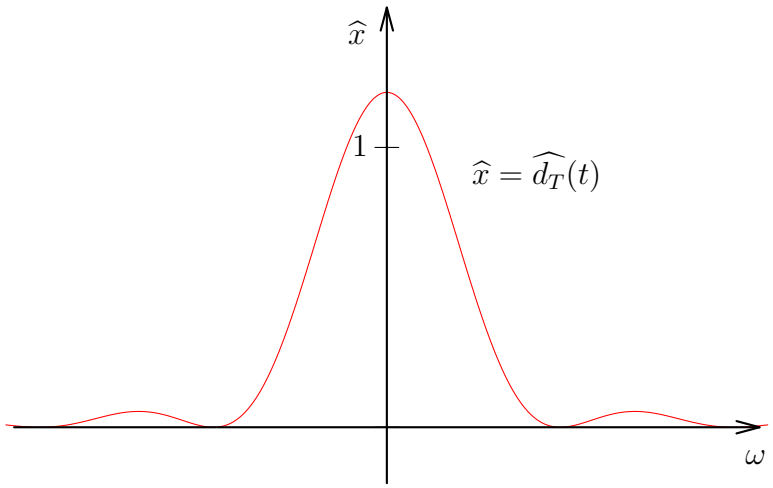
beschrieben durch



hat Fouriertransformierte

$$\widehat{d_T}(\omega) = \frac{4}{T\omega^2\sqrt{2\pi}} \sin^2\left(\frac{\omega T}{2}\right)$$

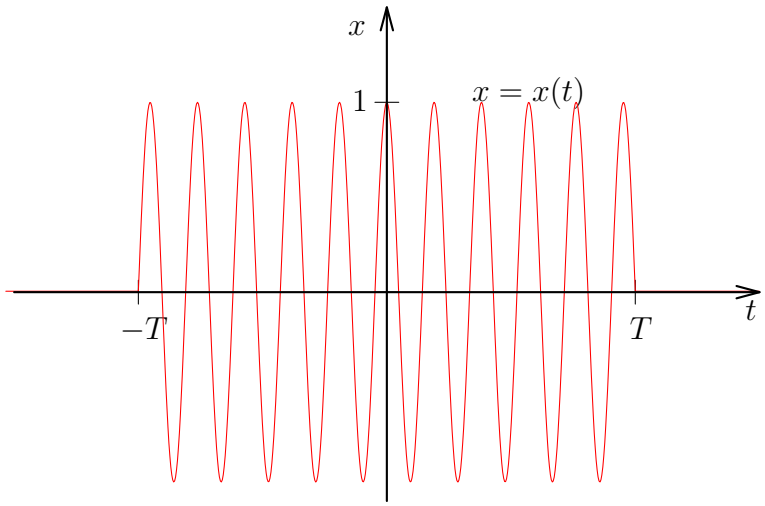
also graphisch



Beispiel 1.2.3. Die Modulation $f(t)$ des Kosinus durch eine Rechtecksfunktion, gegeben durch

$$f(t) = r_T(t) \cdot \cos(\omega_0 t)$$

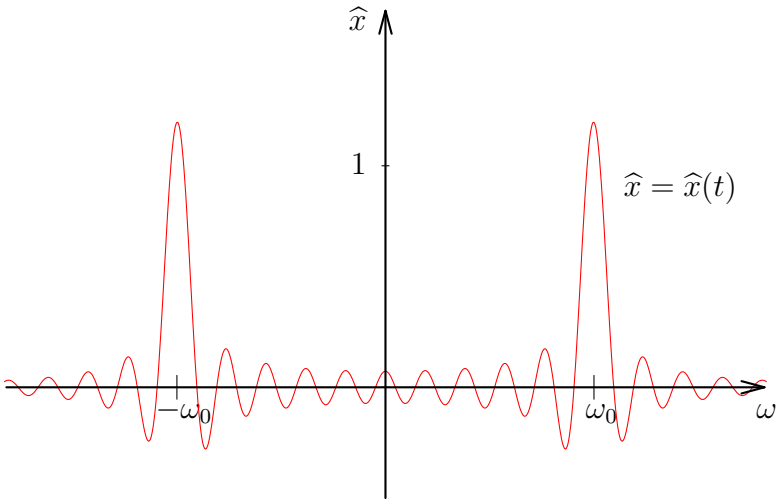
beschrieben durch



hat Fouriertransformierte

$$\widehat{f}(\omega) = \frac{1}{\sqrt{2\pi}} \left(\frac{\sin\left(T(\omega + \omega_0)\right)}{\omega + \omega_0} + \frac{\sin\left(T(\omega - \omega_0)\right)}{\omega - \omega_0} \right)$$

also graphisch



Beispiel 1.2.4. Der **Diracimpuls** $\delta(t)$ ist keine Funktion sondern eine Distribution; er ist indirekt definiert durch die Bedingung, dass

$$\int_{-\infty}^{\infty} x(t) \cdot \delta(t) dt = x(0)$$

für jedes (integrierbare) Signal $x(t)$. Seine Fouriertransformation ist

$$\widehat{\delta}(\omega) = \frac{1}{\sqrt{2\pi}}$$

Beispiel 1.2.5. Der Kosinusimpuls $\cos(\omega_0 t)$ hat Fouriertransformierte

$$\widehat{\cos}(\omega) = \sqrt{\frac{\pi}{2}} \cdot (\delta(\omega - \omega_0) + \delta(\omega + \omega_0))$$

Der Sinusimpuls $\sin(\omega_0 t)$ hat Foruiertransformierte

$$\widehat{\sin}(\omega) = \sqrt{\frac{\pi}{2\mathrm{i}}} \cdot (\delta(\omega - \omega_0) - \delta(\omega + \omega_0))$$

Die für uns entscheidende Eigenschaft der Fouriertransformation ist, dass sich in vielen Fällen aus der Fouriertransformierten $\widehat{x}(\omega)$ eines Signals $x(t)$ das Signal selbst rekonstruieren lässt:

Satz 1.2.1 (Umkehrformel)**.** *Ist $x(t)$ ein stückweise stetiges Signal mit $\int_{-\infty}^{\infty} |x(t)|^2 \, dt < \infty$, so existiert die Fouriertransformierte $\widehat{x}(\omega)$ und es gilt*

$$x(t) = \frac{1}{\sqrt{2\pi}} \left(\int_{-\infty}^{\infty} \widehat{x}(\omega) \cos(\omega t) d\omega \; + \; \mathrm{i} \cdot \int_{-\infty}^{\infty} \widehat{x}(\omega) \cos(\omega t) d\omega \right)$$

an allen Stetigkeitsstellen von $x(t)$.

Bemerkung 1.2.2. Die Gleichheit gilt also im allgemeinen nicht punktweise sondern nur fast überall, also bis auf eine Nullmenge. Ist das Signal stetig, so gilt sie auch punktweise.

1.3 Fourierreihen

In der Analysis haben Sie bereits Reihendarstellungen von Funktionen kennengelernt und gesehen, dass sich einige Funktionen durch ihre Taylorreihen beschreiben und - in gewissen Abschnitten - recht gut durch ihre Taylorpolynome (hinreichend hoher Ordnung) approximieren lassen. Schwierig ist hierbei aber immer die Behandlung von periodischen Funktionen. Jedes (nicht–triviale) Polynome strebt gegen ∞ oder $-\infty$, wenn x gegen ∞ geht, aber periodische Funktionen sind immer beschränkt. Daher können diese allenfalls in einem kleinen Bereich gut durch ihre Taylorpolynome approximiert werden.
Eine Funktione $f : \mathbb{R} \longrightarrow \mathbb{R}$ heißt bekanntlich **periodisch** mit Periode $p > 0$, wenn

$$f(x + p) = f(x) \quad \text{für alle } x \in \mathbb{R}$$

Dann gilt natürlich auch

$$f(x) = f(x + p) = f(x + 2p) = f(x + 3p) = \cdots$$

so dass also f auch periodisch mit Periode $n \cdot p$ für alle $n \in \mathbb{N}$, $n > 0$ ist. Das kleinste $p > 0$ für das f periodisch von der Periode p ist, heißt (falls es denn exisitert) **primitive Periode** von f.

Beispiel 1.3.1. Die Funktionen $f, g : \mathbb{R} \longrightarrow \mathbb{R}$ mit

$$f(x) = \cos(x), \quad g(x) = \sin(x)$$

sind periodisch mit Periode 2π, und 2π ist auch die primitive Periode von f und g.

Beispiel 1.3.2. Wir betrachten ein $\omega > 0$ und Konstanten $A, b \in \mathbb{R}$ mit $A \neq 0$. Die Funktion $f : \mathbb{R} \longrightarrow \mathbb{R}$ mit

$$f(x) = A \cdot \cos(\omega \cdot x + b) \quad \text{für alle } x \in \mathbb{R}$$

ist periodisch mit Periode $\frac{2\pi}{\omega}$, denn

$$\begin{aligned} f\left(x + \tfrac{2\pi}{\omega}\right) &= A \cdot \cos\left(\omega \cdot \left(x + \tfrac{2\pi}{\omega}\right) + b\right) \\ &= A \cdot \cos(\omega \cdot x + b + 2\pi) \\ &= A \cdot \cos(\omega \cdot x + b) \end{aligned}$$

Die Funktionen $\sin(x)$ und $\cos(x)$ sind die bekanntesten periodischen Funktionen. Wie wir sehen werden, sind sie in gewisser Weise auch die Grundbausteine aller periodischen Funktionen. Hierzu benutzen wir eine Reduktion, die es uns erlaubt, uns auf das Studium von 2π–periodischen Funktionen zu beschränken.

Bemerkung 1.3.1. Ist f periodische von der Periode $p > 0$, so ist g mit

$$g(x) = f\left(\frac{p \cdot x}{2\pi}\right) \quad \text{für alle } x \in \mathbb{R}$$

periodisch mit der Periode 2π.
Ist umgekehrt $g(x)$ eine 2π–periodische Funktione, so ist f mit

$$f(x) = g\left(\frac{2\pi \cdot x}{p}\right) \quad \text{für alle } x \in \mathbb{R}$$

eine p–periodische Funktion. Über diese Transformation entsprechen sich die p–periodischen und die 2π–periodischen Funktionen auf eindeutige Weise.
In der Tat gilt

$$g(x + 2\pi) = f\left(\frac{p \cdot x + p \cdot 2\pi}{2\pi}\right) = f\left(\frac{p \cdot x}{2\pi} + p\right)) = f\left(\frac{p \cdot x}{2\pi}\right) = g(x)$$

Wir wollen also jetzt immer annehmen, dass f periodisch von der Periode 2π ist. Zunächst geben wir ein Verfahren an, mit dem 2π–periodische Funktionen konstruiert werden können.

Hilfssatz 1.3.1. *Sind* $\sum_{n=1}^{\infty} a_n$ *und* $\sum_{n=1}^{\infty} b_n$ *zwei absolut konvergente Reihen, und ist* $a_0 \in \mathbb{R}$*, so ist auch die Reihe*

$$\frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cos(nx) + b_n \sin(nx)\right)$$

absolut konvergent für jedes $x \in \mathbb{R}$ und definiert eine 2π–periodische, stetige Funktion

$$f : \mathbb{R} \longrightarrow \mathbb{R}, \quad x \longmapsto \frac{a_0}{2} + \sum_{n=1}^{\infty} (a_n \cos(nx) + b_n \sin(nx))$$

Beweis: Zum Nachweis der absoluten Konvergenz wenden wir das Majorantenkriterium für Reihen an und nutzen aus, dass

$$|\cos(nx)| \leq 1, \quad |\sin(nx)| \leq 1 \qquad \forall x \in \mathbb{R}$$

Damit gilt für jedes $N \in \mathbb{N}$ und jedes $x \in \mathbb{R}$:

$$\begin{aligned} &|\frac{a_0}{2} + \sum_{n=1}^{N} (a_n \cos(nx) + b_n \sin(nx))\,| \\ &\qquad \leq |\frac{a_0}{2}| + \sum_{n=1}^{N} \left(|a_n| \cdot |\cos(nx)| \; + \sum_{n=1}^{N} |b_n| \cdot |\sin(nx)| \right) \\ &\qquad \leq |\frac{a_0}{2}| + \sum_{n=1}^{N} |a_n| \; + \sum_{n=1}^{N} |b_n| \end{aligned}$$

und daraus folgt nach dem Majorantenkriterium und der Voraussetzung die Behauptung über die Konvergenz.
Zum Nachweis der Stetigkeit können wir wie folgt vorgehen:
Wir fixieren ein $\varepsilon > 0$ und ein $x_0 \in \mathbb{R}$. Nach Voraussetzung gibt es dann ein $N \in \mathbb{N}$ mit

$$\sum_{n=N+1}^{\infty} |a_n| \; < \frac{\varepsilon}{8}, \quad \sum_{n=N+1}^{\infty} |b_n| \; < \frac{\varepsilon}{8}$$

Betrachten wir die Partialsumme

$$f_N(x) := \frac{a_0}{2} + \sum_{n=1}^{N} (a_n \cos(nx) + b_n \sin(nx))$$

so ist diese sicherlich stetig (als endliche Summe stetiger Funktionen). Daher gibt es ein $\delta > 0$, so dass für alle x mit $|x - x_0| \; < \delta$ gilt

$$|f_N(x) - f_N(x_0)| \; < \frac{\varepsilon}{2}$$

Aus der absoluten Konvergenz erhalten wir nun

$$\begin{aligned}
|f(x) - f(x_0)| &= |f_N(x) - f_N(x_0) + \\
&\quad \left(\sum_{n=N+1}^{\infty} (a_n(\cos(nx) - \cos(nx_0)) \right. \\
&\quad \left. \left. + b_n(\sin(nx) - \sin(nx_0)) \right) \right) \Bigg| \\
&\leq |f_N(x) - f_N(x_0)| \\
&\quad + \left| \sum_{n=N+1}^{\infty} (a_n(\cos(nx) - \cos(nx_0)) \right. \\
&\quad \left. + b_n(\sin(nx) - \sin(nx_0)) \right) \Bigg| \\
&\leq |f_N(x) - f_N(x_0)| \\
&\quad + \sum_{N+1}^{\infty} (|a_n| \cdot |\cos(nx) - \cos(nx_0)| \\
&\quad + |b_n| \cdot |\sin(nx) - \sin(nx_0)|) | \\
&\leq |f_N(x) - f_N(x_0)| \\
&\quad + \sum_{N+1}^{\infty} (|a_n| \cdot (|\cos(nx)| + |\cos(nx_0)|) \\
&\quad + |b_n| \cdot (|\sin(nx)| + |\sin(nx_0)|)) \\
&\leq |f_N(x) - f_N(x_0)| + \sum_{N+1}^{\infty} (|a_n| \cdot 2 + |b_n| \cdot 2) \\
&< \varepsilon
\end{aligned}$$

und die Stetigkeit ist gezeigt.

Wir betrachten nun eine $2T_0$–periodische Funktion $f : \mathbb{R} \longrightarrow \mathbb{R}$ und nehmen an, dass f auf $[0, 2T_0]$ Riemann–integrierbar ist, also dass

$$\int_0^{2T_0} f(x)dx$$

existiert. Das ist ja bekanntlich immer dann der Fall, wenn f stückweise stetig ist, also in allen für uns interessanten Fällen.

Definition 1.3.1. Die Zahlen

$$\begin{aligned} a_0 &= \tfrac{1}{T_0} \cdot \int_0^{2T_0} f(x)\,dx \\ a_n &= \tfrac{1}{T_0} \cdot \int_0^{2T_0} f(x) \cdot \cos\left(n \cdot \tfrac{\pi}{T_0} \cdot x\right)\,dx \qquad (n \geq 1) \\ b_n &= \tfrac{1}{T_0} \cdot \int_0^{2T_0} f(x) \cdot \sin\left(n \cdot \tfrac{\pi}{T_0} \cdot x\right)\,dx \qquad (n \geq 1) \end{aligned}$$

heißen die **Fourier–Koeffizienten** der Funktion f, und

$$\mathscr{F}_f(x) := \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cdot \cos\left(n \cdot \frac{\pi}{T_0} \cdot x\right) + b_n \cdot \sin\left(n \cdot \frac{\pi}{T_0} \cdot x\right)\right)$$

heißt **Fourier–Reihe** der Funktion f.

Da aufgrund von Bemerkung 1.3.1 jede periodische Funktion auf eine 2π periodische Funktione zurückgeführt werden kann, wollen wir nun speziell eine 2π–periodische Funktion $f : \mathbb{R} \longrightarrow \mathbb{R}$ betrachten. Dann erhalten wir folgende vereinfachte Darstellung der Fourierkoeffizienten und der Fouriereihe

$$\begin{aligned} a_0 &= \tfrac{1}{\pi} \cdot \int_0^{2\pi} f(x)\,dx \\ a_n &= \tfrac{1}{\pi} \cdot \int_0^{2\pi} f(x) \cdot \cos(nx)\,dx \qquad (n \geq 1) \\ b_n &= \tfrac{1}{\pi} \cdot \int_0^{2\pi} f(x) \cdot \sin(nx)\,dx \qquad (n \geq 1) \end{aligned}$$

sind die Fourierkoeffizienten der Funktion f, und

$$\mathscr{F}_f(x) := \frac{a_0}{2} + \sum_{n=1}^{\infty} \left(a_n \cdot \cos(nx) + b_n \cdot \sin(nx)\right)$$

ist die Fourierreihe von f.

Bemerkung 1.3.2. Da f eine 2π–periodische Funktion ist, können wir die Fourierkoeffizienten über jedem Intervall der Länge 2π berechnen, und es gilt

$$\begin{aligned} a_0 &= \tfrac{1}{\pi} \cdot \int_{x_0}^{x_0+2\pi} f(x)\,dx \\ a_n &= \tfrac{1}{\pi} \cdot \int_{x_0}^{x_0+2\pi} f(x) \cdot \cos(nx)\,dx \qquad (n \geq 1) \\ b_n &= \tfrac{1}{\pi} \cdot \int_{x_0}^{x_0+2\pi} f(x) \cdot \sin(nx)\,dx \qquad (n \geq 1) \end{aligned}$$

für jedes $x_0 \in \mathbb{R}$.

Zur weiteren Untersuchung der Fourierreihen betrachten wir deren Partialsummen

$$\mathscr{F}_{f,N}(x) := \frac{a_0}{2} + \sum_{n=1}^{N} (a_n \cdot \cos(nx) + b_n \cdot \sin(nx))$$

die sogenannten **Fourier–Polynome** von f.

Satz 1.3.2. *Ist $f : \mathbb{R} \longrightarrow \mathbb{R}$ eine stetig differenzierbare 2π–periodische Funktion, so gilt*

$$f(x) = \mathscr{F}_f(x) \qquad \text{für alle } x \in \mathbb{R}$$

und die Fourier–Reihe konvergiert gleichmäßig gegen f, d.h. für jedes $\varepsilon > 0$ gibt es ein $N_0 \in \mathbb{N}$, so dass für alle $N \geq N_0$ und alle $x \in \mathbb{R}$ gilt

$$|f(x) - \mathscr{F}_{f,N}(x)| < \varepsilon$$

Auf den Beweis dieser Aussage wollen wir verzichten da die hierfür benötigte Integrationstheorie unseren Rahmen sprengen würde.
Für beliebige 2π–periodische Funktionen gilt die starke Konvergenzaussage aus Satz 1.3.2 nicht mehr, wir erhalten aber immer noch folgendes Resultat.

Satz 1.3.3. *Ist $f : \mathbb{R} \longrightarrow \mathbb{R}$ eine 2π–periodische und auf $[0, 2\pi]$ Riemann–integrierbare Funktion, so konvergiert die Fourier–Reihe von f im quadratischen Mittel gegen f, d.h. für jedes $\varepsilon > 0$ gibt es ein $N_0 \in \mathbb{N}$, so dass für alle $N \geq N_0$ gilt*

$$\frac{1}{2\pi} \cdot \int_0^{2\pi} (f(x) - \mathscr{F}_{f,N}(x))^2 \, dx < \varepsilon$$

Einen Beweis dieser Aussage finden Sie etwa bei O. Forster, *Analysis I*, § 23, Satz 2.

Bemerkung 1.3.3. Für periodische Funktionen spielen die trigonometrischen Funktionen $\sin(nx)$ und $\cos(nx)$ also eine ähnliche Rolle wie die Polynome $1, x, x^2, \ldots$ bei der Approximation beliebiger Funktionen durch Taylorpolynome.

Bemerkung 1.3.4. Mit Hilfe von Bemerkung 1.3.1 können wir für eine beliebige p–periodische Funktion die Fourier–Reihe ermitteln. ist Die Periode also p (anstelle von 2π) so hat die Fourierreihe die Gestalt

$$\frac{a_0}{2} + \sum_{n=1}^{N} \left(a_n \cos\left(\frac{2\pi}{p} nx\right) + b_n \sin\left(\frac{2\pi}{p} \cdot nx\right)\right)$$

wobei in diesem Fall

$$\begin{aligned} a_0 &= \tfrac{2}{p} \cdot \int_0^p f(x)\, dx \\ a_n &= \tfrac{2}{p} \cdot \int_0^p f(x) \cdot \cos\left(\tfrac{2\pi}{p} \cdot nx\right)\, dx \\ b_n &= \tfrac{2}{p} \cdot \int_0^p f(x) \cdot \sin\left(\tfrac{2\pi}{p} \cdot nx\right)\, dx \end{aligned}$$

Beachten Sie, dass diese Definition mit der aus Definition 1.3.1 übereinstimmt. Die Periodenlänge, die hier mit p bezeichnet wird, war dort $2T_0$. Da sich beide Bezeichnungen in der Literatur finden, werden hier auch die Definitonen für beide Formulierungen gegeben.

Für die Berechnung der Fourier–Koeffizienten ist folgende Tabelle von Integralen nützlich, die wir unmittelbar durch Nachrechnen erhalten:

Regel 1.3.4. *Es gilt*

1. $\int_0^{2\pi} \cos(nx)dx = \left[\frac{1}{n} \cdot \sin(nx)\right]_0^{2\pi} = 0.$
2. $\int_0^{2\pi} \sin(nx)dx = \left[\frac{-1}{n} cdot \cos(nx)\right]_0^{2\pi} = 0.$
3. $\int_0^{2\pi} \cos(nx)^2dx = \left[\frac{x}{2} + \frac{1}{4n} \cdot \sin(2nx)\right]_0^{2\pi} = \pi.$
4. $\int_0^{2\pi} \sin(nx)^2dx = \left[\frac{x}{2} - \frac{1}{4n} \cdot \sin(2nx)\right]_0^{2\pi} = \pi.$
5. $\int_0^{2\pi} \sin(nx) \cdot \cos(nx)dx = \left[\frac{1}{2n} \cdot \sin^2(nx)\right]_0^{2\pi} = 0.$

6. Für $n \neq m$ gilt

$$\begin{aligned}
\int_0^{2\pi} \cos(nx) \cdot \cos(mx)dx &= \left[\tfrac{\sin((n-m)x)}{2(n-m)} + \tfrac{sin((n+m)x)}{2(n+m)}\right]_0^{2\pi} = 0 \\
\int_0^{2\pi} \sin(nx) \cdot \cos(mx)dx &= \left[-\tfrac{\cos((n-m)x)}{2(n-m)} - \tfrac{cos((n+m)x)}{2(n+m)}\right]_0^{2\pi} = 0 \\
\int_0^{2\pi} \sin(nx) \cdot \sin(mx)dx &= \left[\tfrac{\sin((n-m)x)}{2(n-m)} - \tfrac{sin((n+m)x)}{2(n+m)}\right]_0^{2\pi} = 0
\end{aligned}$$

Bemerkung 1.3.5. Die Aussagen von Regel 1.3.4 können als Orthogonalitätsbeziehung der trigonometrischen Polynome $\cos(nx), \sin(nx)$ interpretiert werden.

Beispiel 1.3.3. Wir betrachten die Rechtecksschwingung $f : \mathbb{R} \longrightarrow \mathbb{R}$, die auf jedem Intervall $[\,2n\pi,\, 2(n+1)\pi\,[$ $(n \in \mathbb{Z})$ definiert ist durch

$$f(x) = \begin{cases} 1 & \text{für } 2n\pi \leq x < (2n+1)\pi \\ -1 & \text{für } (2n+1)\pi \leq x < 2(n+1)\pi \end{cases}$$

Das ist offensichtlich eine 2π–periodische Funktion und es gilt

$$\begin{aligned}
a_n &= \tfrac{1}{\pi} \cdot \left(\int_0^{\pi} \cos(nx)dx + \int_{\pi}^{2\pi} (-\cos(nx))\, dx \right) \\
&= \tfrac{1}{\pi} \cdot \left(\left[\tfrac{\sin(nx)}{n}\right]_0^{\pi} + \left[-\tfrac{\sin(nx)}{n}\right]_{\pi}^{2\pi} \right) \\
&= 0
\end{aligned}$$

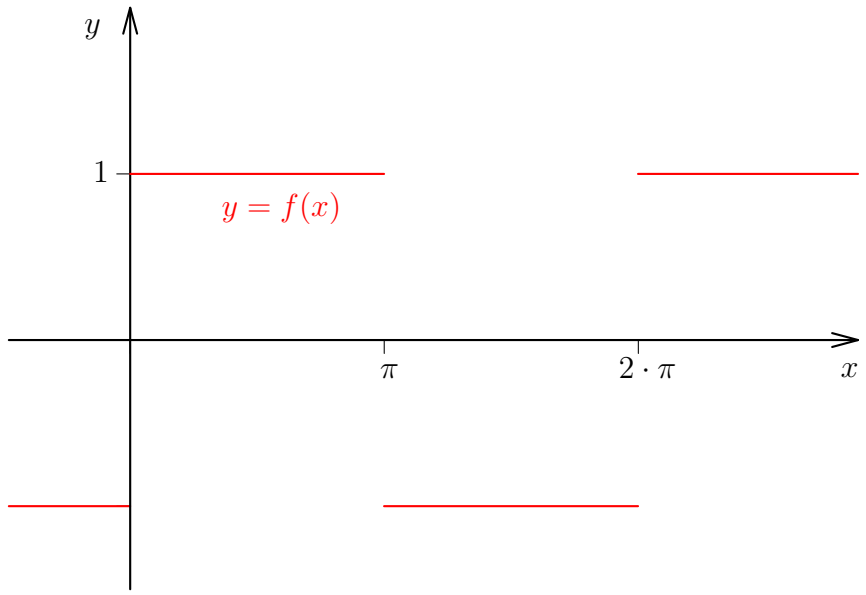
und

$$\begin{aligned}
b_n &= \tfrac{1}{\pi} \cdot \left(\int_0^{\pi} \sin(nx)dx + \int_{\pi}^{2\pi} -\sin(nx)dx \right) \\
&= \tfrac{1}{\pi} \cdot \left(\left[-\tfrac{\cos(nx)}{n}\right]_0^{\pi} + \left[\tfrac{\cos(nx)}{n}\right]_{\pi}^{2\pi} \right) \\
&= \tfrac{2}{n\cdot\pi} \cdot (1 - \cos(n\pi)) \\
&= \begin{cases} 0 & \text{falls } n \text{ gerade} \\ \frac{4}{n\cdot\pi} & \text{falls } n \text{ ungerade} \end{cases}
\end{aligned}$$

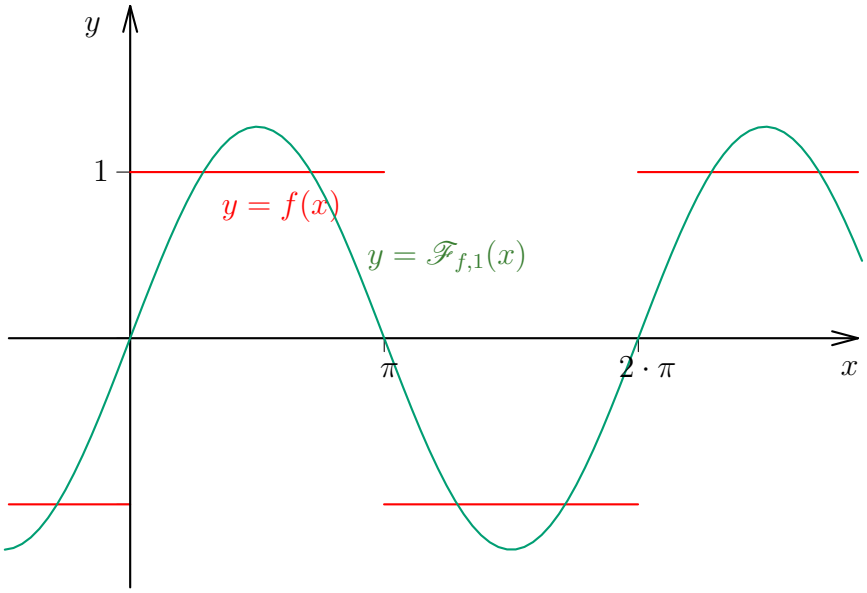
und damit hat f die Fourierreihe

$$\mathscr{F}_f(x) = \frac{4}{\pi} \cdot \sum_{n=0}^{\infty} \frac{\sin((2n+1)x)}{2n+1}$$

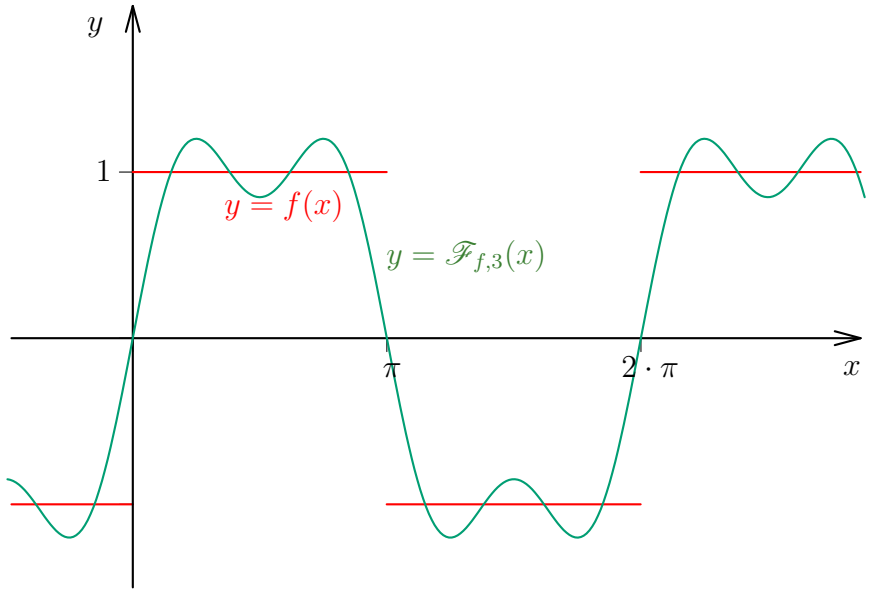
Die Rechtecksschwingung selbst hat den folgenden Graphen



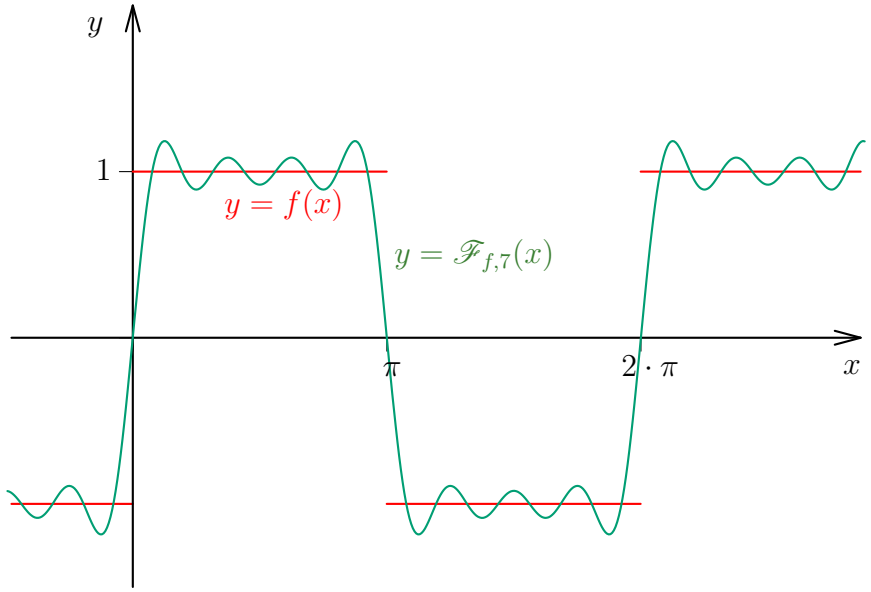
Aus der Fourierreihe erhalten wir eine erste Näherung durch das erste Fourierpolynom $\mathscr{F}_{f,1}(x) = \frac{\pi}{4} \cdot \sin(x)$:



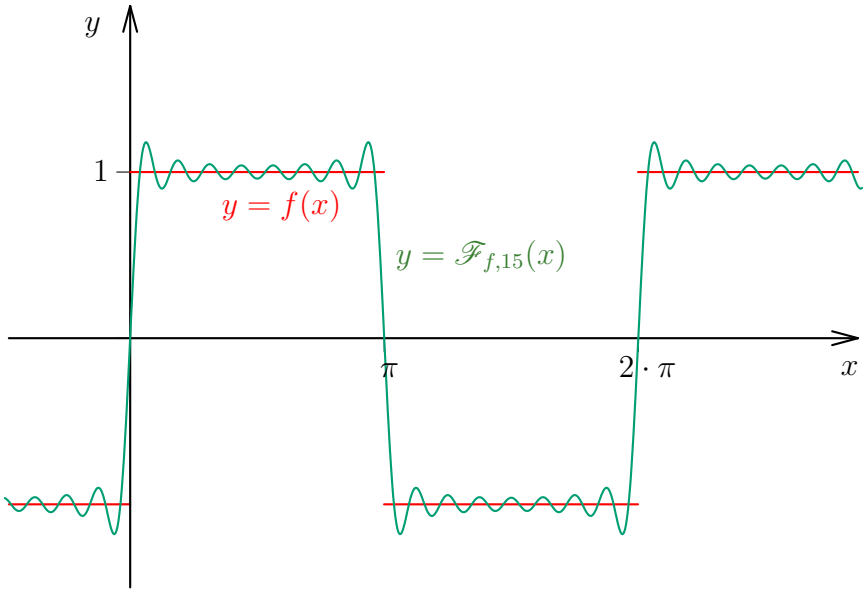
also eine noch sehr ungenaue Näherung. Besser liegen wir schon mit dem dritten Fourierpolynom $\mathscr{F}_{f,3}(x) = \frac{\pi}{4} \cdot \sin(x) + \frac{\pi}{12} \cdot \sin(3x)$:



und das siebte Fourierpolynom $\mathfrak{F}_{f,7}$:



bzw. das fünfzehnte Fourierpolynom $\mathfrak{F}_{f,15}$:



liefern schon ziemlich gute Approximationen (wenn wir von den Sprungstellen absehen).

Bemerkung 1.3.6. In Beispiel 1.3.3 war $a_n = 0$ für alle $n \in \mathbb{N}$. Das ist kein Zufall, denn ganz allgemein gilt:
Ist f eine ungerade 2π–periodische Funktion (gilt also $f(-x) = -f(x)$ für alle x), so gilt

$$a_n = 0 \quad \text{für alle } n \in \mathbb{N}$$

Ist f eine gerade 2π–periodische Funktion (gilt also $f(-x) = f(x)$ für alle x), so gilt

$$b_n = 0 \quad \text{für alle } n \in \mathbb{N}$$

Dazu nutzen wir zunächst aus, dass aufgrund der Peridizität von f gilt

$$\begin{aligned} a_n &= \tfrac{1}{\pi} \cdot \int_0^{2\pi} f(x)\cos(nx)dx \\ &= \tfrac{1}{\pi} \cdot \int_0^{\pi} f(x)\cos(nx)dx + \tfrac{1}{\pi} \cdot \int_{\pi}^{2\pi} f(x)\cos(nx)dx \\ &= \tfrac{1}{\pi} \cdot \int_0^{\pi} f(x)\cos(nx)dx + \tfrac{1}{\pi} \cdot \int_{-\pi}^{0} f(x)\cos(nx)dx \\ &= \tfrac{1}{\pi} \cdot \int_{-\pi}^{\pi} f(x)\cos(nx)dx \end{aligned}$$

und analog

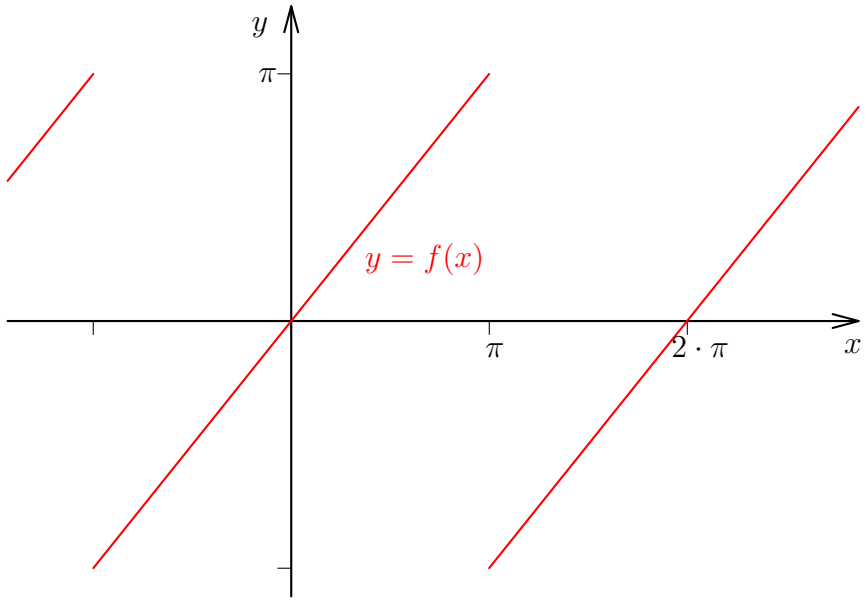
$$b_n = \frac{1}{\pi} \cdot \int_{-\pi}^{\pi} f(x) \sin(nx) dx$$

Aus den Symmetrieeigenschaften folgt nun leicht die Behauptung.

Beispiel 1.3.4. Wir betrachten die Sägezahnfunktion $f : \mathbb{R} \longrightarrow \mathbb{R}$, die für $n \in \mathbb{Z}$ auf dem Intervall $[(2n-1)\pi, (2n+1)\pi[$ definiert ist durch

$$f(x) = \begin{cases} x - 2n\pi & \text{für } (2n-1)\pi \leq x < (2n+1)\pi \\ 0 & \text{für } x = (2n-1)\pi, (2n+1)\pi \end{cases}$$

Auch hier handelt es sich um eine 2π–periodische Funktion, die ungerade ist und folgende Gestalt hat:



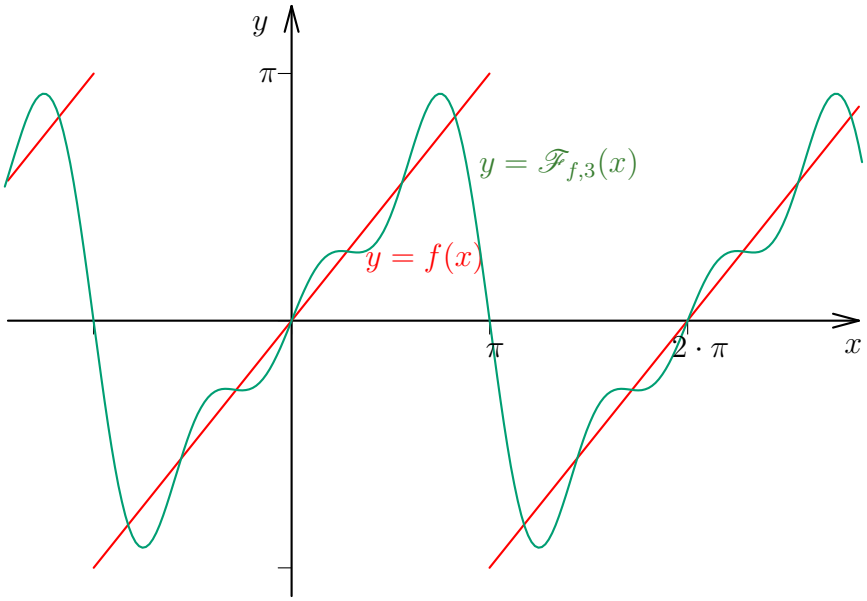
Also müssen wir gemäß Bemerkung 1.3.6 nur die b_n berechnen, und können dies auch über dem Intervall $[-\pi, \pi]$ tun. Hierzu benutzen wir partielle Integration

$$\begin{aligned} b_n &= \tfrac{1}{\pi} \cdot \int_{-\pi}^{\pi} x \cdot \sin(nx) dx \\ &= \tfrac{1}{\pi} \cdot \left(\left[-x \tfrac{\cos(nx)}{n} \right]_{-\pi}^{\pi} + \int_{-\pi}^{\pi} \tfrac{\cos(nx)}{n} dx \right) \\ &= \tfrac{2}{n} \cdot \cos(n\pi) \\ &= 2 \cdot \tfrac{(-1)^{n+1}}{n} \end{aligned}$$

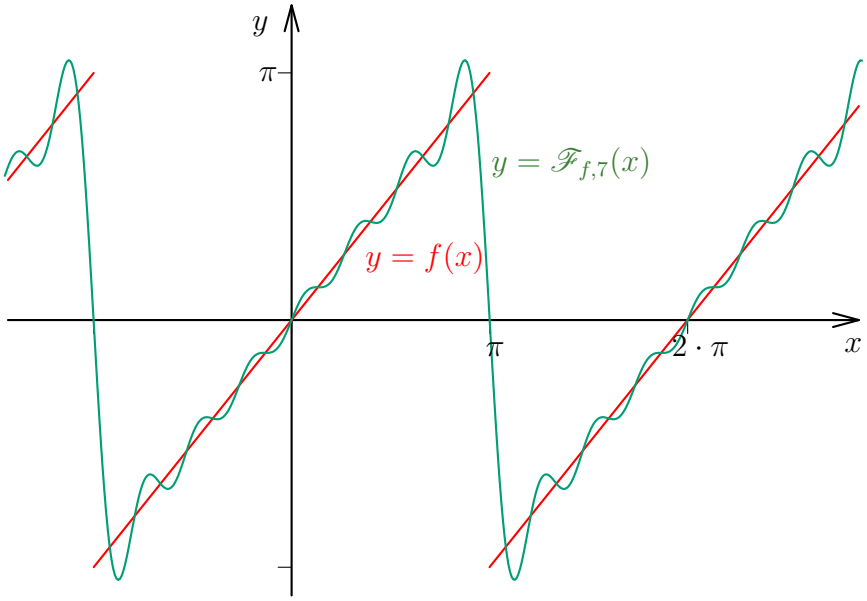
und damit bekommen wir als Fourier–Reihe

$$\mathscr{F}_f(x) = 2 \cdot \sum_{n=1}^{\infty} \frac{(-1)^{n+1} \cdot \sin(nx)}{n}$$

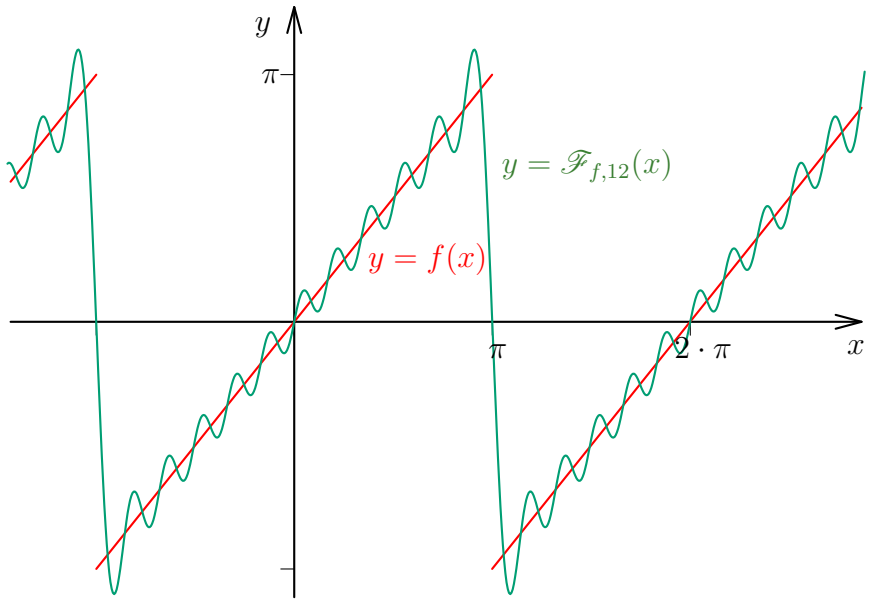
Wir erhalten also als Näherung mit dem dritten Fourierpolynom $\mathscr{F}_{f,3}$:



mit dem siebten Fourierpolynom $\mathscr{F}_{f,7}$:



und mit dem zwölften Fourierpolynom $\mathscr{F}_{[f,12}$:

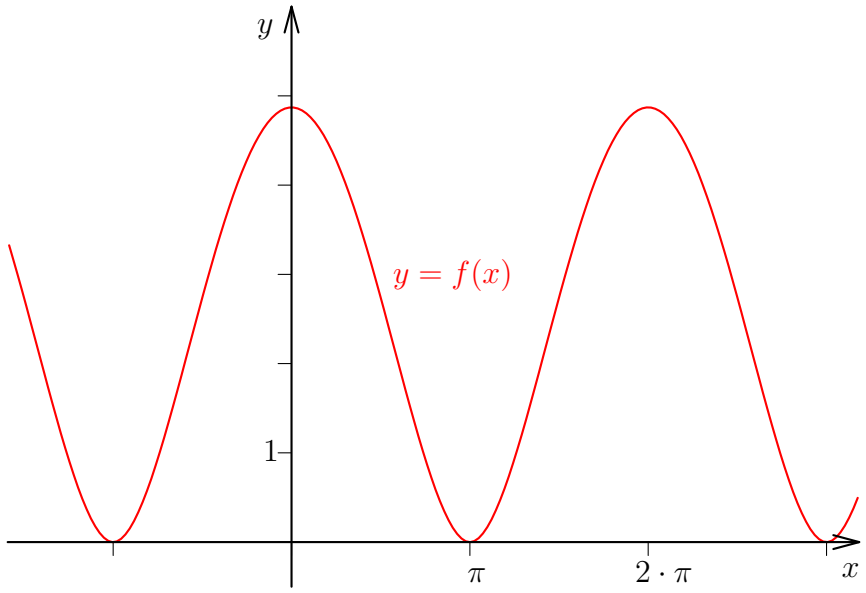


Auch hier erkennt man die Annäherung in den glatten Abschnitten; die Sprungstellen werden immer schneller überbrückt, können aber natürlich durch die Fourierpolynome (die ja alle stetig sind) nicht realisiert werden.

Beispiel 1.3.5. Wir betrachten nun die 2π–periodische Funktion $f : \mathbb{R} \longrightarrow \mathbb{R}$, die auf dem Intervall $]-\pi, \pi]$ gegeben ist durch

$$f(x) = \frac{1}{20} \cdot x^4 - \frac{\pi^2}{10} \cdot x^2 + \frac{\pi^4}{20}$$

(und dann 2π–periodisch fortgesetzt wird), die also folgende Gestalt hat:



Insbesondere ist die Funktion f stetig differenzierbar. Außerdem handelt es sich um eine gerade Funktion, und daher ist $b_n = 0$ für alle n. Ferner berechnen wir

$$a_0 = \frac{1}{\pi} \cdot \int_{-\pi}^{\pi} f(x)\, dx = \frac{4}{75} \cdot \pi^4$$

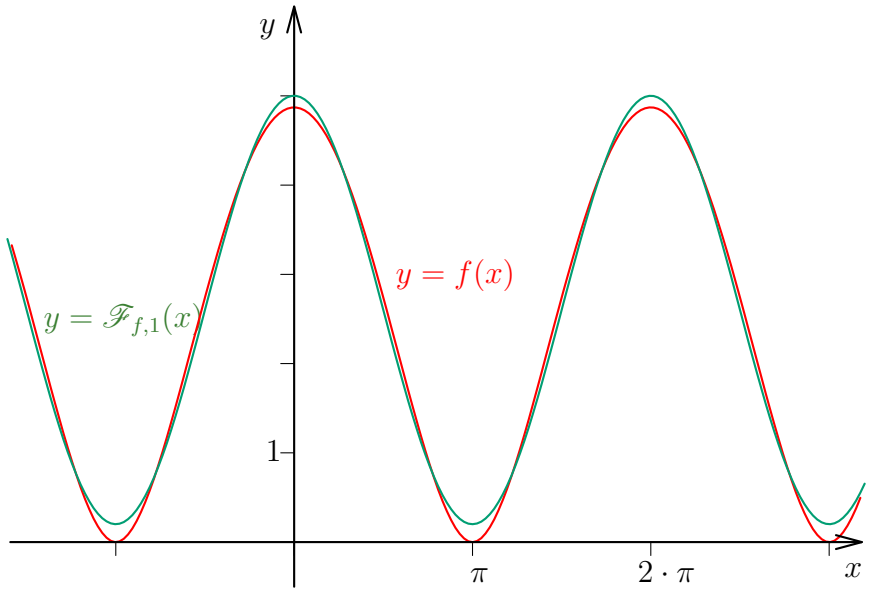
und für $n \geq 1$:

$$a_n = \frac{1}{\pi} \cdot \int_{-\pi}^{\pi} f(x) \cdot \cos(nx)\, dx = (-1)^{n+1} \cdot \frac{12}{5 \cdot n^2}$$

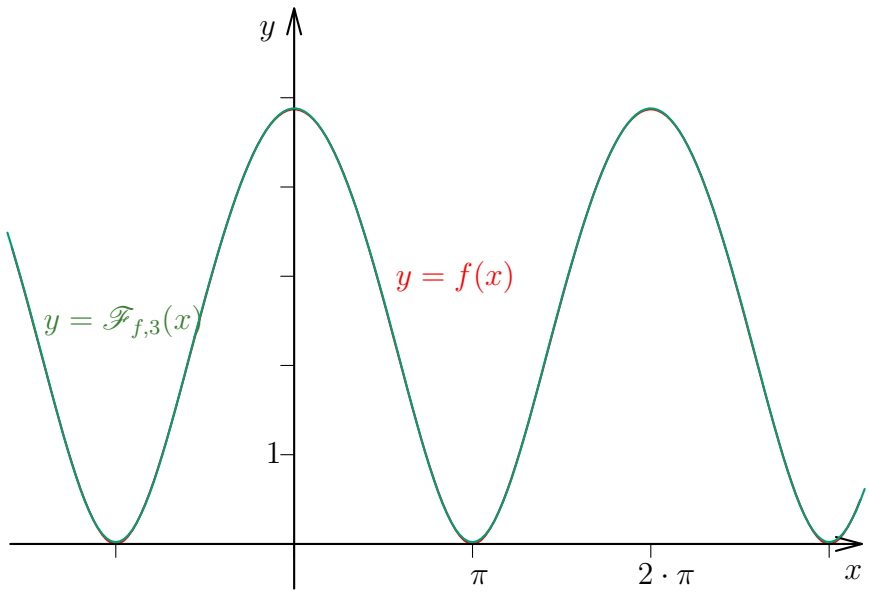
und damit bekommen wir als Fourier–Reihe

$$\mathscr{F}_f(x) = \frac{2}{75} \cdot \pi^4 + \sum_{n=1}^{\infty} \frac{(-1)^{n+1} \cdot 12 \cdot \cos(nx)}{5 \cdot n^4}$$

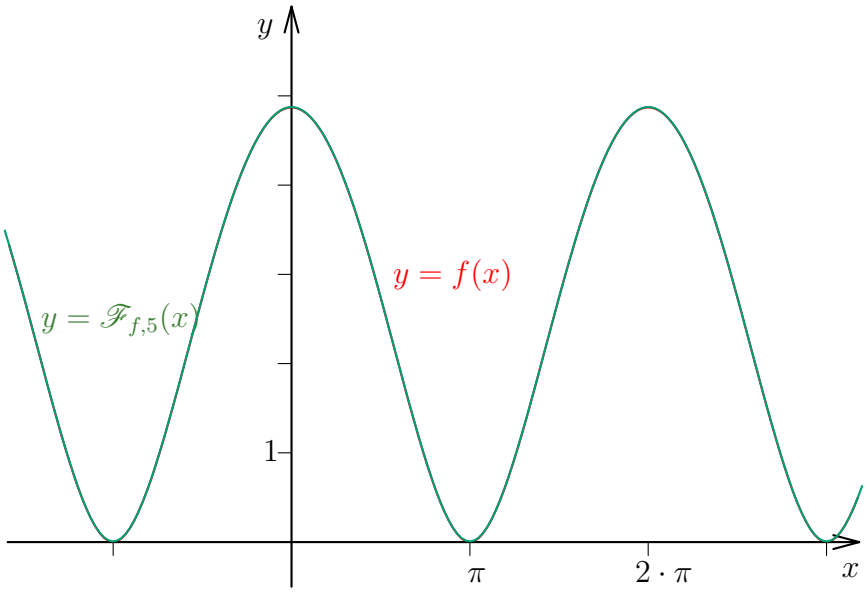
Wir erhalten also als Näherung mit dem ersten Fourierpolynom $\mathscr{F}_{f,1}$:



mit dem drittten $\mathfrak{F}_{f,3}$:



und mit dem fünften $\mathfrak{F}_{f,5}$:



Wir beobachten hier also eine sehr schnelle und vor allem sehr gleichmäßige Konvergenz der Fourierpolynome gegen die Funktion f, wie das in diesem Fall auch schon durch Satz 1.3.2 vorhergesagt wird.

Beispiel 1.3.6. Wir betrachten die Rechtecksschwingung $f : \mathbb{R} \longrightarrow \mathbb{R}$, die auf jedem Intervall $[\,2n,\, 2(n+1)\,]$ $(n \in \mathbb{Z})$ definiert ist durch

$$f(x) = \begin{cases} 1 & \text{für } 2n < x < 2n+1 \\ 0 & \text{für } x = 2n, 2n+1, 2(n+1) \\ -1 & \text{für } 2n+1 < x < 2(n+1) \end{cases}$$

Das ist offensichtlich eine periodische Funktion mit primitiver Periode zwei. Betrachten wir daher die Funktion $g(x) := f\left(\frac{x}{\pi}\right)$, so ist g periodisch mit Periode 2π. In der Tat handelt es sich bei g um die Rechtecksschwingung aus Beispiel 1.3.3, und damit hat g die Fourierreihe

$$\mathscr{F}_g(x) = \frac{4}{\pi} \cdot \sum_{n=0}^{\infty} \frac{\sin((2n+1)x)}{2n+1}$$

Machen wir die Rücktransformation $f(x) = g\,(\pi \cdot x)$, so erhalten wir hieraus als Fourierreihe von f:

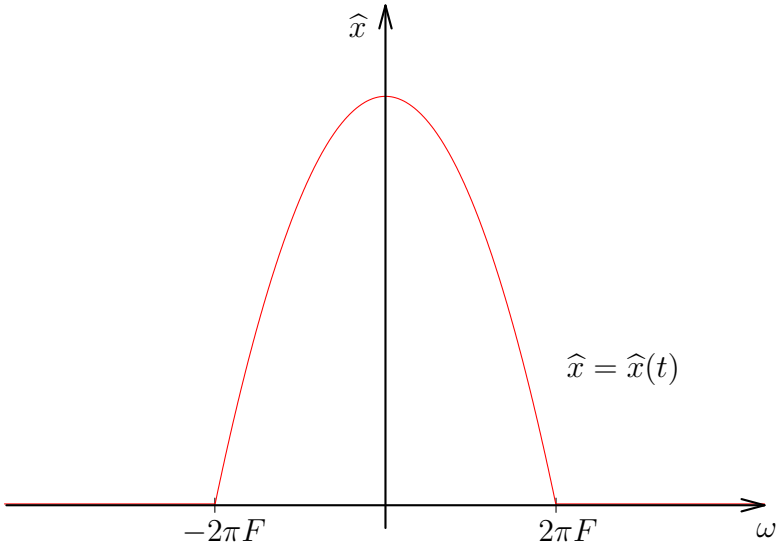
$$\mathscr{F}_f(x) = \frac{4}{\pi} \cdot \sum_{n=0}^{\infty} \frac{\sin\,((2n+1) \cdot \pi \cdot x)}{2n+1}$$

1.4 Das Abtasttheorem

Nun stellt sich die Frage, in wiefern diese Resultate bei der Rekonstruktion von Signalen aus ihren Diskretisierungen benutzt werden können.
Ein Signal $x(t)$ heißt **bandbeschränkt** mit maximaler Frequenz F, wenn die Fouriertransformierte $\widehat{x}(\omega)$ von $x(t)$ existiert, und wenn

$$\widehat{x}(\omega) = 0 \qquad \text{für } \omega \notin [\,-2\pi \cdot F, 2\pi \cdot F\,]$$

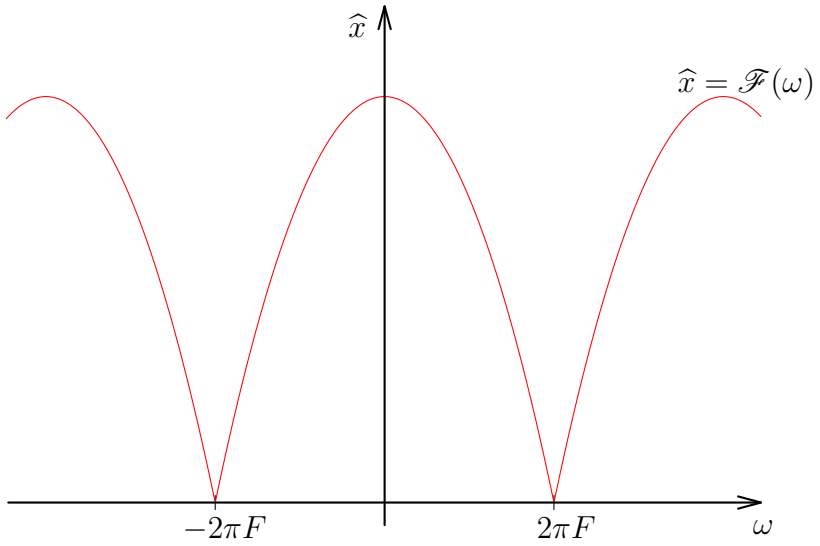
Wir haben also jetzt ein Signal dessen Spektrum (Fouriertransformierte) nur innerhalb des Intervalls $[\,-2\pi \cdot F, 2\pi \cdot F\,]$ von Null verschiedene Werte annehmen kann. Die Fouriertransformierte von $x(t)$ könnte also etwa folgende Gestalt haben



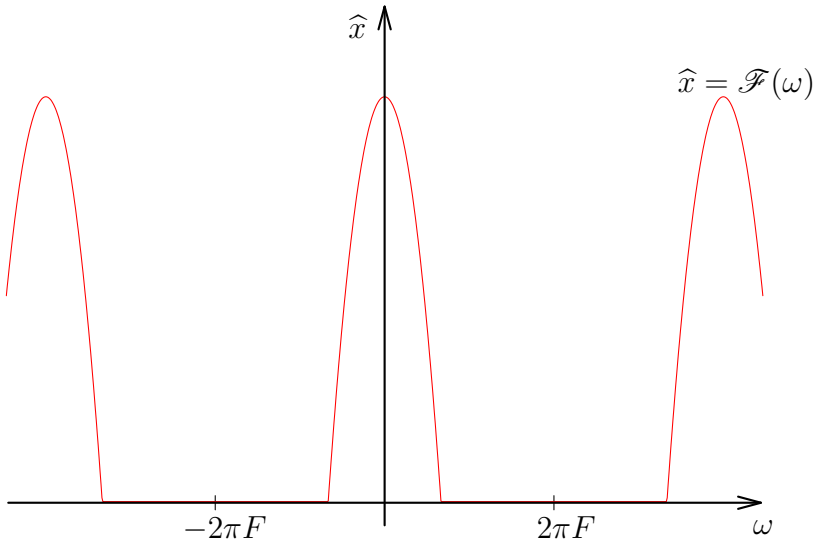
Damit ist $\widehat{x}(\omega)$ sicherlich nicht periodisch, wir können also die Theorie der Fourierreihen nicht anwenden. Allerdings können wir aus $\widehat{x}(\omega)$ eine $4\pi F$–periodische Funktion $\mathscr{F}$ machen ohne dabei Information zu verlieren. Dazu setzen wir $\widehat{x}(\omega)$ ausserhalb des Intervalls $[\,-2\pi F, 2\pi F\,]$ mit Hilfe der Funktionswerte aus dem Intervall $[\,-2\pi F, 2\pi F\,]$ so fort, dass daraus eine $4\pi F$–periodische Funktion wird. Genauer finden wir zu jedem $\omega \in \mathbb{R}$ genau ein $l \in \mathbb{Z}$, so dass $\omega - l \cdot 4\pi F \in [\,-2\pi F, 2\pi F\,]$ und wir setzen

$$\mathscr{F}(\omega) = \widehat{x}(\omega - l \cdot 4\pi F)$$

In unserem Beispiel könnte das etwa so aussehen



oder auch so



Diese Funktion ist jetzt periodisch mit Periode $4\pi F$, und daher können wir sie als Fourierreihe entwickeln,

$$\mathscr{F}(\omega) = \frac{a_0}{2} + \sum_{l=1}^{\infty} \left[a_l \cdot \cos\left(\frac{l\omega}{2F}\right) + b_l \cdot \sin\left(\frac{l\omega}{2F}\right) \right]$$

wobei

$$\begin{aligned} a_l &= \tfrac{1}{2\pi F} \int_{-2\pi F}^{2\pi F} \mathscr{F}(\omega) \cdot \cos\left(\tfrac{l\omega}{2F}\right) d\omega &= \tfrac{1}{2\pi F} \int_{-2\pi F}^{2\pi F} \widehat{x}(\omega) \cdot \cos\left(\tfrac{l\omega}{2F}\right) d\omega \\ b_l &= \tfrac{1}{2\pi F} \int_{-2\pi F}^{2\pi F} \mathscr{F}(\omega) \cdot \sin\left(\tfrac{l\omega}{2F}\right) d\omega &= \tfrac{1}{2\pi F} \int_{-2\pi F}^{2\pi F} \widehat{x}(\omega) \cdot \sin\left(\tfrac{l\omega}{2F}\right) d\omega \end{aligned}$$

Wir wollen nun stets annehmen, dass diese Fourierreihe auch tatsächlich die periodisch gemachte Funktion darstellt, und außerdem dass die Voraussetzungen für die Umkehrtransformation der Fouriertransformation gegeben sind.
Dann gilt ferner nach der Umkehrformel für die Fouriertransformation

$$\begin{aligned} x(t) &= \tfrac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \widehat{x}(\omega) \cdot \cos(\omega t) d\omega + \tfrac{\mathrm{i}}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \widehat{x}(\omega) \cdot \sin(\omega t) d\omega \\ &= \tfrac{1}{\sqrt{2\pi}} \int_{-2\pi F}^{2\pi F} \widehat{x}(\omega) \cdot \cos(\omega t) d\omega + \tfrac{\mathrm{i}}{\sqrt{2\pi}} \int_{-2\pi F}^{2\pi F} \widehat{x}(\omega) \cdot \sin(\omega t) d\omega \end{aligned}$$

Wählen wir speziell die Zeitpunkte $t = \pm\frac{l}{2F}$ so ergibt sich

$$\begin{aligned} x\left(\tfrac{l}{2F}\right) &= \tfrac{2\pi \cdot F}{\sqrt{2\pi}} \left(a_l + \mathrm{i} \cdot b_l\right) \\ x\left(-\tfrac{l}{2F}\right) &= \tfrac{2\pi \cdot F}{\sqrt{2\pi}} \left(a_l - \mathrm{i} \cdot b_l\right) \end{aligned}$$

woraus wiederum folgt

$$\begin{aligned} a_l &= \tfrac{1}{2\sqrt{2\pi F}} \left(x\left(\tfrac{l}{2F}\right) + x\left(-\tfrac{l}{2F}\right)\right) \\ b_l &= \tfrac{-i}{2\sqrt{2\pi F}} \left(x\left(\tfrac{l}{2F}\right) - x\left(-\tfrac{l}{2F}\right)\right) \end{aligned}$$

Damit können wir also die Fourierreihe von $\mathscr{F}(\omega)$ mit Hilfe der Abtastwerte ausdrücken und erhalten

$$\begin{aligned} \mathscr{F}(\omega) &= \sum_{l=\infty}^{\infty} \tfrac{1}{2\sqrt{2\pi F}} \cdot x\left(\tfrac{l}{2F}\right) \cdot \cos\left(\tfrac{l\omega}{2F}\right) \\ &\quad -\mathrm{i} \cdot \sum_{l=-\infty}^{\infty} \tfrac{1}{2\sqrt{2\pi F}} \cdot x\left(\tfrac{l}{2F}\right) \cdot \sin\left(\tfrac{l\omega}{2F}\right) \end{aligned}$$

Daraus leiten wir aber via Umkehrformel auch für $x(t)$ selbst einen Ausdruck ab, der die Abtastwerte involviert. Unter Ausnutzung der Additionstheorem

für Sinus und Cosinus ergibt sich nämlich

$$\begin{aligned}
x(t) &= \tfrac{1}{\sqrt{2\pi}} \cdot \left(\int_{-\infty}^{\infty} \widehat{x}(\omega) \cdot \cos(\omega t) d\omega + \mathrm{i} \cdot \int_{-\infty}^{\infty} \widehat{x}(\omega) \cdot \sin(\omega t) d\omega \right) \\
&= \tfrac{1}{\sqrt{2\pi}} \cdot \left(\int_{-2\pi F}^{2\pi F} \mathscr{F}(\omega) \cdot \cos(\omega t) d\omega + \mathrm{i} \int_{-2\pi F}^{2\pi F} \mathscr{F}(\omega) \cdot \sin(\omega t) d\omega \right) \\
&= \tfrac{1}{4\pi F} \sum_{l=-\infty}^{\infty} x\left(\tfrac{l}{2F}\right) \cdot \left(\int_{-2\pi F}^{2\pi F} \cos\left(\omega\left(t - \tfrac{l}{2F}\right)\right) d\omega \right. \\
&\qquad \left. + \mathrm{i} \cdot \int_{-2\pi F}^{2\pi F} \sin\left(\omega\left(t - \tfrac{l}{2F}\right)\right) d\omega \right) \\
&= \tfrac{1}{4\pi F} \sum_{l=-\infty}^{\infty} 4\pi F \cdot x\left(\tfrac{l}{2F}\right) \cdot \tfrac{\sin(2\pi F t - \pi l)}{2\pi F t - \pi l} \\
&= \sum_{l=-\infty}^{\infty} x\left(\tfrac{l}{2F}\right) \cdot \tfrac{\sin(2\pi F t - \pi l)}{2\pi F t - \pi l}
\end{aligned}$$

Damit haben wir also für $x(t)$ die sogennannte **Kardinalreihendarstellung**

$$x(t) = \sum_{l=-\infty}^{\infty} x\left(\frac{l}{2F}\right) \cdot \frac{\sin(2\pi \cdot F \cdot t - \pi \cdot l)}{2\pi \cdot F \cdot t - \pi \cdot l}$$

hergeleitet und insbesondere gezeigt, dass sich $x(t)$ vollständig und ohne Informationsverlust aus den Abtastwerten $\left\{x\left(\frac{l}{2F}\right)\right\}_{l \in \mathbb{Z}}$ rekonstruieren lässt.

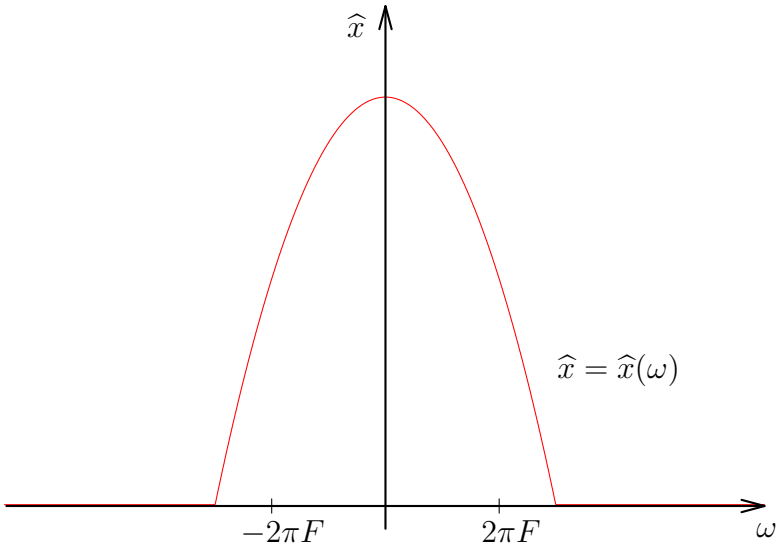
Satz 1.4.1 (Abtasttheorem von Shannon)**.** *Ist $x(t)$ ein durch die maximale Frequenz F bandbeschränktes stetiges Signal, so kann $x(t)$ durch eine Abtastung deren Abtastabstände höchstens $\frac{1}{2F}$ sind, vollständig aus dem daraus entstehenden zeitdiskreten Signal wiederhergestellt werden*

Bemerkung 1.4.1. Das Abtasttheorem lässt sich auch wie folgt formulieren: Wird ein durch die maximale Frequenz F bandbegrenztes Signal mindestens mit doppelter Abtastfrequenz $2 \cdot F$ abgetastet, so kann es aus den Abtastwerten rekonstruiert werden. Bestimmt F auch die minimale Bandbreite, so kann keine kleinere Abtastfrequenz gewählt werden, um das Signal zu rekonstruieren.

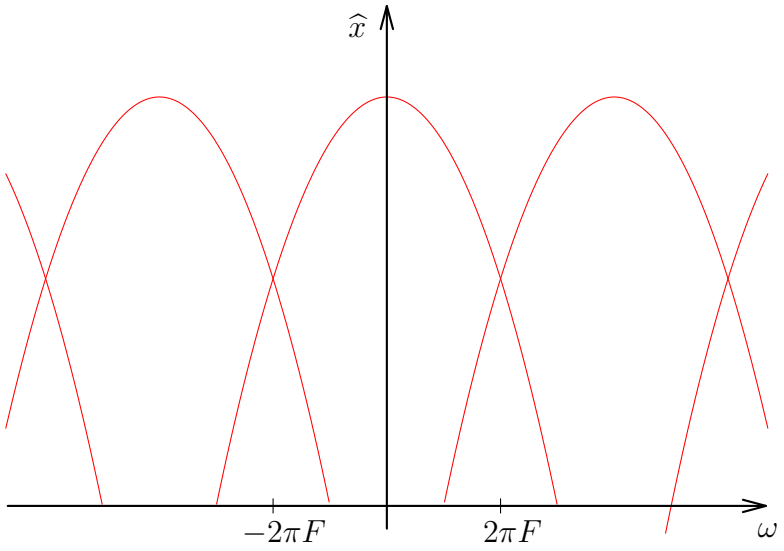
Bemerkung 1.4.2. Dieses Abtasttheorem ist auch als Nyquist–Shannon–Abtasttheorem oder als Whittaker–Kotelnikow–Shannon–Abtasttheorem bekannt.

Bemerkung 1.4.3. Bandbegrenzte Signale treten in der Praxis kaum auf. Allerdings sind in der Regel hohe Frequenzen nicht relevant, da der Mensch Töne ab einer bestimmten Frequenz nicht mehr hört oder Lichtwellen ab einer bestimmten Frequenz nicht mehr sieht. Diese Frequenzen können (etwa mit Hilfe eines Tiefpassfilters) aus dem Originalsignal herausgefiltert werden ohne dadurch relevante Information zu verlieren. Das resultierende Signal ist dann bandbegrenzt und kann mit Hilfe des Abtastthorems von Shannon gesamplet werden. Es ist jedoch notwendig, die irrelevanten Frequenzen vor dem Abtasten herauszufiltern. Werden sie nämlich mitabgetastet, so werden sie beim Wiederherstellen des Signals in den (hör– oder sichtbaren Berreich) transformiert und führen zu Störungen. Dieser *Aliaseffekt* tritt generell bei Abtastung mit zu kleiner Frequenz (Unterabtastung, undersampling) auf.

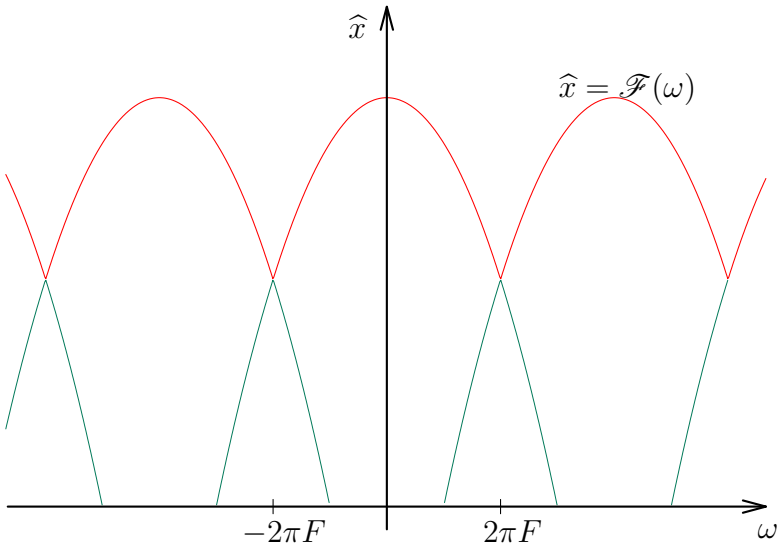
In diesem Beispile wird die Originalbandbreite unterschätzt



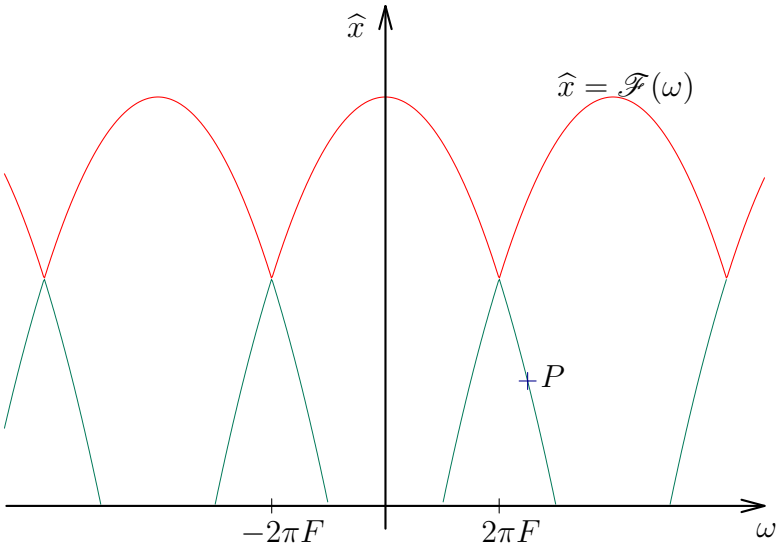
Undersampling durch zu niedrige Abtastfrequenz führt dazu, dass sich die Frequenzbögen überschneiden würden



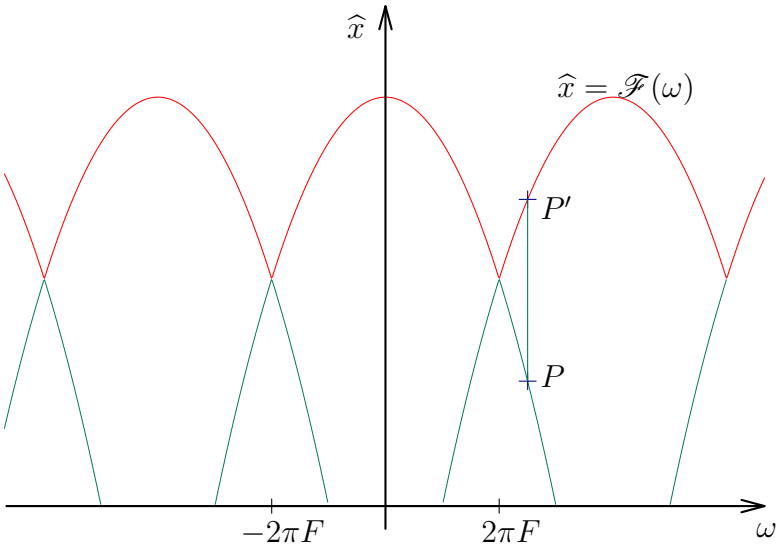
Für die Fourierreihenentwicklung wird dann aber nur folgendes Bild betrachtet



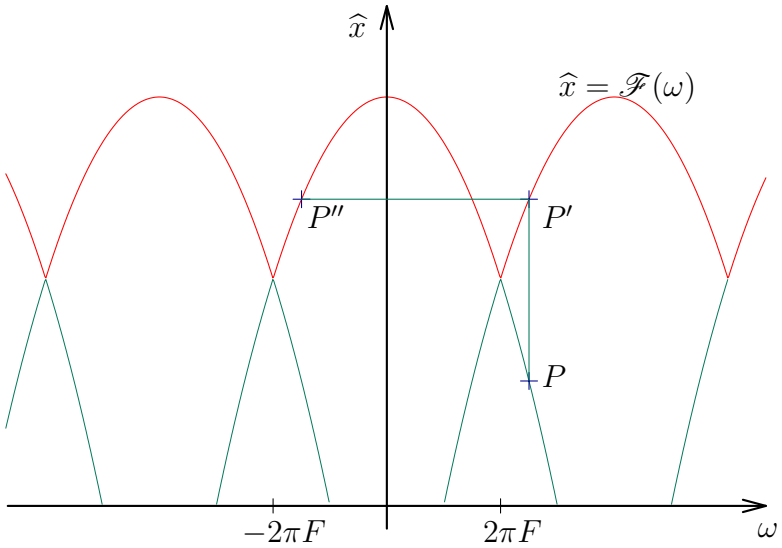
Eine Frequenz (hier gegeben durch den Punkt P), die beim ursprünglichen Signal ausserhalb $[-2\pi F, 2\pi F]$ lag



wird dann im Rahmen der Rekonstruktion mit P' identifiziert



und als Frequenz P'' innerhalb des Intervalls $[-2\pi F, 2\pi F]$ interpretiert und wiedergegeben



und es kommt zum Aliaseffekt.

Bemerkung 1.4.4. Abtasten mit zu hoher Frequenz (als mit einer Frequenz, die die durch das Abtasttheorem geforderte Frequenz von $2F$ übersteigt) wird in der Praxis oft angewendet. Da das Originalsignal in der Regel nicht bandbegrenzt ist, sondern nur der relevante Teil, muss dieser mit Hilfe eines Tiefpassfilters herausgefiltert werden. Ein Tiefpassfilter, der aber alle Frequenzen ausserhalb des relevanten Bereichs unmittelbar abschneidet, ist technisch nicht realisierbar. Daher wird in der Praxis mit einer Frequenz von mindestens $\frac{22}{10} \cdot F = 2.2 \cdot F$ abgetastet, wobei F die maximale relevante Bandbreite bezeichnet.

Kapitel 2

Grundlagen der Codierungstheorie

Digitalisierte Daten und Signale stellen üblicherweise eine sehr große Menge an Informationen dar. Der menschliche Hörbereich etwa geht bis 20.000 Hz. Nach dem Abtasttheorem müssen für die Darstellung dieses Frequenzbereichs mindestens 40.000 Signalwerte pro Sekunde gespeichert werden. Da die akustischen Wellen allerdings über 20.000 Hz hinausgehen, muss der relevante Bereich zunächst erst mit einem Tiefbassfilter ausgeschnitten werden. Hierfür ist eine gewisse Toleranz erforderlich, so dass die Signalwerte nur auf den Frequenzbereich bis ca. 22.000 Hz beschränkt werden können. Daher wurde die Abtastrate für Audiosignale auf 44.100 Hz normiert. Jeder Abtastwert wird dann digital als *Audiobit* abgespeichert. Dafür sind 2 Byte, also 16 Bit, pro Kanal erforderlich. Bei Stereowiedergabe verdoppetl sich also die Datenmenge, so dass pro Sekunde Musik über 1.000.000 Bits an Binärdaten anfallen. Eine solche Menge von Informationen ist praktisch nicht fehlerfrei zu speichern. Um das Audiosignal zu rekonstruieren, iet es daher notwendig, Fehler in der Speicherung und der Übertragung zu erkennen und zu korrigieren.

Der grundsätzliche Ansatz hierzu ist, die Nachricht mit Redundanzen so anzureichern, dass auch aus einer fehlerhaft übertragenen Nachricht noch auf deren Inhalt geschlossen werden kann.

2.1 Fehlererkennung und Fehlerkorrektur

Bei der Frage der Sicherheit und Zuverlässigkeit der Datenspeicherung und Datenübertragung unterscheidet man zwei grundsätzliche Problembereiche

1. Fehlererkennung: Wie kann ich erkennen, dass ein empfangener Datensatz unkorrekt ist?

2. Fehlerkorrektur: Wie kann ich aus den empfangenen Daten die ursprüngliche Nachricht rekonstruieren?

Wir wollen das zunächst anhand eines Beispiels darstellen:
Situation: Übertragen werden sollen Bilder, die sich nur aus den Farben WEISS $= (0,0)$, HELLGRAU $= (0,1)$, DUNKELGRAU $= (1,0)$ und SCHWARZ $= (1,1)$ zusammensetzen. Offensichtlich kann ein Übertragungsfehler an einer Stelle zu einer starken Verfälschung des Bildes führen. Durch Anreicherung mit Redundanzen soll dieses Risiko verringert werden.
Nicht alle Anreicherungen sind geschickt.

Beispiel 2.1.1. Wir betrachten die folgende Anreicherung

$$\begin{array}{llll} (0,0) & \longmapsto & c_1 = (0,0,0,0,0) & (1,0) \longmapsto c_3 = (1,0,0,0,0) \\ (0,1) & \longmapsto & c_2 = (0,1,0,0,0) & (1,1) \longmapsto c_4 = (1,1,0,0,0) \end{array}$$

Diese Anreicherung ist ganz offensichtlich wenig hilfreich. Wollen wir etwa dunkelgrau übertragen, also $(1,0,0,0,0)$ und tritt eine Fehler auf, so könnte etwa $(0,0,0,0,0)$ ankommen. Der Empfänger hat in diesem Fall keine Chance, den Fehler auch nur zu erkennen.

Beispiel 2.1.2. Wir betrachten nun die folgende Anreicherung

$$\begin{array}{llll} (0,0) & \longmapsto & c_1 = (0,0,0,0,0) & (1,0) \longmapsto c_3 = (1,0,1,0,0) \\ (0,1) & \longmapsto & c_2 = (0,1,1,0,0) & (1,1) \longmapsto c_4 = (1,1,0,0,0) \end{array}$$

Diese Anreicherung ist schon etwas besser. Wollen wir etwa dunkelgrau übertragen, also $(1,0,1,0,0)$ und tritt eine Fehler auf, so könnte etwa $(0,0,1,0,0)$ ankommen. Der Empfänger hat kann in diesem Fall auf jeden Fall sehen, dass das eingehende Datum nicht korrekt ist, denn es ist nicht in der Liste

der möglichen c_i. Er kann also den Fehler erkennen. Allerdings kann er ihn nicht korrigieren, denn es ist für ihn nicht möglich, zu entscheiden, ob bei der Übertragung von $(0,0,0,0,0)$ (also weiss) oder bei der Übertragung von $(1,0,1,0,0)$ (also dunkelgrau) ein Fehler aufgetreten ist.
Es ist eine leichte Übung, festzustellen, dass bei Auftreten eines einzelnen Fehlers in der Übertragung immer festgestellt werden kann, dass die Übertragung fehlerhaft war.

Beispiel 2.1.3. Wir betrachten nun die folgende Anreicherung

$$\begin{array}{llll} (0,0) & \longmapsto & c_1 = (0,0,0,0,0) & (1,0) \longmapsto c_3 = (1,0,1,0,1) \\ (0,1) & \longmapsto & c_2 = (0,1,1,1,0) & (1,1) \longmapsto c_4 = (1,1,0,1,1) \end{array}$$

Nach dieser Anreicherung unterscheiden sich je zwei der erzeugten **Codewörter** an mindestens drei Stellen. Es handelt sich um eine geschickte und sinnvolle Anreicherung, denn damit lässt sich ein Fehler an einer Stelle korrigieren: Empfängt R etwa das Wort $a = (1,1,1,0,1)$, so erkennt er zunächst sofort, dass es sich nicht um eine korrekte Nachricht handelt. Er kann nun wie folgt argumentieren: Der Datenstrom a unterscheidet sich von c_3 an genau einer Stelle, von c_4 dagegen an 2, von c_2 an 3 und von c_1 sogar an 4 Stellen. Daher hat S höchstwahrscheinlich die Nachricht c_3 gesendet, also die Farbe dunkelgrau.

Erstrebenswert sind Zeichenfolgen, die sich an möglichst vielen Stellen unterscheiden.

2.1.1 Das Prinzip der Fehlererkennung

Um Fehler zu Erkennen, werden die einzelnen Datensätze üblicherweise um eine Prüfziffer angereichert, die sich aus den informationstragenden Zeichen errechnet. So kann man etwa in einem Byte (also in 8 Bit) an 7 Stellen Information speichern und an der achten Stelle ein *Paritätsprüfbit* einfügen. Dieses Paritätsprüfbit wird dabei immer so gesetzt, dass sowohl die Anzahl der Einsen als auch die Anzahl der Nullen in den acht Stellen gerade ist.

Beispiel 2.1.4. Wir betrachten eine Information a, die in einer Folge von vier Ziffern $a_1, \ldots, a_4$ im Bereich $0, \ldots, 6$ abgelegt ist,

$$a = (a_1, a_2, a_3, a_4) \qquad a_i \in \{0, \ldots, 6\}$$

etwa

$$a = (2, 3, 1, 6)$$

Zur Fehlererkennung fügen wir eine Prüfziffer a_5 (zwischen 0 und 6) hinzu, so dass die Summe der Ziffern durch 7 teilbar ist, also

$$c = (a_1, a_2, a_3, a_4, a_5) \quad \text{mit } a_1 + a_2 + a_3 + a_4 + a_5 \equiv 0 \bmod 7$$

in unserem Beispiel also

$$c = (2, 3, 1, 6, 2)$$

Dabei ist die Prüfziffer eindeutig bestimmt. Wird nur eine der Zahlen falsch übertragen, so kann dies erkannt werden, denn dann ist die Summe zwangsläufig nicht mehr durch 7 teilbar. Erhalten wir also

$$m = (2, 2, 1, 6, 2)$$

so bilden wir die Prüfsumme, also die Summe aller Ziffern, und erhalten

$$2 + 2 + 1 + 6 + 2 = 13$$

eine Zahl, die nicht durch 7 teilbar ist. Damit ist klar, dass ein Fehler aufgetreten ist. Wir können jedoch nicht erkennen, an welcher Stelle.

Auch im Alltagsleben begegnen uns täglich fehlererkennende Codierungsverfahren

Der ISBN–10 Code:

Bücher sind schon seit langem mit einer eindeutigen Klassifizierungsnummer versehen, die zur Sicherheit eine Prüfziffer enthält. Klassischerweise wurde hierfür ISBN–10 (**I**nternational **S**tandard **B**ook **N**umber) verwendet, eine zehnstellige Kennung, die für jeden Buchtitel eindeutig ist. Dabei enthalten die ersten 9 Stellen alle Informationen über das Buch, und sie sind wie folgt aufgebaut:

- Der erste Zahlenblock enthält die Ländernummer. So steht etwa ”3” für den deutschsprachigen Raum oder ”7” für China.
- Der zweite Zahlenblock enthält die Verlagsnummer, also die eindeutige Kennzeichnung des Verlags.

- Der dritte Zahlenblock enthält die vom Verlag vergebene Titelnummer.
- Der vierte Block enthält ein Prüfkennzeichen.

Dieses Prüfzeichen p wird aus der Information $(a_1, a_2, \ldots, a_9)$ wie folgt berechnet:

1. Bestimme die Summe
$$s = a_1 + 2a_2 + 3a_3 + \cdots + 9a_9 = \sum_{l=1}^{9} l \cdot a_l$$
2. Dividiere s durch 11 mit Rest
$$s = q \cdot 11 + r$$
mit einer ganzen Zahl $r \in \{0, 1, \ldots, 10\}$.
3. Falls $r = 10$ setze $p = X$, andernfalls setze $p = r$.

Beispiel 2.1.5. Wir betrachten ein Buch, dessen 9 Informationsstellen die Gestalt $3 - 86680 - 192$ haben.

1. $s = 3 + 2 \cdot 8 + 3 \cdot 6 + 4 \cdot 6 + 5 \cdot 8 + 6 \cdot 0 + 7 \cdot 1 + 8 \cdot 9 + 9 \cdot 2 = 198$.
2. $s = 18 \cdot 11$ Rest 0.
3. $p = 0$

Die ISBN-10 Nummer dieses Buches ist also $3 - 86680 - 192 - 0$.

Beispiel 2.1.6. Wir betrachten ein Buch, dessen 9 Informationsstellen die Gestalt $3 - 680 - 08783$ haben.

1. $s = 3 + 2 \cdot 6 + 3 \cdot 8 + 4 \cdot 0 + 5 \cdot 0 + 6 \cdot 8 + 7 \cdot 7 + 8 \cdot 9 + 9 \cdot 3 = 227$.
2. $s = 20 \cdot 11$ Rest 7.
3. $p = 7$

Die ISBN–10 Nummer dieses Buches ist also $3 - 680 - 08783 - 7$.

Wird also der ISBN–10 Code eines Buches eingescannt, so kann leicht überprüft werden, ob sich das eingelesene Prüfzeichen wirklich nach obiger Formel aus den anderen neun Ziffern errechnet. Ist das nicht der Fall, so ist (mindestens) eine der zehn Stellen falsch eingelesen worden. Damit kann also ein einzelner Lesefehler erkannt werden. Eine automatische Korrektur ist jedoch nicht möglich. Die Nummer muss nochmals gescannt werden. Falls mehrere Versuche scheitern, bleibt immer noch die Möglichkeit, den ISBN–10–Code direkt abzutippen.

Der ISBN–13 und EAN–Code:

Inzwischen findet sich auf fast allen Artikeln eine eindeutige Produktkennung, in Europa die dreizehnstellige EAN (**E**uropean **A**rticle **N**umber). Auch Bücher werden heutzutage üblicherweise nach diesem Verfahren gekennzeichnet. In diesem Fall sprechen wir aber von der ISBN–13–Kennzeichnung. Sie ist ähnlich aufgebaut wie die ISBN–10 Nummer, startet allerdings mit den drei Ziffern 978 oder 979 (für die Artikelgruppe Buch). Die Informationsstellen der ISBN–10 aus Beispiel 2.1.5 etwa werden zu den Informationsstellen 978-3-86680-192 der ISBN–13. Die Prüfziffer wird allerdings in diesem Fall anders berechnet. Ist dabei $(a_1, a_2, \ldots, a_{12})$ der informationstragende Teil, so gehen wir vor wie folgt:

1. Bestimme die Summe
$$s = a_1 + 3a_2 + a_3 + 3a_4 + \cdots + a_{11} + 3a_{12} = \sum_{l=1}^{6} a_{2l-1} + \sum_{l=1}^{6} 3 \cdot a_{2l}$$
2. Dividiere s durch 10 mit Rest
$$s = q \cdot 10 + r$$
mit einer ganzen Zahl $r \in \{0, 1, \ldots, 9\}$.
3. Falls $r = 0$ setze $p = 0$, andernfalls setze $p = 10 - r$.

Beispiel 2.1.7. Wir greifen wieder das Buch aus Beispiel 2.1.5 auf. Wie wir schon gesehen haben, sind seine informationstragenden Teile die Ziffernfolge 978-3-86680-192

1. $s = 9 + 3 \cdot 7 + 8 + 3 \cdot 3 + 8 + 3 \cdot 6 + 6 + 3 \cdot 8 + 0 + 3 \cdot 1 + 9 + 3 \cdot 2 = 121$
2. $s = 12 \cdot 10$ Rest 1.
3. $p = 10 - 1 = 9$.

Die ISBN–13 Nummer dieses Buches ist also $978 - 3 - 680 - 08783 - 9$.

Genauso wie der ISBN–10 erkennt ISBN–13 einen Fehler beim Einlesen.

2.1.2 Das Prinzip der Fehlerkorrektur

Um Fehler automatisch korrigieren zu können, reicht offensichtlich eine Prüfsumme, also ein einziges zusätzliches Zeichen nicht aus. Damit lässt sich allenfalls feststellen, ob ein Fehler aufgetreten ist, nicht aber, an welcher Stelle und wie er zu beheben ist. Um die Fehlerstelle zu lokalisieren und den Fehler dann auch zu beheben, benötigen wir mehr Zusatzinformation, d.h. mehr als eine Prüfziffer, wie wir schon am Beispiel 2.1.3 gesehen haben. Wie mit zwei Prüfziffern ein Fehler erkannt, lokalisiert und behoben werden kann, wollen wir nun an einem Beispiel zeigen.

Beispiel 2.1.8. Wir betrachten wieder eine Information a, die in einer Folge von vier Ziffern $a_1, \ldots, a_4$ im Bereich $0, \ldots, 6$ abgelegt ist,

$$a = (a_1, a_2, a_3, a_4) \qquad a_i \in \{0, \ldots, 6\}$$

etwa

$$a = (2, 3, 1, 6)$$

Zur Fehlerkorrektur fügen wir nun zwei Prüfziffern a_5 und a_6 (zwischen 0 und 6) hinzu, und zwar so, dass gilt

$$\begin{array}{ccccccccccc} a_1 & + & a_2 & + & a_3 & + & a_4 & + & a_5 & + & a_6 & \equiv & 0 \bmod 7 \\ a_1 & + & 2a_2 & + & 3a_3 & + & 4a_4 & + & 5a_5 & + & 6a_6 & \equiv & 0 \bmod 7 \end{array}$$

In unserem Beispiel etwa muss dann gelten

$$\begin{array}{ccccccccc} 12 & + & a_5 & + & a_6 & \equiv & 0 \bmod 7 \\ 35 & + & 5a_5 & + & 6a_6 & \equiv & 0 \bmod 7 \end{array}$$

also

$$\begin{array}{rcrcl} a_5 & + & a_6 & \equiv & 2 \bmod 7 \\ 5a_5 & + & 6a-6 & \equiv & 0 \bmod 7 \end{array}$$

Diese Problemstellung wird eindeutig durch die Prüfziffern $a_5 = 5$ und $a_6 = 4$ (im Bereich $0, \ldots, 6$) gelöst, und wir speichern/senden

$$c = (2, 3, 1, 6, 5, 4)$$

Mit diesem Ansatz sind wir nun in der Lage, einen Fehler zu korrigieren. Nehmen wir dazu an, dass wir das Wort

$$m = (2, 2, 1, 6, 5, 4)$$

erhalten haben. Wir bilden zunächst die beiden Prüfsummen

$$\begin{array}{rcccccccccccl} P_1 & = & a_1 & + & a_2 & + & a_3 & + & a_4 & + & a_5 & + & a_6 & \bmod 7 \\ P_2 & = & a_1 & + & 2a_2 & + & 3a_3 & + & 4a_4 & + & 5a_5 & + & 6a_6 & \bmod 7 \end{array}$$

also in unserem Beispiel

$$\begin{array}{rcrcl} P_1 & = & 20 & \equiv & 6 \bmod 7 \\ P_2 & = & 82 & \equiv & 5 \bmod 7 \end{array}$$

Unter der Annahme, dass nur ein Fehler auftritt, haben wir je nach der Stelle, an der der Fehler auftritt ein anderes Verhältnis der beiden Prüfsummen (wenn wir *mod* 7 rechnen):

$$\begin{array}{lrcl} \text{Fehler an der Stelle 1:} & \text{Prüfsumme 2} & \equiv & 1 \cdot \text{ Prüfsumme 1} \\ \text{Fehler an der Stelle 2:} & \text{Prüfsumme 2} & \equiv & 2 \cdot \text{ Prüfsumme 1} \\ \text{Fehler an der Stelle 3:} & \text{Prüfsumme 2} & \equiv & 3 \cdot \text{ Prüfsumme 1} \\ \text{Fehler an der Stelle 4:} & \text{Prüfsumme 2} & \equiv & 4 \cdot \text{ Prüfsumme 1} \\ \text{Fehler an der Stelle 5:} & \text{Prüfsumme 2} & \equiv & 5 \cdot \text{ Prüfsumme 1} \\ \text{Fehler an der Stelle 6:} & \text{Prüfsumme 2} & \equiv & 6 \cdot \text{ Prüfsumme 1} \end{array}$$

In unserem Beispiel sehen wir

$$2 \cdot 6 = 12 \equiv 5 \bmod 7$$

und wir schließen, dass der Fehler an der Stelle 2 aufgetreten ist. Damit haben wir bereits folgenden Rumpfbestandteil der gesendeten Wortes gefunden

$$c^* = (2, x, 1, 6, 5, 4)$$

und lediglich x ist noch nicht klar. Einsetzen in die erste Prüfsumme liefert nun, dass gelten muss

$$2 + x + 1 + 6 + 5 + 4 \equiv 0 \bmod 7$$

also

$$x + 18 \equiv 0 \bmod 7$$

und diese Beziehung wird eindeutig durch $x = 3$ gelöst. Damit haben wir in der Tat

$$c = (2, 3, 1, 6, 5, 4)$$

rekonstruiert, nach Weglassen der Prüfziffern also

$$a = (2, 3, 1, 6)$$

Bemerkung 2.1.1. Es ist wichtig, dass wir Reste bezüglich einer Primzahl (hier 7) bilden, denn nur dann kann die Beziehung der Prüfsummen eindeutig aufgelöst werden.

Bemerkung 2.1.2. Dieses Bespiel erläutert bereits die grundsätzliche Idee der Codierungstheorie:

1. Eine geeignete Anzahl von Prüfzeichen wird durch mathematische Formeln ermittelt.

2. Aus diversen Prüfsummen und ihren Beziehungen zueinander werden die fehlerhaften Stellen eines übertragenen Wortes ermittelt und die Fehler behoben.

Die praktische Umsetzung ist jedoch mit einigen Schwierigkeiten verbunden, wie wir noch sehen werden.

2.2 Grundbegriffe der Codierungstheorie

Zur exakten Formulierung der Problemstellung, mit der wir uns im Rahmen der Codierungstheorie beschäftigen wollen, fixieren wir zunächst einige Grundlagen:

- Grundbausteine der Nachrichten sind **Buchstaben** aus einem fixierten **Alphabet** $\mathbb{A}$ (etwa $\mathbb{A} = \{0, 1\}$), also einer endlichen Menge $\mathbb{A}$ mit q Elementen.

- Die Buchstaben werden zu Gruppen (**Wörtern**) einer fixierten Länge k zusammengefasst. Wir arbeiten also über einem Nachrichtenraum der Gestalt $M = \mathbb{A}^k$ (etwa $M = \{0, 1\}^2$). Versendet werden sollen Folgen von Wörtern.

- Die **Nachrichtenwörter** $m \in M$ werden nach fixierten (üblicherweise linearen) Regeln mit Redundanzen angereichert und in **Codewörter** c einer festen Länge n (über dem selben Alphabet) umgewandelt (etwa $m \in \{0, 1\}^2 \longmapsto c \in \{0, 1\}^5$). Die Codierung ist also eine (injektive) Abbildung $c : M \longrightarrow \mathbb{A}^n$.

Diese Vorschrift heißt **Codierung** und die Menge C der angereicherten Nachrichten $c \in \mathbb{A}^n$ bezeichnet man als Code $C \subseteq \mathbb{A}^n$. Genauer:

Definition 2.2.1. Ein q–**adischer Code** C ist eine nicht–leere Teilmenge $C \subseteq \mathbb{A}^n$.
Die Zahl $k = \log_q(|C|)$ heißt **logarithmische Kardinalität** von C und n heißt **Blocklänge** von C. Die Zahl $R = \frac{k}{n}$ heißt **Informationsrate** von C. Wir nennen C dann einen $[n, k]_q$–Code oder $[n, k]$–Code, falls $\mathbb{A}$ klar ist.

Beispiel 2.2.1. Der in Beispiel 2.1.8 betrachtete Code C ist ein $[6, 4]_7$–Code. Seine Informationsrate ist also $R = \frac{4}{6} = \frac{2}{3}$.

Um aussagen über die Qualität des Codes zu treffen, sind die Zahlen n und k nicht ausreichend, wie die unterschiedliche Qualität der in den Beispielen 2.1.1, 2.1.2 und 2.1.3 zeigt.

Definition 2.2.2. Die **Hammingmetrik** d auf $\mathbb{A}^n$ ist gegeben durch

$$d((a_1, \ldots, a_n), (b_1, \ldots, b_n)) = |\{i \in \{1, \ldots, n\} |\, a_i \neq b_i\}|$$

Bemerkung 2.2.1. Die Hammingmetrik von zwei n-Tupeln a und b bezeichnet die Anzahl der Stellen, an denen sich a und b unterscheiden.

Beispiel 2.2.2. $d((1, 2, 3), (3, 2, 1)) = 2$.

Definition 2.2.3. Ist C ein $[n,k]_q$–Code, so heißt

$$d(C) := \min\{d(a,b)|a,b \in C, a \neq b\}$$

heißt **Minimalabstand** oder **Zuverlässigkeit** von C.

Beispiel 2.2.3. Der Code aus Beispiel 2.1.1 hat Zuverlässigkeit 1, der Code aus Beispiel 2.1.2 hat Zuverlässigkeit 2 und der Code aus Beispiel 2.1.3 hat Zuverlässigkeit 3.

Beispiel 2.2.4. Der Code aus Beispiel 2.1.8 hat Zuverlässigkeit 3.

Bemerkung 2.2.2. Die Zuverlässigkeit $d(C)$ lässt sich wie folgt interpretieren:
Je größer $d(C)$ ist, desto leichter ist es möglich, Fehler bei der Übertragung zu erkennen und zu korrigieren. Wenn sich je zwei Codewörter an vielen Stellen unterscheiden, so ist es sehr unwahrscheinlich, dass ein Codewort als ein anderes interpretiert wird.

Bemerkung 2.2.3. Falls $d(C) = 1$, so ist es nicht möglich, einen Fehler bei der Übertragung eines Wortes sicher zu erkennen. Es gibt zwei Codewörter a und b, die sich nur an einer Stelle unterscheiden, und wird bei der Übertragung von a an genau dieser Stelle fehlerhafterweise der zu b gehörige Buchstabe ausgelesen, so besteht keine Möglichkeit, dies zu erkennen.
Falls $d(C) = 2$, so kann ein einzelner Fehler bei der Übertragung eines Wortes sicher erkannt aber nicht notwendig behoben werden.
Falls $d(C) \geq 3$, so kann ein einzelner Fehler bei der Übertragung eines Wortes sicher erkannt und behoben werden.

Bezeichnung: Ist C ein $[n,k]_q$–Code mit Zuverlässigkeit $d = d(C)$, so nennen wir C auch einen $[n,k,d]_q$–Code.

Bezeichnung: Ist $a \in \mathbb{R}$, so bezeichnen wir mit $\lfloor a \rfloor$ die größte ganze Zahl, die nicht grösser ist als a,

$$\lfloor a \rfloor = \max\{z \in \mathbb{Z} |\, z \leq a\}$$

Beispiel 2.2.5. $\lfloor 5.43 \rfloor = 5$, $\lfloor \pi \rfloor = 3$ und $\lfloor -1.23 \rfloor = -2$.

Definition 2.2.4. Ist C ein $[n,k,d]_q$–Code, so heißt so heißt C ein $\lfloor\frac{d-1}{2}\rfloor$–fehlerkorrigierender Code, und $t = \lfloor\frac{d-1}{2}\rfloor$ heißt die **Fehlerkorrekturschranke** von C.

Beispiel 2.2.6. Der Code C aus Beispiel 2.1.3 ist 1–fehlerkorrigierend.

Beispiel 2.2.7. Der Code C aus Beispiel 2.1.8 ist 1–fehlerkorrigierend.

Bemerkung 2.2.4. Der wesentliche Punkt bei der Arbeit mit Codes ist (neben der Anreicherungsvorschrift) die Frage, wie wir aus einem empfangenen Wort das tatsächliche gesendete Codewort (und damit die ursprüngliche Nachricht) zurückbekommen. Ausgangspunkt ist dabei die Überlegungen, dass wir ein empfangenes Wort a, dass als ein c in der Liste der möglichen Codewörter auftaucht, als genau dieses Codewort c interpretieren werden. Wenn wir ein korrektes Wort empfangen, gehen wir davon aus, dass dieses Wort auch tatsächlich gesendet wurde.
Entsprechend gehen wir davon aus, dass bei einem fehlerhaften Wort a, dass sich von einem zulässigen Codewort c nur an ein oder zwei Stellen unterscheidet, von allen anderen aber an vielen Stellen, in der Tat dieses Wort c gesendet wurde (**Prinzip der Maximum–Likelhood–Decodierung**).
Ganz allgemein:
Wird ein Wort a empfangen, so interpretieren wir a als dasjenige Codewort c für das gilt

$$d(a,c) < d(a,\widetilde{c}) \quad \text{für alle } c \in C$$

falls ein solches c existiert. Falls ein solches c nicht existiert, wird c nicht decodiert sondern als fehlerhaft und unkorrigierbar gekennzeichnet.

Definition 2.2.5. Ein $[n,k,d]_q$–Code C heißt **vollkommen**, wenn es ein $t \in \mathbb{N}$ gibt mit

1. $d(C) = 2t+1$.
2. Für alle $x \in \mathbb{A}^n$ gibt es genau ein $c \in C$ mit $d(a,c) \leq t$.

In diesem Fall heißt C *vollkommener, t–fehlerkorrigierende Code.*

Beliebige allgemeine Codes finden in der modernen Praxis der Datenübertragung kaum noch Verwendung. Üblicherweise nutzt man nur Alphabete $\mathbb{A}$ mit Zusatzstruktur und codes C, die in irgendeiner Weise diese Struktur ausnutzen. Die häufigste Annahme dabei ist, dass $\mathbb{A}$ ein Körper ist und $C \subseteq \mathbb{A}^n$ ein Untervektorraum. Dazu ist es aber zunächst erforderlich, diese Objekte genauer zu studieren.

Kapitel 3

Grundlagen linearer Codes

Um die Frage der Codierung und Decodierung in den Griff zu bekommen, ist es notwendig, (lineare) Zusatzstrukturen auf den Objekten zu betrachten.

3.1 Endliche Körper

Zu Wiederholung: Ein **Körper** ist eine nicht–leere Menge K mit zwei ausgezeichneten Elementen 0 und 1, wobei $0 \neq 1$, und mit zwei inneren Verknüpfungen (also Abbildungen) $+$ und $\cdot$

$$\begin{aligned} + &: K \times K \longrightarrow K, \qquad (a,b) \longmapsto a+b \\ \cdot &: K \times K \longrightarrow K, \qquad (a,b) \longmapsto a \cdot b \end{aligned}$$

so dass gilt

1. $(K,+)$ ist eine kommutative Gruppe mit neutralem Element 0.
2. $(K \setminus \{0\}, \cdot)$ ist eine kommutative Gruppe mit neutralem Element 1.
3. Es gilt das Distributivgesetz, d.h. für alle $a,b,c \in K$ gilt

$$a \cdot (b+c) = a \cdot b + a \cdot c$$

Beispiel 3.1.1. Die Mengen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ (mit den bekannten Additionen und Multiplikationen) sind Körper.

Beispiel 3.1.2. Die Menge $\mathbb{N}$ und $\mathbb{Z}$ mit den bekannten Additionen und Multiplikationen sind keine Körper.

Beispiel 3.1.3. Wir betrachten die Menge $M = \{0, 1\}$ mit Addition und Mulitplikation, die durch die folgenden Tafeln gegeben sind:

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Dann ist $(M, +, \cdot)$ ein Körper.

Bemerkung 3.1.1. Der Körper M aus Beispiel 3.1.3 entspricht $\mathbb{Z}/2\mathbb{Z}$, also den Restklassen von $\mathbb{Z}$ modulo 2.

Beispiel 3.1.4. Ist p eine Primzahl, so ist $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ein Körper.
Dabei ist $\mathbb{Z}/p\mathbb{Z}$ die Menge der Äquivalenzklassen modulo der Äquivalenzrelation $\sim$, die gegeben ist durch

$$m \sim n \iff m - n \text{ ist durch } p \text{ teilbar}$$

und Addition und Multiplikation werden induziert durch Addition und Multiplikation der ganzen Zahlen:
Bezeichnen wir mit $[n]$ die Äquivalenzklasse, die das Element n enthält, so gilt also

$$\begin{aligned} [n] + [m] &= [n + m] \\ [n] \cdot [m] &= [n \cdot m] \end{aligned}$$

Das ist unabhängig von der Wahl der speziellen Repräsentanten der Äquivalenzklassen, d.h. sind $n, n' \in \mathbb{Z}$ mit $[n] = [n']$ und sind $m, m' \in \mathbb{Z}$ mit $[m] = [m']$, so gilt

$$\begin{aligned} [n' + m]' &= [n + m] \\ [n' \cdot m'] &= [n \cdot m] \end{aligned}$$

Damit können Addition, Subtraktion und Multiplikation in $\mathbb{F}_p$ einfach realisiert werden. So gilt etwa in $\mathbb{F}_{13}$:

$$\begin{aligned} [6] + [11] &= 17 \mod 13 = [4] \\ [6] - [11] &= -5 \mod 13 = [8] \\ [6] \cdot [11] &= 36 \mod 13 = [1] \end{aligned}$$

Etwas komplizierter ist die Division bzw. die Bestimmung eines inversen Elements. Das erfolgt in der Regel mit Hilfe des erweiterten euklidischen Algorithmus. In dieser Form liefert der euklidische Algorithmus nämlich nicht nur den größten gemeinesamen Teiler g von zwei ganzen Zahlen a und b, er liefert auch eine Darstellung

$$g = m \cdot a + n \cdot b$$

mit ganzen Zahlen m und n. Wenden wir das an auf die Primzahl p und eine Zahl $a \in \{1, \ldots, p-1\}$ (die ein Element von $\mathbb{F}_p$ repräsentiert), so gilt natürlich

$$1 = \mathrm{ggT}(p, a)$$

denn p ist eine Primzahl. Der euklidische Algorithmus liefert aber nun eine Darstellung

$$1 = m \cdot p + n \cdot a$$

und damit modulo p eine Beziehung

$$[1] = [n \cdot a] = [n] \cdot [a]$$

(da $[m \cdot p] = 0$). Also gilt

$$\frac{1}{[a]} = [n]$$

Das soll hier an zwei Beispielen ausgeführt werden: Wir berechnen im Körper $\mathbb{F}_{79}$ die Elemente

$$a = \frac{1}{42}, \quad b = \frac{7}{40}$$

und drücken die Ergebnisse mit den Standardrepräsentanten $0, 1, \ldots, 78$ aus. Beachten Sie dabei, dass wir in der Regel die Klammern [ ] bei der Darstellung von Elementen von $\mathbb{R}_p$ weglassen werden; aus dem Kontext ist immer klar, ob wir von ganzen Zahlen oder von Restklassen sprechen.
In beiden Fällen ist die Benutzung des erweiterten euklidischen Algorithmuses möglich:

$$\begin{aligned} 79 &= 1 \cdot 42 + 37 \\ 42 &= 1 \cdot 37 + 5 \\ 37 &= 7 \cdot 5 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

Rückrechnung ergibt

$$\begin{aligned} 1 &= 5 - 2 \cdot 2 = 5 - 2 \cdot (37 - 7 \cdot 5) = 15 \cdot 5 - 2 \cdot 37 \\ &= 15 \cdot (42 - 37) - 2 \cdot 37 = 15 \cdot 42 - 17 \cdot 37 = 15 \cdot 42 - 17 \cdot (79 - 42) \\ &= 32 \cdot 42 - 17 \cdot 79 \end{aligned}$$

also

$$1 = 32 \cdot 42 - 17 \cdot 79 \mod 79 = 32 \cdot 42 \mod 79$$

und damit

$$\frac{1}{42} = 32$$

Für b berechnen wir zunächst $\frac{1}{40}$:

$$\begin{aligned} 79 &= 1 \cdot 40 + 39 \\ 40 &= 1 \cdot 39 + 1 \\ 39 &= 39 \cdot 1 + 0 \end{aligned}$$

Rückrechnung ergibt

$$1 = 40 - 1 \cdot 39 = 40 - 1 \cdot (79 - 40) = 2 \cdot 40 - 79$$

also

$$\frac{1}{40} = 2$$

(das kann natürlich auch durch Ausprobieren bestimmt werden), und damit

$$b = 7 \cdot \frac{1}{40} = 7 \cdot 2 = 14$$

Definition 3.1.1. Ein Körper $(K, +, \cdot)$ heißt **endlicher Körper**, wenn $|K| < \infty$.

Beispiel 3.1.5. Die Körper aus den Beispielen 3.1.3 und 3.1.4 sind endliche Körper.

Beispiel 3.1.6. Wir betrachten die Menge $M = \{0, 1, \alpha, \alpha+1\}$ mit Addition und Mulitplikation, die durch die folgenden Tafeln gegeben sind:

$+$	0	1	α	$\alpha+1$
0	0	1	α	$\alpha+1$
1	1	0	$\alpha+1$	α
α	α	$\alpha+1$	0	1
$\alpha+1$	$\alpha+1$	α	1	0

bzw.

$\cdot$	0	1	α	$\alpha+1$
0	0	0	0	0
1	0	1	α	$\alpha+1$
α	0	α	$\alpha+1$	1
$\alpha+1$	0	$\alpha+1$	1	α

Dann ist $(M, +, \cdot)$ ein endlicher Körper mit 4 Elementen, den wir mit $\mathbb{F}_4$ bezeichnen.
Dabei ist allerdings $\mathbb{F}_4$ nicht isomorph zum Ring $\mathbb{Z}/4\mathbb{Z}$, denn in $\mathbb{F}_4$ gilt für jedes Element a:

$$a + a = 0$$

und das ist in $\mathbb{Z}/4\mathbb{Z}$ nicht der Fall.

Der Ring $\mathbb{Z}/4\mathbb{Z}$ ist auch kein Körper, denn in $\mathbb{Z}/4\mathbb{Z}$ gilt

$$2 \cdot 2 = 0$$

also das Produkt von zwei von Null vierschiedenen Elementen liefert den Wert 0, was in einem Körper nie der Fall sein kann. Genauer gilt sogar:

Satz 3.1.1. *Der Ring $\mathbb{Z}/n\mathbb{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Ist K ein (endlicher oder unendlicher) Körper, so schreiben wir kurz

$$n = n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n\text{–mal}}$$

und für $a \in K$ beliebig

$$n \cdot a = \underbrace{a + a + \cdots + a}_{n\text{–mal}}$$

Bemerkung 3.1.2. Ist K ein endlicher Körper, so gibt es immer eine Zahl $n \in \mathbb{N}$, $n > 0$ mit

$$n = 0 \qquad \text{in } K$$

Da K endlich ist, muss es nämlich $r > 0$ und $s > 0$ mit $r \neq s$ geben mit

$$r \cdot 1 = s \cdot 1$$

wobei wir annehmen können, dass $s > r$ (andernfalls vertauschen wir die Rollen von r und s). Dann gilt aber

$$0 = s \cdot 1 - r \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{s-r\text{–mal}}$$

Setzen wir also $n = s - r$, so haben wir das gesuchte n gefunden.

Definition 3.1.2. Ist K ein endlicher Körper, so heißt das kleinste $n \in \mathbb{N}$, $n > 0$ mit

$$n \cdot 1 = 0 \qquad \text{in } K$$

die **Charakteristik** von K.
Ist n die Charakteristik von K, so schreiben wir

$$\text{char}(K) = n$$

Beispiel 3.1.7. Der Körper K aus Beispiel 3.1.3 hat die Charakteristik 2, ebenso der Körper $\mathbb{F}_4$ aus Beispeil 3.1.3.

Beispiel 3.1.8. Der Körper $\mathbb{F}_3$ hat die Charakteristik 3.

Satz 3.1.2. *Ist K ein endlicher Körper, so ist* $\text{char}(K)$ *eine Primzahl.*

Beweis: Wir schreiben $n = \text{char}(K)$ und nehmen an, n ist keine Primzahl, also $n = r \cdot s$ mit echten Teilern r und s. Dann gilt

$$r \cdot 1 \neq 0 \qquad s \cdot 1 \neq 0$$

da $r, s < n$, aber

$$(r \cdot 1) \cdot (s \cdot 1) = rs \cdot 1 = n \cdot 1 = 0$$

Das ist ein Widerspruch zur Nullteilerfreiheit von K, und damit ist n eine Primzahl.

Satz 3.1.3 (Frobenius–Formel)**.** *Ist $p = \text{char}(K)$, so gilt*

$$(a + b)^p = a^p + b^p \qquad \textit{für alle } a, b \in K$$

Beweis: Zunächst gilt ganz allgemein

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} \cdot b + \binom{p}{2} a^{p-2} \cdot b^2 + \cdots + \binom{p}{p-1} a \cdot b^{p-1} + b^p$$

Nun wissen wir, dass

$$\binom{p}{k} = \frac{p!}{k! \cdot (p-k)!} \in \mathbb{N}$$

d.h. $k! \cdot (p-k)! | p!$. Für $1 \leq k \leq p-1$ wird aber weder $k!$ noch $(p-k)!$ von p geteilt. Da aber p Teiler von $p!$ ist, muss notwendig gelten

$$p | \binom{p}{k} \qquad \text{für alle } 1 \leq k \leq p-1$$

Damit gilt aber

$$\binom{p}{k} \cdot 1 = 0 \quad \text{in } k \text{ für } 1 \leq k \leq p-1$$

und damit reduziert sich obiger Ausdruck zu

$$(a+b)^p = a^p + b^p$$

Ist nun $p = \text{char}(K)$, so können wir $\mathbb{F}_p$ als Teilmenge von K betrachten, wenn wir $[n] \in \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit

$$\underbrace{1 + \cdots + 1}_{n\text{–mal}} = n \cdot 1 \in K$$

identifizieren. Wegen $p \cdot 1 = 0$ ist das unabhängig vom Repräsentanten n (zunächst nur für $n > 0$, aber wie man leicht sieht geht das auch für $n < 0$). Dabei gilt offensichtlich

$$\begin{array}{rcccccl} [n] + [m] & = & [n+m] & \equiv & (n+m) \cdot 1 & = & n \cdot 1 + m \cdot 1 \\ [n] \cdot [m] & = & [n \cdot m] & \equiv & (n \cdot m) \cdot 1 & = & (n \cdot 1) \cdot (m \cdot 1) \end{array}$$

Dadurch wird $\mathbb{F}_p$ also zu einem Teilkörper (Unterkörper) von K.

Definition 3.1.3. Ist K ein endlicher Körper der Charakteristik $p > 0$, so heißt $\mathbb{F}_p$ der Primkörper von K.

Wir betrachten einen (endlichen) Körper K und eine nicht–leere Menge V.

Definition 3.1.4. Ein K–Vektorraum $(V, +, \cdot)$ ist eine nicht–leere Menge V zusammen mit einer Vektoraddition

$$V \times V \longrightarrow V, \quad (v, w) \longmapsto v + w$$

und einer Skalarmultiplikation

$$K \times V \longrightarrow V, \quad (r, v) \longmapsto r \cdot v$$

so dass für alle Vektoren $u, v, w \in V$ und für $r, s \in K$ gilt

V1: $(u + v) + w = u + (v + w)$

V2: $v + w = w + v$.

V3: Es gibt ein Element $0 \in V$ mit $v + 0 = v$.

V4: Zu jedem $v \in V$ gibt es ein $-v \in V$ mit $v + (-v) = 0$.

V5: $(r \cdot s) \cdot v = r \cdot (s \cdot v)$.

V6: $r \cdot (v + w) = r \cdot v + r \cdot w$.

V7: $(r + s) \cdot v = r \cdot v + s \cdot v$.

V8: $1 \cdot v = v$.

Beispiel 3.1.9. Für jedes $t \in \mathbb{N}$ ist $M = K^t$ mit komponentenweise definierter Addition und Skalarmultiplikation

$$\begin{aligned} (v_1, v_2, \ldots, v_t) + (w_1, w_2, \ldots, w_t) &= (v_1 + w_1, v_2 + w_2, \ldots, v_t + w_t) \\ r \cdot (v_1, v_2, \ldots, v_t) &= (r \cdot v_1, r \cdot v_2, \ldots, r \cdot v_t) \end{aligned}$$

ein K–Vektorraum.

Beispiel 3.1.10. Ist M eine beliebige nichtleere Menge, und ist

$$V = \mathrm{Abb}(M, K) = \{f : M \longrightarrow K\}$$

die Menge der Abbildungen von M nach K, so wird V zum K–Vektorraum mit der Vektoraddition gegeben durch

$$f + g : M \longrightarrow K, \quad m \longmapsto f(m) + g(m)$$

für $f, g \in V$ und mit der Skalarmultiplikation gegeben durch

$$r \cdot f : M \longrightarrow K, \quad m \longmapsto r \cdot f(m)$$

für $r \in K$ und $f \in V$.

Bemerkung 3.1.3. Begriffe wie *Erzeugendensystem*, *lineare Unabhängigkeit* oder *Basis* können für Vektorraäume über beliebigen Körpern definiert und untersucht werden. Die Sätze aus der linearen Algebra für Vektorräume (über den reellen oder komplexen) Zahlen gelten hier genauso. Speziell besitzt jeder K–Vektorraum eine Basis und alle Basen eines K–Vektorraums V haben die gleiche Länge (d.h. die gleiche Anzahl von Elementen). Diese Länge bezeichnen wir mit $\dim(V)$ und nennen sie die *Dimension des K–Vektorraums V*.

Wir betrachten nun einen Körper K und einen K–Vektorraum V.

Definition 3.1.5. Ein K–Untervektorraum (oder kurz Untervektorraum) $U \subseteq V$ ist eine Teilmenge $U \subseteq V$ mit den folgenden Eigenschaften:

1. U ist nicht leer.
2. Für $u, v \in U$ ist $u + v \in U$.
3. Für $u \in U$ und $r \in K$ ist $r \cdot u \in U$.

Beispiel 3.1.11. Für jedes $n > 0$ ist

$$U = \{x = (r, r, \ldots, r) |\ r \in K\} \subseteq K^n$$

ein K–Untervektorraum von K^n

Beispiel 3.1.12. Die Teilmenge

$$C = \{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\} \subseteq \mathbb{F}_2^3$$

ist ein $\mathbb{F}_2$–Untervektorraum von $\mathbb{F}_2^3$.

1. Offensichtlich ist C nicht leer.
2. Für $u, v \in C$ kann durch direktes Nachrechnen überprüft werden, dass $u + v \in C$.
3. Da $\mathbb{F}_2 = \{0, 1\}$ ist nur noch zu überprüfen, ob für $u \in C$ sowohl $1 \cdot u \in C$ als auch $0 \cdot u \in C$. Beides ist jedoch klar.

Bemerkung 3.1.4. Ein K–Untervektorraum $U \subseteq V$ ist selbst wieder ein Vektorraum (mit den Operationen von V). Daher können wir auch bei Untervektorräumen von Basen und Dimension sprechen.

Beispiel 3.1.13. Der Vektor $v = (1, 1, \ldots, 1) \in K^n$ bildete eine Basis des Untervektorraums $U \subseteq K^n$ aus Beispiel 3.1.11. Also gilt $\dim_K(U) = 1$.
Die Vektoren $u = (1, 1, 0)$ und $v = (1, 0, 1)$ bilden eine Basis des Untervektorraums $C \subseteq \mathbb{F}_2^3$ aus Beispiel 3.1.12. Also gilt $\dim_{\mathbb{F}_2}(C) = 2$.

Bemerkung 3.1.5. Ist K ein endlicher Körper der Charakteristik $p > 0$, so ist K ein $\mathbb{F}_p$–Vektorraum. Wir wissen bereits, dass $\mathbb{F}_p \subseteq K$ ein Unterkörper ist. Die Vektoraddition von K ist dabei die übliche Addition im Körper K, und die Skalarmultiplikation entsteht durch Einschränkung der Körpermultiplikation auf $\mathbb{F}_p$, d.h. $[n] \cdot r = (n \cdot 1) \cdot r$.
Damit gilt insbesondere, dass es ein $l \in \mathbb{N}$ gibt, so dass

$$|K| = p^l$$

und dabei ist l die Dimension von K als $\mathbb{F}_p$–Vektorraum.

Ausser den Körpern $\mathbb{F}_p$ kennen wir bis jetzt nur einen endlichen Körper mit 4 Elementen. Der folgende Satz liefert uns nicht nur eine Fülle solcher Körper sondern auch noch eine Methodik, deren Arithmetik mit Hilfe der Arithmetik der Körper $\mathbb{F}_p$ zu beschreiben.

Satz 3.1.4. *Ist $q = p^l$ so gibt es einen (bis auf Isomorphie eindeutigen) Körper $\mathbb{F}_q$ mit q Elementen. Dabei hat $\mathbb{F}_q$ die Charakteristik $p > 0$ und es gibt ein $\alpha \in F_q$ so dass $1, \alpha, \alpha^2, \ldots, \alpha^{l-1}$ ist eine Basis von K als $\mathbb{F}_p$–Vektorraum ist. Insbesondere haben wir also eine Relation*

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

Definition 3.1.6. Eine Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

heißt **definierende Relation** des Körpers $\mathbb{F}_q$.

Regel 3.1.5. *Mit Hilfe einer definierenden Relation lassen sich die Addition und die Multiplikation im Körper $\mathbb{F}_q$ vollständig beschreiben:*

- *Ist $x \in \mathbb{F}_q$ beliebig, so gibt es eindeutig bestimmte Elemente $a_0, \ldots, a_{l-1} \in \mathbb{F}_p$ mit*
$$x = a_{l-1} \cdot \alpha^{l-1} + \cdots + a_1 \cdot \alpha + a_0$$
- *Sind $x = a_{l-1} \cdot \alpha^{l-1} + \cdots + a_1 \cdot \alpha + a_0$ und $y = b_{l-1} \cdot \alpha^{l-1} + \cdots + b_1 \cdot \alpha + b_0$ zwei Elemente in $\mathbb{F}_q$, so gilt*
$$x + y = (a_{l-1} + b_{l-1}) \cdot \alpha^{l-1} + (a_{l-2} + b_{l-2}) \cdot \alpha^{l-2} + \cdots + (a_1 + b_1) \cdot \alpha + a_0 + b_0$$
- *Die Multiplikation in $\mathbb{F}_q$ ist gegeben durch*
$$\alpha^i \cdot \alpha^j = \alpha^{i+j}$$
unter Ausnutzung der definierenden Relation, d.h. immer wenn $i + j \geq l$, so wird ein α^l durch $r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$ ersetzt.

Beispiel 3.1.14. Der Körper $M = \mathbb{F}_4$ aus Beispeil 3.1.6 wird gegeben durch die defnierende Relation

$$\alpha^2 = \alpha + 1$$

Beispiel 3.1.15. Der Körper $\mathbb{F}_8$ kann definiert werden durch die Relation

$$\alpha^3 = \alpha + 1$$

so dass also

$$\mathbb{F}_8 = \{0, 1, \alpha, \alpha+1, \alpha^2, \alpha^2+1, \alpha^2+\alpha, \alpha^2+\alpha+1\}$$

mit den Rechenvorschriften

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

und

$\cdot$	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Dabei ergeben sich die Formeln etwa wie folgt

$$\begin{aligned}
\alpha^2 \cdot (\alpha^2+1) &= \alpha^4 + \alpha^2 \\
&= \alpha \cdot \alpha^3 + \alpha^2 \\
&= \alpha \cdot (\alpha+1) + \alpha^2 \\
&= \alpha^2 + \alpha + \alpha^2 \\
&= 2 \cdot \alpha^2 + \alpha \\
&= \alpha
\end{aligned}$$

wobei wir auch noch ausgenutzt haben, dass $2 = 0$ im Primkörper $\mathbb{F}_2$.

Beispiel 3.1.16. Der Körper $\mathbb{F}_8$ kann auch definiert werden durch die Relation

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

Eine definierende Relation ist also nicht eindeutig. Allerdings kann eine definierende Relation auch nicht beliebig sein, denn die Relation

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

etwa definiert den Körper $\mathbb{F}_8$ nicht. Entscheidend ist dabei immer, ob durch die Relation eine Multiplikation erklärt wird, für die gilt

$$x \cdot y \neq 0 \quad \text{wenn immer } x \neq 0 \text{ und } y \neq 0$$

Bei der Relation $\alpha^3 = \alpha^2 + 1$ ist das der Fall, bei der Relation $\alpha^3 = \alpha^2 + \alpha + 1$ jedoch nicht, denn bei dieser Relation gilt

$$\begin{aligned}(\alpha + 1) \cdot (\alpha^2 + 1) &= \alpha^3 + \alpha^2 + \alpha + 1 \\ &= \alpha^2 + \alpha + 1 + \alpha^2 + \alpha + 1 \\ &= 0\end{aligned}$$

In diesem Fall wäre also das Produkt der beiden von Null verschiedenen Elemente $\alpha + 1$ und $\alpha^2 + 1$ gleich 0, was in einem Körper nicht sein kann.

Bemerkung 3.1.6. Die Relation

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

beschreibt genau dann den Körper $\mathbb{F}_q$ (mit $q = p^l$), wenn sie **irreduzibel** ist: Dazu schreiben wir zunächst die Relation als

$$\alpha^l - r_{l-1}\alpha^{l-1} - \cdots - r_1 \cdot \alpha - r_0$$

ersetzen die α durch eine Polynomvariable X und erhalten

$$f(X) = X^l - r_{l-1} \cdot X^{l-1} - \cdots - r_1 \cdot X - r_0 \quad \in \mathbb{F}_p[X]$$

Die Relation heißt dann irreduzibel, wenn es keine Polynome $g(X)$ und $h(X)$ vom Grad höchstens $l - 1$ gibt mit

$$f(X) = g(X) \cdot h(X)$$

(wobei das Polynomprodukt über $\mathbb{F}_p$ zu berechnen ist).

Definition 3.1.7. Ist

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

eine Relation, die den Körper $\mathbb{F}_q$ (mit $q = p^l$) beschreibt und ist

$$f(X) = X^l - r_{l-1} \cdot X^{l-1} - \cdots - r_1 \cdot X - r_0 \quad \in \mathbb{F}_p[X]$$

das (wie oben) daraus abgeleitete Polynom, so heißt $f(X)$ **Minimalpolynom** von $\mathbb{F}_q/\mathbb{F}_p$.

Für Relationen niedrigen Grades lässt sich sehr leicht überprüfen, ob eine Relation die definierende Relation eines Körpers ist:
Eine Relation

$$\alpha^2 = r_0 + r_1\alpha$$

definiert genau dann den Körper $\mathbb{F}_{p^2}$, wenn das Polynom $f(X) = X^2 - r_1X - r_0$ keine Nullstelle in $\mathbb{F}_p$ hat. Die Beziehung $\alpha^2 = \alpha + 1$ definiert daher $\mathbb{F}_4$ über $\mathbb{F}_2$, denn für $f(X) = X^2 + X + 1$ gilt:

$$f(0) = 1 \neq 0, \quad f(1) = 1 \neq 0$$

Dagegen definiert $\alpha^2 = 1$, den Körper $\mathbb{F}_4$ über $\mathbb{F}_2$ nicht, denn für $f(X) = X^2 + 1$ gilt:

$$f(1) = 0$$

Eine Relation

$$\alpha^3 = r_0 + r_1\alpha + r_2\alpha^2$$

definiert genau dann den Körper $\mathbb{F}_{p^3}$, wenn das Polynom $f(X) = X^3 - r_2X^2r_1X - r_0$ keine Nullstelle in $\mathbb{F}_p$ hat. Die Beziehung $\alpha^3 = \alpha^2 + 1$ definiert daher $\mathbb{F}_8$ über $\mathbb{F}_2$, denn für $f(X) = X^3 + X^2 + 1$ gilt:

$$f(0) = 1 \neq 0, \quad f(1) = 1 \neq 0$$

Dagegen definiert $\alpha^3 = \alpha^2 + \alpha + 1$, den Körper $\mathbb{F}_8$ über $\mathbb{F}_2$ nicht, denn für $f(X) = X^3 + X^2 + X + 1$ gilt:

$$f(1) = 0$$

Beispiel 3.1.17. Eine Relation

$$\alpha^4 = r_0 + r_1\alpha + r_2\alpha^2 + r_3\alpha^3$$

definiert genau dann den Körper $\mathbb{F}_{p^4}$, wenn das Polynom $f(X) = X^4 - r_3X^3 - r_2X^2 r_1X - r_0$ keine Nullstelle in $\mathbb{F}_p$ hat und keinen quadratischen Faktor über $\mathbb{F}_p$ abspaltet.
Damit definiert etwa die Relation $\alpha^4 = \alpha + 1$ den Körper $\mathbb{F}_{16}$, denn für das Polynom $f(X) = X^4 + X + 1$ gilt:

1. $f(X)$ hat keine Nullstelle in $\mathbb{F}_2$, denn $f(0) = 1$, $f(1) = 1$.

2. $f(X)$ hat keinen quadratischen Teiler über $\mathbb{F}_2$. Als möglicher Teiler kommt dabei nur $q(X) = X^2 + X + 1$ in Frage, denn alle anderen quadratischen Poylnome über $\mathbb{F}_2$ haben eine Nullstelle. Es gilt jedoch

$$f(X) \div q(X) = X^2 + X \quad \text{Rest } 1$$

Die Relation $\alpha^4 = \alpha^3 + \alpha + 1$ dagegen definiert $\mathbb{F}_{16}$ nicht, denn das Polynom $f(X) = X^4 + X^3 + X + 1$ erfüllt $f(1) = 0$, hat also eine Nullstelle in $\mathbb{F}_2$.
Ebenso definiert die Relation $\alpha^4 = \alpha^2 + 1$ den Körper $\mathbb{F}_{16}$ nicht, den das Polynom $f(X) = X^4 + X^2 + 1$ hat zwar keine Nullstelle in $\mathbb{F}_2$ ($f(0) = 1$ und $f(1) = 1$), aber

$$f(X) = (X^2 + X + 1) \cdot (X^2 + X + 1)$$

dh. $f(X)$ hat einen quadratischen Teiler.

Bemerkung 3.1.7. Der Beweis von Satz 3.1.4, insbesondere der Nachweis der Existenz und der Eindeutigkeit (in einem geeigneten Sinn) sowie der Existenz eines Elements α wie behauptet übersteigt den Rahmen dieser Veranstaltung. Ist jedoch ein Element α gefunden, so dass $1, \alpha, \ldots, \alpha^{l-1}$ eine $\mathbb{F}_p$–Basis von $\mathbb{F}_q$ ist, so gibt es, da ja $\alpha^l \in \mathbb{F}_q$, notwendigerweise $r_0, \ldots, r_{l-1} \in \mathbb{F}_p$ mit

$$\alpha^l = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{l-1}\alpha^{l-1}$$

da sich α^l mit Hilfe der Basis darstellen lassen muss. Die Regeln für die Addition und die Multiplikation ergeben sich daraus und aus den Vektorraumeigenschaften.

Bemerkung 3.1.8. Obwohl es (bis auf Isomorphie) nur einen Körper mit $q = p^l$ Elementen gibt, kann dieser in der Regel durch viele definierende Relation beschrieben werden. Die Umrechnung von einer Darstellung in eine andere (also der Wechsel von einem α zu einem anderen) ist dabei nicht offensichtlich.

Wir betrachten nun wieder einen Körper $\mathbb{F}_q$ mit $q = p^l$ Elementen.

Satz 3.1.6. *Der Körper $\mathbb{F}_q$ kann beschrieben werden durch ein α mit definierender Relation*

$$\alpha^l = r_{l-1} \cdot \alpha^{l-1} + r_{l-2} \cdot \alpha^{l-2} + \cdots + r_1 \cdot \alpha + r_0$$

so dass

$$\mathbb{F}_q \setminus \{0\} = \{\alpha, \alpha^2, \ldots, , \alpha^{q-2}, \alpha^{q-1} = 1\}$$

Auch ein Beweis dieses Aussage übersteigt den Rahmen dieser Veranstaltung.

Der wichtigste Körper für die digitale Datenverarbeitung ist der Körper $\mathbb{F}_{256}$ mit $2^8 = 256$ Elementen (also mit den Bytes als Elementen). Dieser Körper kann beschrieben werden durch die Relation

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

Wir überlassen es dem Leser, sich davon zu überzeugen, dass das Polynom

$$f(X) = X^8 - X^4 - X^3 - X^2 - 1 = X^8 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$$

irreduzibel ist, sich also nicht als Produkt von zwei Polynomen schreiben lässt. Für diese Relation gilt auch

$$\mathbb{F}_{256} \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^{254}, \alpha^{255} = 1\}$$

Für Speicherung der Elemente und die Darstellung der Arithmetik beschreiben wir ein Element $x \in \mathbb{F}_{256}$ als 8–Tupel

$$x = (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \in \mathbb{F}_2^8$$

von Binärzahlen $b_i \in \mathbb{F}_2$ (beachten Sie dabei die Reihenfolge von b_7 bis b_0) und identifizieren dieses für die Rechnung mit

$$x = b_7\alpha^7 + b_6\alpha^6 + \cdots + b_1\alpha + b_0$$

Damit gilt also etwa

$$\begin{aligned} 1 &= (0,\,0\,,0\,,0\,,0\,,0\,,0\,,1) \\ \alpha &= (0,\,0\,,0\,,0\,,0\,,0\,,1\,,0) \\ \alpha^2 &= (0,\,0\,,0\,,0\,,0\,,1\,,0\,,0) \\ &\vdots \\ \alpha^7 &= (1,\,0\,,0\,,0\,,0\,,0\,,0\,,0) \end{aligned}$$

und, aufgrund der definierenden Relation

$$\alpha^8 = (0,\,0\,,0\,,1\,,1\,,1\,,0\,,1)$$

Beispiel 3.1.18. Wir betrachten die beiden Elemente $x, y \in \mathbb{F}_{256}$ mit

$$x = (1,\,1\,,0\,,1\,,1\,,1\,,0\,,1), \qquad y = (0\,,0\,,1\,,1\,,0\,,0\,,1\,,1)$$

Hierfür gilt

$$\begin{aligned} x + y &= (1+0, 1+0, 0+1, 1+1, 1+0, 1+0, 0+1, 1+1) \\ &= (1,\,1,\,1,\,0,\,1,\,1,\,1,\,0) \end{aligned}$$

und

$$\begin{aligned} x \cdot y &= ((1,\,1,\,0,\,1,\,1,\,1,\,0,\,1) \cdot (0,\,0,\,1,\,1,\,0,\,0,\,1,\,1) \\ &= (1+\alpha^2+\alpha^3+\alpha^4+\alpha^6+\alpha^7) \cdot (1+\alpha+\alpha^4+\alpha^5) \\ &= 1+\alpha+\alpha^4+\alpha^5+\alpha^2+\alpha^3+\alpha^6+\alpha^7+\alpha^3+\alpha^4+\alpha^7+\alpha^8+\alpha^4 \\ &\quad +\alpha^5+\alpha^8+\alpha^9+\alpha^6+\alpha^7+\alpha^{10}+\alpha^{11}+\alpha^7+\alpha^8+\alpha^{11}+\alpha^{12} \\ &= 1+\alpha+\alpha^2+\alpha^4+\alpha^8+\alpha^9+\alpha^{10}+\alpha^{12} \\ &= 1+\alpha+\alpha^2+\alpha^4+\alpha^4+\alpha^3+\alpha^2+1+\alpha\cdot(\alpha^4+\alpha^3+\alpha^2+1) \\ &\quad +\alpha^2\cdot(\alpha^4+\alpha^3+\alpha^2+1)+\alpha^4\cdot(\alpha^4+\alpha^3+\alpha^2+1) \\ &= 1+\alpha+\alpha^2+\alpha^4+\alpha^4+\alpha^3+\alpha^2+1+\alpha^5+\alpha^4+\alpha^3+\alpha \\ &\quad +\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha^8+\alpha^7+\alpha^6+\alpha^4 \\ &= \alpha^2+\alpha^4+\alpha^7+\alpha^8 \\ &= \alpha^2+\alpha^4+\alpha^7+\alpha^4+\alpha^3+\alpha^2+1 \\ &= 1+\alpha^3+\alpha^7 \\ &= (1,\,0,\,0,\,0,\,1,\,0,\,0,\,1) \end{aligned}$$

Für die arithmetische Behandlung der Multiplikation wichtig ist die folgende Formel

$$\begin{aligned}\alpha \cdot & (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \\ &= (0,\, 0\,, 0\,, 0\,, 0\,, 0\,, 1\,, 0) \cdot (b_7, b_6, b_5, b_4, b_3, b_2, b_1, b_0) \\ &= (b_6, b_5, b_4, b_3, b_2, b_1, b_0,\, 0) + b_7 \cdot (0,\, 0\,, 0\,, 1\,, 1\,, 1\,, 0\,, 1)\end{aligned}$$

Eine entscheidende Eigenschaft eines Körpers K ist, dass es zu jedem Element $r \in K \setminus \{0\}$ ein Inverses s bezüglich der Multiplikation gibt, also ein Element $s \in K \setminus \{0\}$ mit $r \cdot s = 1$. Für dieses Element s schreiben wir auch r^{-1} und nennen es das inverse Element zu r. In endlichen Körpern kann dieses inverse Element am einfachsten durch Potenzbilden gefunden werden:

Satz 3.1.7. *Ist K ein endlicher Körper mit $q = p^n$ Elementen, und ist $r \in K \setminus \{0\}$, so gilt*

$$r^{q-1} = 1$$

Also gilt speziell für das Element $s = r^{q-2}$:

$$r \cdot s = 1$$

d.h.

$$r^{-1} = r^{q-2}$$

Beweis: Da K ein Körper (mit q Elementen) ist, ist $K \setminus \{0\}$ bezüglich der Multiplikation eine Gruppe der Ordnung $q-1$. Nach den allgemeinen Regeln aus der Gruppentheorie teilt damit die Ordnung eines jeden Elements aus $K \setminus \{0\}$ die Ordnung dieser Gruppe, also $q-1$, und daraus ergibt sich diese Aussage.

Beispiel 3.1.19. Wir betrachten den Körper $K = \mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha^2 + 1$ und das Element

$$r = \frac{1}{\alpha + 1} = (0, 1, 1)^{-1}$$

Dann gilt

$$r = (\alpha+1)^{8-2} = (\alpha+1)^6 = ((\alpha+1)^2)^2 \cdot (\alpha+1)^2$$

wobei

$$\begin{array}{rcl} (\alpha+1)^2 & = & \alpha^2+1 \\ ((\alpha+1)^2)^2 & = & (\alpha^2+1)^2 \quad = \quad \alpha^4+1 \\ & = & \alpha^3+\alpha+1 \quad = \quad \alpha^2+1+\alpha+1 \\ & = & \alpha^2+\alpha \end{array}$$

also

$$\begin{array}{rcll} r & = & (\alpha^2+\alpha)\cdot(\alpha^2+1) & = \quad \alpha^4+\alpha^2+\alpha^3+\alpha \\ & = & \alpha^3+\alpha+\alpha^2+\alpha^2+1+\alpha & = \quad \alpha^3+1 \\ & = & \alpha^2+1+1 & = \quad \alpha^2 \\ & = & (1,0,0) & \end{array}$$

Wird die Arithmetik eines endlichen Körpers sehr oft ausgenutzt und sind viele Gleichungssysteme zu lösen, so kann die Berechnung der inversen Elemente durch Ausnutzung von Satz 3.1.6 weiter stark vereinfacht werden. Die Relation $\alpha^3 = \alpha^2 + 1$, die den Körper $\mathbb{F}_8$ definiert etwa erfüllt

$$\mathbb{F}_8 \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^7 = 1\}$$

und eine einfache Rechnung ergibt

$$\begin{array}{rcl} \alpha & = & \alpha \\ \alpha^2 & = & \alpha^2 \\ \alpha^3 & = & \alpha^2+1 \\ \alpha^4 & = & \alpha^2+\alpha+1 \\ \alpha^5 & = & \alpha+1 \\ \alpha^6 & = & \alpha^2+\alpha \\ \alpha^7 & = & 1 \end{array}$$

Daraus lesen wir nun unmittelbar ab

$$\frac{1}{\alpha+1} = \frac{1}{\alpha^5} = \frac{\alpha^7}{\alpha^5} = \alpha^2$$

Auch Division lassen sich damit leicht durchführen, etwa

$$\frac{\alpha+1}{\alpha^2+1} = \frac{\alpha^5}{\alpha^3} = \alpha^2$$

oder

$$\frac{\alpha^2+\alpha+1}{\alpha^2+\alpha} = \frac{\alpha^4}{\alpha^6} = \frac{1}{\alpha^2} = \frac{\alpha^7}{\alpha^2} = \alpha^5 = \alpha+1$$

Beispiel 3.1.20. Wir betrachten wieder den Körper $K = \mathbb{F}_8$, diesmal aber gegeben durch die Relation $\alpha^3 = \alpha + 1$. Auch hier gilt

$$\mathbb{F}_8 \setminus \{0\} = \{\alpha, \alpha^2, \ldots, \alpha^7 = 1\}$$

und in diesem Fall rechnen wir nach, dass

$$\begin{aligned}
\alpha &= \alpha \\
\alpha^2 &= \alpha^2 \\
\alpha^3 &= \alpha + 1 \\
\alpha^4 &= \alpha^2 + \alpha \\
\alpha^5 &= \alpha^2 + \alpha + 1 \\
\alpha^6 &= \alpha^2 + 1 \\
\alpha^7 &= 1
\end{aligned}$$

Daher gilt in dieser Situation

$$\frac{1}{\alpha + 1} = \frac{1}{\alpha^3} = \frac{\alpha^7}{\alpha^3} = \alpha^4 = \alpha^2 + \alpha$$

und für die Division erhalten wir

$$\frac{\alpha + 1}{\alpha^2 + 1} = \frac{\alpha^3}{\alpha^6} = \frac{1}{\alpha^3} = \frac{\alpha^7}{\alpha 3} = \alpha^4 = \alpha^2 + \alpha$$

oder

$$\frac{\alpha^2 + \alpha + 1}{\alpha^2 + \alpha} = \frac{\alpha^5}{\alpha^4} = \alpha$$

Die explizite Arithmetik eines endlichen Körpers hängt also stark davon ab, welches α bzw. welche Erzeugerrelation wir wählen. Zu beachten ist aber, dass der Körper insgesamt eindeutig ist, dass es also nur einen Körper mit acht Elementen gibt (wenn auch mit unterschiedlichen Beschreibungen). Definieren wir etwa $\mathbb{F}_8$ durch $\alpha^3 = \alpha + 1$, so gilt für das Element $\widetilde{\alpha} = \alpha^3$ in diesem Körper die Relation

$$\widetilde{\alpha}^3 = \alpha^9 = \alpha^2 = (\alpha^2 + 1) + 1 = \alpha^6 + 1 = \widetilde{\alpha}^2 + 1$$

Das Element $\widetilde{\alpha} = \alpha^3$ erfüllt also die Relation $\widetilde{\alpha}^3 = \widetilde{\alpha}^2 + 1$ in diesem Körper und definiert ebenfalls $\mathbb{F}_8$.

Beispiel 3.1.21. Im Körper $\mathbb{F}_8$ hat die Einheitengruppe $E(\mathbb{F}_8) = \mathbb{F}_8 \setminus \{0\}$ genau 7 Elemente, ist also zyklisch von Primzahlordnung. Daraus folgt, dass jedes Element $a \in E(\mathbb{F}_8)\setminus\{1\}$ die Einheitengruppe $E(\mathbb{F}_8)$ erzeugt und hieraus wiederum lässt sich leicht ableiten, dass jedes Element $a \in E(\mathbb{F}_8) \setminus \{1\}$ entweder die Relation $a^3 = a + 1$ oder $a^3 = a^2 + 1$ erfüllt, also den Körper $\mathbb{F}_8$ erzeugt, dh. jedes Element $a \in \mathbb{F}_8$, $a \neq 0, 1$ erzeugt sowohl den Körper $\mathbb{F}_8$ als auch die zyklisch Gruppe $E(\mathbb{F}_8)$.
Das ist nicht bei allen Körpern so. Betrachten wir etwa den Körper $\mathbb{F}_{16}$ mit der Relation $\alpha^4 = \alpha + 1$, so gilt hierfür:

$$\begin{aligned}
\alpha^1 &= \alpha & \qquad \alpha^9 &= \alpha^3 + \alpha \\
\alpha^2 &= \alpha^2 & \alpha^{10} &= \alpha^2 + \alpha + 1 \\
\alpha^3 &= \alpha^3 & \alpha^{11} &= \alpha^3 + \alpha^2 + \alpha \\
\alpha^4 &= \alpha + 1 & \alpha^{12} &= \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^5 &= \alpha^2 + \alpha & \alpha^{13} &= \alpha^3 + \alpha^2 + 1 \\
\alpha^6 &= \alpha^3 + \alpha^2 & \alpha^{14} &= \alpha^3 + 1 \\
\alpha^7 &= \alpha^3 + \alpha + 1 & \alpha^{15} &= 1 \\
\alpha^8 &= \alpha^2 + 1
\end{aligned}$$

sodass also α auch die Einheitengruppe erzeugt,

$$E(\mathbb{F}_{16}) = \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{15}\}$$

Betrachten wir dagegen $\beta = \alpha^3$, so gilt hierfür

$$\begin{aligned}
\beta^4 = \alpha^{12} &= \alpha^3 + \alpha^2 + \alpha + 1 \\
&= (\alpha^3 + \alpha) + (\alpha^3 + \alpha^2) + \alpha^3 + 1 \\
&= \alpha^9 + \alpha^6 + \alpha^3 + 1 \\
&= \beta^3 + \beta^2 + \beta + 1
\end{aligned}$$

Also erfüllt β die Relation

$$\beta^4 = \beta^3 + \beta^2 + \beta + 1$$

und damit definiert β den Körper $\mathbb{F}_{16}$, denn man überzeugt sich leicht, dass das Polynom $f(X) = X^4 + X^3 + X^2 + X + 1$ weder eine Nullstelle in $\mathbb{F}_2$ noch einen quadratische Teiler über $\mathbb{F}_2$ hat (vergleiche Beispiel 3.1.17). Allerdings gilt

$$\beta^5 = \left(\alpha^3\right)^5 = \alpha^{15} = 1$$

dh. das Element β hat die Ordnung 5 und erzeugt daher die Einheitengruppe nicht (die ja die Ordnung 15 hat).
Betrachten wir das Element $\gamma = \alpha^2 + \alpha \ (= \alpha^5)$, so gilt hierfür

$$\gamma^3 = \left(\alpha^5\right)^3 = \alpha^{15} = 1$$

also hat γ die Ordnung 3 und erzeugt die Einheitengruppe daher ebenfalls nicht. Ferner ist

$$\begin{aligned} \gamma^2 = \alpha^{10} &= \alpha^2 + \alpha + 1 \\ &= \gamma + 1 \end{aligned}$$

Also erfüllt γ die Relation

$$\gamma^2 = \gamma + 1$$

und damit erzeugt γ den Körper $\mathbb{F}_4$ (als Unterkörper von $\mathbb{F}_{16}$), dh. die Teilmenge

$$M = \{0, \gamma, \gamma^2, \gamma^3 = 1\} \subseteq \mathbb{F}_{16}$$

ist selbst schon ein Körper, und zwar der Körper $\mathbb{F}_4$ mit 4 Elementen.

Bemerkung 3.1.9. In den Körpern $\mathbb{F}_p$ mit einer Primzahl p haben wir das inverse Element mithilfe des erweiterten euklidischen Algorithmus berechnet. Dieses Verfahren kann auf Körper $\mathbb{F}_q$ wie folgt verallgemeinert werden:
Wir nehmen an, dass $\mathbb{F}_q$ durch die Relation

$$\alpha^l = r_0 + r_1\alpha + r_2\alpha^2 + \cdots + r_{l-1}\alpha^{l-1}$$

beschreiben wird und bilden daraus das Minimalpolynom

$$f(X) = X^l - r_{l-1} \cdot X^{l-1} - \cdots - r_1 \cdot X - r_0 \quad \in \mathbb{F}_p[X]$$

der Körpererweiterung $\mathbb{F}_q/\mathbb{F}_p$.
Ist nun $a = a_0 + a_1\alpha + \cdots + a_{l-1}\alpha^{l-1}$ ein Element von $\mathbb{F}_q \setminus \{0\}$, so betrachten wir das zugehörige Polynom

$$a(X) = a_{l-1} \cdot X^{l-1} + \cdots + a_1 \cdot X + a_0$$

Da wir im Polynomring, genauso wie in $\mathbb{Z}$ (Polynom-)Division mit Rest durchführen können, können wir den (erweiterten) euklidischen Algorithmus

für die Polynome $f(X)$ und $a(X)$ vollständig auf diese Situation übertragen. Auch hier wird nach mehrfachem Durchführen die Division ohne Rest aufgehen und auch hier ist der letzte nicht-verschwindende Rest der größte gemeinsame Teiler. Da nach Voraussetzung aber $f(X)$ keine Teiler hat und $a(X)$ kein Vielfaches von $f(x)$ ist (denn $a \neq 0$), sind $f(X)$ und $a(X)$ teilerfremd und der größte gemeinsame Teiler ist immer 1 (bzw. eine Einheit im Körper $\mathbb{F}_p$).
Durch Rückwärtsrechnen finden wir auch hier Polynome $g(X)$ und $h(X)$ mit

$$1 = g(X) \cdot a(X) + h(X) \cdot f(X)$$

Setzen wir nun α für X ein, so wird daraus

$$1 = g(\alpha) \cdot a(\alpha) + h(\alpha) \cdot f(\alpha) = g(\alpha) \cdot a$$

(denn $f(\alpha) = 0$ in $\mathbb{F}_q$). Damit ist $g(\alpha)$ das multiplikative Inverse von a, dh. ist

$$g(X) = g_0 + g_1 \cdot X + \cdots + g_t \cdot X^t$$

so ist

$$\frac{1}{a} = g_0 + g_1\alpha + \cdots + g_t\alpha^t$$

Beispiel 3.1.22. Wir betrachten den Körper $\mathbb{F}_4$ mit 4 Elementen, gegeben durch die Relation $\alpha^2 = \alpha + 1$, also das Minimalpolynom $f(X) = X^2 + X + 1$, und das Element $a = \alpha + 1$. Hierfür gilt

$$a(X) = X + 1$$

und der euklidische Algorithmus liefert

1. $f(X) = X \cdot a(X) + 1$.
2. $a(X) = (X + 1) \cdot 1 + 0 \quad \rightarrow$ STOPP, Division geht ohne Rest auf.

Rückwärtsrechnen liefert

$$1 = f(X) - X \cdot a(X) = 1 \cdot f(X) + X \cdot (X + 1)$$

Einsetzen von α für X ergibt in $\mathbb{F}_4$:

$$1 = \alpha \cdot (\alpha + 1)$$

also

$$\frac{1}{\alpha+1} = \alpha$$

Beispiel 3.1.23. Wir betrachten den Körper $\mathbb{F}_8$ mit 8 Elementen, gegeben durch die Relation $\alpha^3 = \alpha+1$, also das Minimalpolynom $f(X) = X^3+X+1$, und das Element $a = \alpha^2 + \alpha + 1$. Hierfür gilt

$$a(X) = X^2 + X + 1$$

und der euklidische Algorithmus liefert

1. $f(X) = (X+1) \cdot a(X) + X$.
2. $a(X) = (X+1) \cdot X + 1$.
3. $X = X \cdot 1 + 0 \quad \rightarrow$ STOPP, Division geht ohne Rest auf.

Rückwärtsrechnen liefert

$$\begin{aligned} 1 &= (X+1) \cdot X + a(X) \\ &= (X+1) \cdot f(X) + (X+1) \cdot (X+1) \cdot a(X) + a(X) \\ &= (X+1) \cdot f(X) + X^2 \cdot a(X) \end{aligned}$$

Einsetzen von α für X ergibt in $\mathbb{F}_8$:

$$1 = \alpha^2 \cdot (\alpha^2 + \alpha + 1)$$

also

$$\frac{1}{\alpha^2+\alpha+1} = \alpha^2$$

Nachdem nun klar ist, wie in einem endlichen Körper $K = \mathbb{F}_q$ gerechnet wird, können wir uns auch mit Fragen der linearen Algebra über diesem Körper beschäftigen. Für die Codierungstheorie von Interesse sind dabei vor allem die Vektorräume $V = \mathbb{F}_q^n$ und lineare Gleichungssysteme sowie Matrizen. Für Gleichungssysteme und Matrizen gelten die Konzepte und Regeln, die auch in der linearen Algebra über den reellen und komplexen Zahlen gelten.

Beispiel 3.1.24. Wir betrachten den Körper $K = \mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha^2 + 1$ und das (homogene) lineare Gleichungssystem

$$\begin{aligned} (\alpha+1) \cdot x_1 &+ \alpha \cdot x_2 &+ x_3 &= 0 \\ \alpha^2 \cdot x_1 &+ x_2 &+ \alpha \cdot x_3 &= 0 \end{aligned}$$

Dieses Gleichungssystem wird als beschrieben durch die Koeffizientenmatrix

$$A = \begin{pmatrix} (\alpha+1) & \alpha & 1 \\ \alpha^2 & 1 & \alpha \end{pmatrix}$$

Nach Beispiel 3.1.20 gilt

$$\frac{1}{\alpha+1} = \alpha^2$$

Multiplizieren wir daher Gleichung I mit α^2, so erhalten wir

$$\begin{array}{rcrcrcl} x_1 & + & \alpha^3 \cdot x_2 & + & \alpha^2 \cdot x_3 & = & 0 \\ \alpha^2 \cdot x_1 & + & x_2 & + & \alpha \cdot x_3 & = & 0 \end{array}$$

also, nach Ausnutzung der Relation

$$\begin{array}{rcrcrcl} x_1 & + & (\alpha^2+1) \cdot x_2 & + & x_3 & = & 0 \\ \alpha^2 \cdot x_1 & + & x_2 & + & \alpha \cdot x_3 & = & 0 \end{array}$$

Subtrahieren wir $\alpha^2 \cdot I$ von II, so erhalten wir

$$\begin{array}{rcrcrcl} x_1 & + & (\alpha^2+1) \cdot x_2 & + & x_3 & = & 0 \\ & & (\alpha^4+\alpha^2+1) \cdot x_2 & + & (\alpha^4+\alpha) \cdot x_3 & = & 0 \end{array}$$

wobei wir schon ausgenutzt haben, dass $- = +$ in der Charakteristik 2. Nach Ausnutzung der Relation

$$\begin{array}{rcrcrcl} x_1 & + & (\alpha^2+1) \cdot x_2 & + & x_3 & = & 0 \\ & & \alpha \cdot x_2 & + & (\alpha^2+1) \cdot x_3 & = & 0 \end{array}$$

Da $\frac{1}{\alpha} = \alpha^2 + \alpha$, ergibt Multiplikation der zweiten Gleichung mit $\alpha^2 + \alpha$:

$$\begin{array}{rcrcrcl} x_1 & + & (\alpha^2+1) \cdot x_2 & + & x_3 & = & 0 \\ & & x_2 & + & \alpha^2 \cdot x_3 & = & 0 \end{array}$$

wobei die Relation bereits ausgenutzt wurde. Damit haben wir das Gleichungssystem auf Normalform gebracht und sehen, dass x_3 die einzige freie Variable ist. Eine Basis des Lösungsraums erhalten wir - wie über den reellen Zahlen - dadurch, dass wir $x_3 = 1$ setzen und das zugehörige Gleichungssystem lösen. Wir erhalten

$$x_2 = \alpha^2, \quad x_1 = \alpha^2 + \alpha + 1$$

und damit ist

$$v = \begin{pmatrix} \alpha^2 + \alpha + 1 \\ \alpha^2 \\ 1 \end{pmatrix} = \begin{pmatrix} (1,1,1) \\ (0,0,1) \\ (1,0,0) \end{pmatrix}$$

eine Basis des Lösungsraums des Gleichungssystems.

Bemerkung 3.1.10. Ganz allgemein gilt für endliche Körper $\mathbb{F}_q$ (genauso wie für $\mathbb{R}$ oder $\mathbb{C}$):
Die Lösungsmenge L eines homogenen Gleichungssystems in n Unbekannten über $\mathbb{F}_q$ ist eine $\mathbb{F}_q$–Untervektorraum von $\mathbb{F}_q^n$.
Ist A die Koeffizientenmatrix des linearen Gleichungssystems, so gilt

$$\dim(L) + \mathrm{rg}(A) = n$$

3.2 Lineare Codes

Wir betrachten einen endlichen Körper $k = \mathbb{F}_q$ mit $q = p^l$ Elementen.

Definition 3.2.1. Ein **linearer** $[n,k]_q$**–Code** ist ein $\mathbb{F}_q$–Untervektorraum $C \subseteq \mathbb{F}_q^n$ der Dimension k.

Bemerkung 3.2.1. Ein linearer $[n,k]_q$–Code ist ein $[n,k]_q$–Code im Sinne von Abschnitt 2.2, also ein Code der Länge n und der logarithmischen Kardinalität k.

Beispiel 3.2.1. Die Teilmenge

$$C = \{(0,0,0),(1,1,0),(0,1,1),(1,0,1)\} \subseteq \mathbb{F}_2^3$$

ist ein linearer $[3,2]_2$–Code mit $d(C) = 2$.
Das $C \subseteq \mathbb{F}_2^3$ ein Untervektorraum der Dimension 2 ist, haben wir schon in Beispiel 3.1.12 von Abschnitt 3.1 gesehen. Dass $d(C) = 2$ kann sofort nachgerechent werden.

Definition 3.2.2. Ist $C \subseteq \mathbb{F}_q^n$ ein lineare Code und $c = (c_1, \ldots, c_n) \in C$, so heißt

$$w(c) = d(c,0) = |\{i \in \{1,\ldots,n\} |\, c_i \neq 0\}|$$

das **Gewicht** von c.

Beispiel 3.2.2. Im Beispiel 3.2.1 gilt

$$\begin{aligned} w((0,0,0)) &= 0 \\ w((1,1,0)) &= 2 \\ w((0,1,1)) &= 2 \\ w((1,0,1)) &= 2 \end{aligned}$$

Satz 3.2.1. *Ist $C \subseteq \mathbb{F}_q^n$ ein linearer $[n,k]_q$–Code, so gilt*

$$d(C) = min\{w(c)|\ c \in C \setminus \{0\}\}$$

Beweis: Setze

$$\delta(C) = \min\{w(c)|\ c \in C \setminus \{0\}\}$$

und wähle ein $c = (c_1, \ldots, c_n) \in C$ mit

$$\delta(C) = w(c) = |\{i : c_i \neq 0\}|$$

Dann gilt

$$\delta(C) = d(c, \overrightarrow{0})$$

und deshalb gilt sicherlich

$$\delta(C) \geq d(C)$$

Da $d(C)$ das Minimaum aller paarweisen Abstände ist. Ferner gibt es $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$ mit $d(C) = d(x,y)$. Setzen wir

$$z = x - y = (z_1, \ldots, z_n)$$

wobei $z_i = x_i - y_i$, so ist $Z \in C$, da $C \subseteq \mathbb{F}_q^n$ ein Untervektorraum ist, und es gilt

$$x_i \neq y_i \iff z_i \neq 0$$

Damit erhalten wir sofort aus der Definition

$$w(z) = |\{i : z_i \neq 0\}| = d(x,y)$$

Da nach Definition $\delta(C) \leq w(c)$ folgt hieraus die Ungleichung

$$\delta(C) \leq d(C)$$

und damit erhalten wir insgesamt

$$\delta(C) = d(C)$$

Folgerung 3.2.2. *Ist C ein linearer $[n,1]_q$–Code und bildet der Vektor v eine Basis von C, so gilt*

$$d(C) = w(v)$$

Beweis: Jedes Elemente $c \in C$ ist ein Vielfaches von v, $c = r \cdot v$. Schreiben wir also $v = (v_1, \ldots, v_n)$ und $c = (c_1, \ldots, c_n)$, so ist $c_i = r \cdot v_i$. Speziell gilt also, falls $r \neq 0$:

$$c_i \neq 0 \iff v_i \neq 0$$

und aus Satz 3.2.1 folgt die Behauptung.

Beispiel 3.2.3. Ist $n \geq 3$ und C der $[n,2]_q$–Code mit Basis

$$v_1 = (1,1,1,\ldots,1,1), \quad v_2 = (0,1,1,\ldots,1,1)$$

so gilt $w(v_1) = n$, $w(v_2) = n-1$, aber $d(C) = 1$, denn auch das Element

$$c = v_1 - v_2 = (1,0,0,\ldots,0,0)$$

liegt in C. Für allgemeine Codes kann der Minimalabstand also nicht aus einer Basis berechnet werden.

Beispiel 3.2.4. Für jedes $n \geq 1$ ist die Teilmenge

$$C = \{(r,r,\ldots,r) \in \mathbb{F}_q^n \,|\, r \in \mathbb{F}_q\} \subseteq \mathbb{F}_q^n$$

ein linearer $[n,1]_q$–Code mit $d(C) = n$.
Das $C \subseteq \mathbb{F}_q^n$ ein Untervektorraum der Dimension 1 ist, haben wir schon in Beispiel 3.1.11 von Abschnitt 3.1 gesehen. Offensichtlich gilt für $r \in \mathbb{F}_q \setminus \{0\}$:

$$w((r,r,\ldots,r)) = n$$

und aus Satz 3.2.1 folgt $d(C) = n$.
Der Code C heißt n–**facher Wiederholungscode**.

Beispiel 3.2.5. Für jedes $n \geq 2$ ist die Teilmenge

$$C = \{x_1, \ldots, x_n) \in \mathbb{F}_q^n | \sum_{i=1}^{n} c_i = 0\}$$

ein linearer $[n, n-1]_q$–Code mit $d(C) = 2$.
Also Lösungsmenge des homogenen linearen Gleichungssystems

$$x_1 + x_2 + \cdots + x_n = 0$$

ist C ein Untervektorraum. Die Koeffizientenmatrix ist

$$A = (1\,1\,\cdots\,1)$$

also ist $\mathrm{rg}(A) = 1$, und deshalb nach dem Rangsatz

$$\dim(C) = n - 1$$

Offensichtlich ist kein $x \in \mathbb{F}_q^n$ mit $w(x) = 1$ (also mit genau einer von Null verschiedenen Komponente) eine Lösung des linearen Gleichungssystems. Also gilt für jedes $c \in C \setminus \{\overrightarrow{0}\}$ sicherlich $w(c) \geq 2$. Umgekehrt gilt

$$c = (1, -1, 0, \ldots, 0) \in C$$

es gibt also $c \in C \setminus \{\overrightarrow{0}\}$ mit $w(c) = 2$. Aus Satz 3.2.1 folgt daher $d(C) = 2$. Der Code C heißt **Paritätsprüfcode der Länge** n.

Beispiel 3.2.6. Die Lösungsmenge C des homogenen linearen Gleichungssystems

$$\begin{array}{rcrcrcl} (\alpha+1)\cdot x_1 & + & \alpha\cdot x_2 & + & x_3 & = & 0 \\ \alpha^2\cdot x_1 & + & x_2 & + & \alpha\cdot x_3 & = & 0 \end{array}$$

aus Beispiel 3.1.24 in Abschnitt 3.1 ist ein $[3, 1]_8$–Code. Eine Basis von C bildet der Vektor

$$v = \begin{pmatrix} \alpha^2+\alpha+1 \\ \alpha^2 \\ 1 \end{pmatrix} = \begin{pmatrix} (1,1,1) \\ (0,0,1) \\ (1,0,0) \end{pmatrix}$$

wie wir dort gesehen haben. Der Code besteht also aus allen Vielfachen von v, und daher gilt

$$d(C) = w(v) = 3$$

3.2.1 Beschreibung lineare Codes mit Basen

Ist $C \subseteq \mathbb{F}_q^n$ ein k–dimensionaler linearer Code, so gibt es k Elemente $v_1, \ldots, v_k \in C$ so dass sich jedes Element $c \in C$ schreiben lässt als

$$c = a_1 v_1 + a_2 v_2 + \cdots + a_k v_k \qquad (\text{mit } \ a_i \in \mathbb{F}_p)$$

und diese Darstellung ist eindeutig, d.h. C bestitzt eine Basis der Länge k. Schreiben wir

$$v_1 = (v_{1,1}, \ldots, v_{1,n}), \ldots, v_k = (v_{k_1}, \ldots, v_{k,n})$$

mit $v_{i,j} \in \mathbb{F}_q$, so heißt die Matrix

$$G = \begin{pmatrix} v_{1,1} & v_{1,2} & \ldots & v_{1,n} \\ v_{2,1} & v_{2,2} & \ldots & v_{2,n} \\ \vdots & & \ddots & \vdots \\ v_{k,1} & v_{k,2} & \ldots & v_{k,n} \end{pmatrix}$$

eine **Erzeugermatrix** von C.

Bemerkung 3.2.2. Ein linearer Code ist durch eine Erzeugermatrix eindeutig bestimmt.

Beispiel 3.2.7. Betrachten wir wieder den Code

$$C = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\} \subseteq \mathbb{F}_2^3$$

aus Beispiel 3.2.1, so ist

$$v_1 = (1,1,0), v_2 = (0,1,1)$$

eine Basis von C, und dementsprechend ist

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

eine Erzeugermatrix von C. Es ist aber auch

$$\widetilde{v}_1 = (1,1,0), \widetilde{v}_2 = (1,0,1)$$

eine Basis von C, und damit

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

eine Erzeugermatrix von C. Erzeugermatrizen sind also nicht eindeutig bestimmt.

Beispiel 3.2.8. Durch die Vektoren $v_1 = (2, 1, 0)$ und $v_2 = (0, 1, 2)$ in $\mathbb{F}_3^2$ wird eine linearer $[3, 2]_3$–Code (mit Basis v_1, v_2) definiert, der die Erzeugermatrix

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

hat. Hierfür gilt

$$d(C) = 2$$

Warnung.:
Ist $v_1, \ldots, v_k$ eine Basis einen linearen $[n, k]_q$–Codes C, so kann $d(C)$ nicht aus den $v_1, \ldots, v_k$ direkt abgelesen werden. So definieren etwa die Vektoren

$$v_1 = (1, 1, 1, 1, 0), \quad v_2 = (0, 1, 1, 1, 1) \in \mathbb{F}_2^5$$

einen linearen $[5, 2]_2$–Code C mit $d(C) = 2$. Es gilt jedoch

$$w(v_1) = w(v_2) = 4$$

3.2.2 Beschreibung lineare Codes mit Gleichungssystemen

Untervektorräume von $\mathbb{F}_q^n$ können mit Hilfe von Basen beschrieben werden. Wie in der linearen Algebra über $\mathbb{R}$ ist es aber auch über endlichen Körpern möglich, Untervektorräume durch lineare Gleichungssysteme zu beschreiben. In Matrizennotation erhalten wir

Satz 3.2.3. *Ist $C \subseteq \mathbb{F}_q^n$ ein lineare $[n, k]_q$–Code, so gibt es eine $(n-k) \times n$–Matrix H mit*

$$C = \{(c_1, \ldots, c_n) |\ H \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

Bemerkung 3.2.3. Die Matrix H aus Satz 3.2.3 hat nach dem Rangsatz dann

$$\mathrm{rg}(H) = n - k$$

Definition 3.2.3. Eine $(n-k) \times n$–Matrix H mit

$$C = \{(c_1, \ldots, c_n) |\ H \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

heißt **Paritätsprüfmatrix** des Codes C.

Beispiel 3.2.9. Betrachten wir wieder den Code

$$C = \{(0,0,0), (1,1,0), (0,1,1), (1,0,1)\} \subseteq \mathbb{F}_2^3$$

aus Beispiel 3.2.1, so ist dieser gegeben durch das lineare Gleichungssystem

$$x_1 + x_2 + x_3 = 0$$

(bestehend aus nur einer Gleichung), hat also Paritätsprüfmatrix

$$H = (1\ 1\ 1)$$

Beispiel 3.2.10. In Beispiel 2.1.8 aus Abschnitt 2.1.2 wurde über $\mathbb{F}_7$ gearbeitet. Dabei wurden die Prüfziffern a_5, a_6 durch das folgende Gleichungssystem (über $\mathbb{F}_7$) bestimmt:

$$\begin{array}{ccccccccccccc} a_1 & + & a_2 & + & a_3 & + & a_4 & + & a_5 & + & a_6 & = & 0 \\ a_1 & + & 2a_2 & + & 3a_3 & + & 4a_4 & + & 5a_5 & + & 6a_6 & = & 0 \end{array}$$

Der dort betrachtete Code war also gegeben durch die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

Aus der Paritätsprüfmatrix kann die Qualität des Codes direkt abgeleitet werden:

Satz 3.2.4. *Ist H die Paritätsprüfmatrix eines linearen $[n,k]_q$–Codes und ist $d = d(C)$ der Minimalabstand von C, so gilt*

1. *Es gibt d Spalten von H, die linear abhängig sind.*

2. *Je $d-1$ Spalten von H sind linear unabhängig.*

Beweis: Da C linear ist, gibt es ein Element $c \in C$ mit $w(c) = d$. Zur Vereinfachung der Notation wollen wir annehmen, dass

$$c = (c_1, \ldots, c_d, 0, \ldots, 0)$$

(sodass also notwendig $c_1 \neq 0, \ldots, c_d \neq 0$) Sind dann $\overrightarrow{h_1}, \ldots, \overrightarrow{h_d}$ die ersten d Spalten von H, so folgt aus

$$H \cdot \overrightarrow{c} = \overrightarrow{0}$$

dass

$$c_1 \cdot \overrightarrow{h_1} + \cdots + c_d \cdot \overrightarrow{h_d} = \overrightarrow{0}$$

und damit sind die ersten d Spalten von H linear unabhängig.
Wir haben noch zu zeigen, dass je $d-1$ Spalten von H linear unabhängig sind. Das zeigen wir mit Widerspruch und nehmen an, dass es $d-1$ linear abhängig Spalten in H gibt. Zur Vereinfachung der Notation nehmen wir wieder an, dass es die $d-1$ ersten Spalten $\overrightarrow{h_1}, \ldots, \overrightarrow{h_{d-1}}$ sind (der allgemeine Fall geht genau so, ist aber schwieriger zu notieren). Das bedeutet, dass es $r_1, \ldots, r_{d-1}$ in $\mathbb{F}_q$ gibt, nicht alle gleich Null, sodass

$$r_1 \cdot \overrightarrow{h_1} + \cdots + r_{d-1} \cdot \overrightarrow{h_{d-1}} = \overrightarrow{0}$$

Setzen wir dann $r = (r_1, \ldots, r_{d-1}, 0, \ldots, 0) \in \mathbb{F}_q^n$, so gilt hierfür $r \neq 0$ und $w(r) \leq d-1$, aber

$$H \cdot \overrightarrow{r} = r_1 \cdot \overrightarrow{h_1} + \cdots + r_{d-1} \cdot \overrightarrow{h_{d-1}} = \overrightarrow{0}$$

Beispiel 3.2.11. Der lineare $[5,2]_2$–Code mit Paritätsprüfmatrix

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

hat $d(C) = 3$, denn je zwei Spalten sind linear unabhängig, aber die erste, die dritte und die fünfte Spalte sind linear abhängig.

Ist eine Code durch seine Paritätsprüfmatrix gegeben, so kann daraus leicht eine Erzeugermatrix gewonnen werden. Betrachten wir etwa den Code aus Beispiel 3.2.10 mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

so hat diese Matrix die Normalform

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$$

und das zugehörige homogene Gleichungssystem dementsprechend die freien Variablen x_3, x_4, x_5 und x_6. Nach unserem Standardverfahren erhalten wir eine Basis des Lösungsraums als

$$\begin{aligned} g_1 &= (1,\, 5,\, 1\,0,\, 0,\, 0) \\ g_2 &= (1,\, 4,\, 0\,1,\, 0,\, 0) \\ g_3 &= (1,\, 3,\, 0\,0,\, 1,\, 0) \\ g_4 &= (1,\, 2,\, 0\,0,\, 0,\, 1) \end{aligned}$$

Diese Vektoren bilden daher eine Basis des Codes C, und damit ist eine Erzeugermatrix gegeben durch

$$G = \begin{pmatrix} 1 & 5 & 1 & 0 & 0 & 0 \\ 1 & 4 & 0 & 1 & 0 & 0 \\ 1 & 3 & 0 & 0 & 1 & 0 \\ 1 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Nach der gleichen Methode lässt sich aber auch die Paritätsprüfmatrix aus der Erzeugermatrix herleiten:
Ist G eine Erzeugermatrix eines $[n,k]_q$–Codes und ist

$$\begin{aligned} h_1 &= (h_{1,1}, h_{1,2}, \ldots, h_{1,n}) \\ h_2 &= (h_{2,1}, h_{2,2}, \ldots, h_{2,n}) \\ &\vdots \\ h_{n-k} &= (h_{n-k,1}, h_{n,2}, \ldots, h_{n-k,n}) \end{aligned}$$

eine Basis des Lösungsraums des homogenen Gleichungssystems

$$G \cdot \overrightarrow{x} = \overrightarrow{0}$$

so ist

$$H = \begin{pmatrix} h_{1,1} & h_{1,2} & \dots & h_{1,n} \\ h_{2,1} & h_{2,2} & \dots & h_{2,n} \\ & & \ddots & \\ h_{n-k,1} & h_{n-k,2} & \dots & h_{n-k,n} \end{pmatrix}$$

eine Paritätsprüfmatrix von C.
Das ergibt sich leicht aus den Regeln der Matrizenmultiplikation. Daraus folgt nämlich, dass

$$H \cdot \overrightarrow{g_i} = \overrightarrow{0}$$

für alle Zeilen g_i von G (also alle Basisvektoren von C). Aus Ranggründen folgt dann schon

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot \overrightarrow{c} = \overrightarrow{0}$$

und damit ist H eine Paritätsprüfmatrix von C.

Beispiel 3.2.12. Für den $[5, 2]_2$–Code mit Erzeugermatrix

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

ist

$$\begin{aligned} h_1 &= (1, 1, 1, 0, 0) \\ h_2 &= (0, 1, 0, 1, 0) \\ h_3 &= (1, 1, 0, 0, 1) \end{aligned}$$

eine Basis des Lösungsraums des homogenen Gleichungssystems

$$G \cdot \overrightarrow{x} = \overrightarrow{0}$$

und daher

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

eine Paritätsprüfmatrix.

3.2.3 Qualitätsschranken linearer Codes

Wir betrachten einen allgemeinen lineare $[n, k, d]_q$–Code C, wobei $d = d(C)$ der Minimalabstand dieses Codes ist. Dann heißt

$R = \frac{k}{n}$ die Informationsrate

$\delta = \frac{d}{n}$ die relative Zuverlässigkeit

dieses Codes. Für die Praxis interessant und relevant sind lineare Codes C, die bei großem n eine hohe Informationsrate R und eine hohe relative Zuverlässigkeit δ liefern (wobei es natürlich vom Übertragungskanal abhängt, ob die Gewichtung mehr auf der Informationsrate oder mehr auf der Zuverlässigkeit liegt). Das Problem dabei ist, dass sich Informationsrate und Zuverlässigkeit nicht simultan beliebig steigern lassen.

Regel 3.2.5. *Für einen beliebigen $[n, k, d]_q$–Code gelten die folgenden Schranken*

1. *Singleton–Schranke:* $k + d \leq n + 1$.
2. *Griesemer–Schranke:* $n \geq \sum_{i=0}^{k-1} \lceil \frac{d}{q^i} \rceil$.
3. *Plotkin–Schranke:* $d \leq \frac{nq^k(q-1)}{(q^k-1)q}$.
4. *Hamming–Schranke:* $n - k \geq \log_q \left(\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i} \cdot (q-1)^i \right)$.

Vor allem für große n existieren auch noch schärfere Schranken (asymptotische Schranken).

Definition 3.2.4. Ein linearer $[n, k]_q$–Code C heißt **MDS–Code** (*minimal distance separable code*), wenn

$$d(C) = n + 1 - k$$

wenn für diesen Code also die Singleton–Schranke angenommen wird.

Diese Schranken liefern alle 'negative' Resulate insofern als sie Einschränkungen für die Konstruktion mächtiger Codes darstellen. Es gibt aber auch positive Resultate, etwa

Satz 3.2.6. *(Gilbert–Varshamov–Schranke)*
Falls

$$q^{n-k} \geq \sum_{i=0}^{d-2} \binom{n-1}{i} \cdot (q-1)^i$$

so gibt es einen lineare $[n,k,d]_q$–Code.

3.2.4 Duale Codes

Wir betrachten auf $\mathbb{F}_q^n$ die Paarung

$$\langle\ ,\ \rangle : \mathbb{F}_q^n \times \mathbb{F}_q^n \longrightarrow \mathbb{F}_q$$

mit

$$\langle x, y\rangle = \sum_{i=1}^{n} x_i \cdot y_i$$

(wobei $x = (x_1, \ldots, x_n)$ und $y = (y_1, \ldots, y_n)$).
Die Paarung $\langle\ ,\ \rangle$ ist bilinear und nicht ausgeartete, d.h. ist $x \in \mathbb{F}_q^n$ mit $\langle x, y\rangle = 0$ für alle $y \in \mathbb{F}_q^n$, so gilt schon $u = 0$.

Bemerkung 3.2.4. Die Paarung $\langle\ ,\ \rangle$ lässt sich mit dem Matrizenprodukt beschreiben:

$$\langle x, y\rangle = x \cdot y^\top$$

Definition 3.2.5. ist $C \subseteq \mathbb{F}_q^n$ ein $[n,k]_q$–Code, so heißt

$$C^\perp = \{v \in \mathbb{F}_q^n |\, \langle u, v\rangle = 0 \quad \forall u \in C\}$$

der zu C **duale Code**.

Satz 3.2.7. *Es gilt*

1. *$C^\perp$ ist ein $[n, n-k]_q$–Code.*
2. *$\left(C^\perp\right)^\perp = C$.*

3. *Ist G eine Erzeugermatrix von C, so ist G eine Paritätsprüfmatrix von $C^\perp$ und ist H eine Paritätsprüfmatrix von C, so ist H eine Erzeugermatrix von $C^\perp$.*

Beweis: Wir betrachten eine Erzeugermatrix G von C und bezeichnen mit $g_1, \ldots, g_k$ die Zeilen von G (die also eine Basis von C bilden). Dann gilt

$$\begin{aligned} v \in C^\perp &\iff \langle u, v\rangle = 0 \quad \forall c \in C \\ &\iff \langle g_i, v\rangle = 0 \quad \forall i \in \{1, \ldots, k\} \\ &\iff G \cdot v^\top = 0 \end{aligned}$$

Damit ist G eine Paritätsprüfmatrix von $C^\perp$. Entsprechend ist eine Paritätsprüfmatrix H von C eine Erzeugermatrix von $C^\perp$.
Daraus folgen alle Aussagen des Satzes sofort.

Beispiel 3.2.13. Wir betrachten den $[4,2]_q$–Code

$$C = \{(v_1, v_2, 0, 0) \in \mathbb{F}_q^4 |\, v_1, v_2 \in \mathbb{F}_q\}$$

Dann gilt

$$C^\perp = \{(0, 0, v_3, v_4) \in \mathbb{F}_q^4 |\, v_3, v_4 \in \mathbb{F}_q\}$$

Beispiel 3.2.14. Wir betrachten den $[2,1]_2$–Code

$$C = \{(0,0), (1,1)\}$$

Dann gilt

$$C^\perp = \{(0,0), (1,1)\}$$

In diesem Fall stimmen also C und $C^\perp$ überein.

Definition 3.2.6. Ein Code C heißt **selbstdual**, wenn $C = C^\perp$.

Kapitel 4

Spezielle lineare Codes

Viele der in der Praxis verwendeten linearen Codes zeichnen sich durch Zusatzeigenschaften aus, des es erleichtern, mit Ihnen zu arbeiten. Wir fixieren eine Primzahl $p > 0$ und betrachen einen endlichen Körper $\mathbb{F}_q$ mit $q = p^l$ Elementen.

4.1 Ausgewählte spezielle Beispiele

Beispiel 4.1.1. Der n–**fache Wiederholungscode** $C \subseteq \mathbb{F}_q^n$ ist der $[n, 1, n]_q$–Code

$$C = \{(r, r, \ldots, r) \in \mathbb{F}_q^n | \, r \in \mathbb{F}_q\}$$

(vergleiche auch Beispiel 3.2.4).

Beispiel 4.1.2. Der **Paritätstprüfcode** $C \subseteq \mathbb{F}_q^n$ der Länge n ist der $[n, n-1, 2]_q$–Code

$$C = \{(x_1, \ldots, x_n) \in \mathbb{F}_q^n | \sum_{i=1}^{n} x_i = 0\}$$

(vergleiche auch Beispiel 3.2.5).

Bemerkung 4.1.1. Der n–fache Wiederholungscode hat Erzeugermatrix

$$G = (1\,1\,\ldots\,1)$$

und der Paritätsprüfcode der Länge n hat die Paritätsprüfmatrix

$$H = (1\,1\,\ldots\,1)$$

Die beiden Codes sind also dual zueinander.

Die meisten interessanten Codes sind jedoch komplizierter in ihrer Beschreibung.
Wir betrachen ein n von der Form $n = 2^k - 1$ und alle möglichen k–Tupel $v = \begin{pmatrix} a_1 \\ \vdots \\ a_k \end{pmatrix}$ mit $a_i \in \{0, 1\}$ ohne das Nulltupel $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$. Hiervon gibt es genau n Stück $v_1, \ldots, v_n$. Wir betrachten die $k \times n$–Matrix

$$H = (v_1 \ \ldots \ v_n)$$

mit den v_i als Spalten.

Satz 4.1.1. *Die Matrix H ist die Paritätsprüfmatrix eines vollkommenen $[n, n-k, 3]_2$–Codes.*

Beweis: Die Matrix H definiert durch

$$C = \{x \in \mathbb{F}_2^n | \, H \cdot x^\top = 0\}$$

sicherlich einen Untervektorraum $C \subseteq \mathbb{F}_2^n$, also einen binären Code. Offensichtlich ist $\mathrm{rg}(H) = k$, da H die Matrix

$$\begin{pmatrix} 1 & 0 & 0 & \ldots & 0 \\ 0 & 1 & 0 & \ldots & 0 \\ & & & \ddots & \\ 0 & 0 & 0 & \ldots & 1 \end{pmatrix}$$

als Teilmatrix enthält. Damit ist

$$\dim(C) = n - k$$

Je zwei Spalten von C sind linear unabhängig, also gilt $d(C) \geq 3$. Da mit je zwei Spalten v_1, v_2 von H (mit $v_1 \neq v_2$) aber auch die Summe $v_1 + v_2$ eine Spalte von H ist, gibt es drei Spalten von H, die linear abhängig sind, und damit ist $d(C) = 3$.
Zu $u \in C$ betrachten wir

$$B(u) = \{x \in \mathbb{F}_2^n | \, d(x, u) \leq 1\}$$

also die Menge aller Elemente, die sich höchstens an einer Stelle von u unterscheiden. Da wir über $\mathbb{F}_2$ arbeiten, gilt

$$|B(u)| = 1 + n = 1 + 2^k - 1 = 2^k$$

Da $d(C) = 3$ gilt

$$B(u) \cap B(v) = \emptyset \qquad \text{für } u, v \in C \text{ mit } u \neq v$$

und da C ein $[n, n-k]_2$–Code ist, gilt

$$|C| = 2^{n-k}$$

Damit erhalten wir

$$|\bigcup_{u \in C} B(c)| = \sum_{u \in C} |B(u)| = 2^{n-k} \cdot 2^k = 2^n = |\mathbb{F}_2^n|$$

so dass also gilt

$$\bigcup_{u \in C} B(c) = \mathbb{F}_2^n$$

und damit ist C ein vollkommener Code.

Definition 4.1.1. Der Code C heißt **Hammingcode**

Beispiel 4.1.3. Für $k = 3$ gilt

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

4.2 Zyklische Codes

Definition 4.2.1. Ein linearer $[n, k]_q$–Code $C \subseteq \mathbb{F}_q^n$ heißt **zyklisch**, wenn gilt:
Ist $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in C$, so ist auch $\widetilde{c} = (c_n, c_1, c_2, \ldots, c_{n-1}) \in C$.

Beispiel 4.2.1. Der $[4, 2]_2$–Code

$$C = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\} \subseteq \mathbb{F}_2^4$$

ist zyklisch.

Beispiel 4.2.2. Der $[4,2]_2$–Code

$$C = \{(0,0,0,0),(1,1,1,0),(0,1,1,1),(1,0,0,1)\} \subseteq \mathbb{F}_2^4$$

ist nicht zyklisch.

Bemerkung 4.2.1. Für ein $c = (c_1, c_2, \ldots, c_{n-1}, c_n) \in \mathbb{F}_q^n$ bezeichnen wir mit $c^{[1]} = (c_n, c_1, c_2, \ldots, c_{n-1})$ das Element von $\mathbb{F}_q^n$, das dadurch entsteht, dass wir alle Komponenten um eine Stelle nach rechts verschieben. Ein Code C ist also genau dann zyklisch, wenn für $c \in C$ auch $c^{[1]} \in C$.
Ist $\mathbf{g_1}, \ldots, \mathbf{g_k}$ Basis eines $[n,k]_q$–Codes C, so ist C genau dann zyklisch, wenn $\mathbf{g_1}^{[1]}, \ldots, \mathbf{g_k}^{[1]} \in C$.
Ist nämlich C zyklisch, so muss für alle $c \in C$ gelten: $c^{[1]} \in C$, speziell also für $\mathbf{g_1}, \ldots, \mathbf{g_k}$. Gilt umgekehrt $\mathbf{g_1}^{[1]}, \ldots, \mathbf{g_k}^{[1]} \in C$, und ist $c \in C$ beliebig, so schreiben wir

$$c = a_1 \cdot \mathbf{g_1} + \cdots a_k \cdot \mathbf{g_k}$$

Dann ist $c^{[1]} = a_1 \cdot \mathbf{g_1}^{[1]} + \cdots a_k \cdot \mathbf{g_k}^{[1]}$, und das ist ein Element von C, da $\mathbf{g_l}^{[1]} \in C$ für alle l.

Zum besseren Studium der zyklischen Codes benötigen wir Polynome über endlichen Körpern.

Definition 4.2.2. Ein **Polynom** über $\mathbb{F}_q$ ist ein Ausdruck der Form

$$f(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

mit $a_0, \ldots, a_n \in \mathbb{F}_q$ und mit einer Unbekannten X.
Die Zahlen $a_l \in \mathbb{F}_q$ heißen die **Koeffizienten** des Polynoms $f(X)$.
Ist $a_n \neq 0$, so heißt $\deg(f) = n$ der **Grad** von $f(X)$.
Mit $\mathbb{F}_q[X]$ bezeichnen wir die Menge der Polynome über $\mathbb{F}_q$.

Beispiel 4.2.3. Der Ausdruck

$$f(X) = 3 + 2X + 4X^5$$

ist ein Polynom über $\mathbb{F}_7$, wenn wir 3, 2 und 4 als Elemente von $\mathbb{F}_7$ betrachten.

Beispiel 4.2.4. Ist $\mathbb{F}_4$ der Körper mit 4 Elementen, definiert durch $\alpha^2 = \alpha + 1$, so ist

$$f(X) = 1 + \alpha \cdot X^2 + (\alpha + 1) \cdot X^3$$

ein Polynom über $\mathbb{F}_4$ vom Grad 3.

Bemerkung 4.2.2. Auch die Elemente von $\mathbb{F}_q$ sind Polynome (mit $n = 0$), die **konstanten Polynome**

Bemerkung 4.2.3. Wir betrachten zwei Polynome

$$f(X) = a_0 + a_1X + \cdots + a_nX^n, \quad g(X) = b_0 + b_1X + \cdots + b_mX^m$$

(über demselben Körper $\mathbb{F}_q$). Diese Polynome können addiert werden, indem die Koeffizienten addiert werden, also im Fall $n \leq m$:

$$(f+g)(X) = a_0+b_0+(a_1+b_1)\cdot X+\cdots+(a_n+b_n)\cdot X^n+b_{n+1}X^{n+1}+\cdots b_mX^m$$

und im Fall $n > m$:

$$(f+g)(X) = a_0+b_0+(a_1+b_1)\cdot X+\cdots+(a_m+b_m)\cdot X^m+a_{m+1}X^{m+1}+\cdots+a_nX^n$$

Sie können aber auch multipliziert werden, und zwar (wie über $\mathbb{R}$) nach der Formel

$$\begin{aligned}(f \cdot g)(X) &= a_0 \cdot b_0 + (a_1 \cdot b_0 + a - 0 \cdot b_1) \cdot X + \cdots \\ &\quad \cdots + (a_n \cdot b_{m-1} + a_{n-1}b_m) \cdot X^{n+m-1} + a_n \cdot b_m \cdot X^{n+m} \\ &= \sum_{k=0}^{n+m} \left(\sum_{i+j=k} a_i b_j \right) \cdot X^k\end{aligned}$$

(wobei Multiplikationen und Additionen der Koeffizienten natürlich in $\mathbb{F}_q$ durchzuführen sind).
Die Polynome $\mathbb{F}_q[X]$ bilden also einen Ring.

Beispiel 4.2.5. Über $\mathbb{F}_2$ gilt

$$(X^2 + X + 1) + (X^2 + 1) = X$$

und

$$(X^2 + X + 1) \cdot (X^2 + 1) = X^4 + X^3 + X + 1$$

Bemerkung 4.2.4. Wie auch über $\mathbb{R}$ können Polynome mit Rest dividiert werden. Dabei ist aber auch hier zu beachten, dass die Rechnungen in $\mathbb{F}_q$ durchzuführen sind, dass also etwa über $\mathbb{F}_2$ gilt

$$(X^4+1) \div (X+1) = X^3 + X^2 + X + 1 \qquad \text{Rest } 0$$

wohingegen über $\mathbb{R}$ gilt

$$(X^4+1) \div (X+1) = X^3 - X^2 + X - 1 \qquad \text{Rest } 2$$

Satz 4.2.1. *Ist C ein zyklischer $[n,k]_q$–Code, so gibt es Elemente $g_0, \ldots, g_{n-k} \in \mathbb{F}_q$ und $h_0, \ldots, h_k \in \mathbb{F}_q$ mit den folgenden Eigenschaften*

1. $\big(g_0 + g_1 X + \cdots + g_{n-k}X^{n-k}\big) \cdot \big(h_0 + h_1 X + \cdots + h_k X^k\big) = X^n - 1$ *über* $\mathbb{F}_q$.

2. *Die Matrix*

$$G = \begin{pmatrix} g_0 & g_1 & \cdots & & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & & \cdots & g_{n-k-1} & g_{n-k} & 0 & \cdots & 0 \\ \vdots & & & \ddots & & & & & & \vdots \\ 0 & 0 & & g_0 & & & & & & g_{n-k} \end{pmatrix}$$

   mit n Spalten und k Zeilen ist eine Erzeugermatrix von G.

3. *Die Matrix*

$$H = \begin{pmatrix} h_k & h_{k-1} & \cdots & & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & & & \ddots & & & & & & \vdots \\ 0 & 0 & & h_k & & & & & & h_0 \end{pmatrix}$$

   mit n Spalten und $n-k$ Zeilen ist eine Paritätsprüfmatrix von G.

Umgekehrt definieren auch zwei Polynome

$$G(X) = g_0 + g_1 X + \cdots + g_{n-k}X^{n-k}, \quad H(X) = h_0 + h_1 X + \cdots + h_k X^k$$

mit $G(X) \cdot H(X) = X^n - 1$ über $\mathbb{F}_q$ einen zyklischen $[n,k]_q$–Code (mit Erzeuger– und Paritätsprüfmatrix wie oben beschrieben).

Beweis: Wir wollen nur den Teil zeigen, der besagt, dass G (wie oben konstruiert) die Erzeugermatrix eines zyklischen $[n,k]_q$–Codes ist, wenn $G(X)$ und $H(X)$ Polynome sind mit $G(X)\cdot H(X) = X^n - 1$.
Da $g_0 \cdot h_0 = -1$, ist $g_0 \neq 0$, und daher liegt G in Zeilen–Stufen–Form vor, dh. die Zeilen $\mathbf{g_1}, \ldots, \mathbf{g_k}$ von G sind linear unabhängig und daher Basis eines $[n,k]_q$–Codes C. Um zu zeigen, dass dieser Code zyklisch ist, reicht es nach Bemerkung 4.2.1,zu zeigen, dass $\mathbf{g_1}^{[1]}, \ldots, \mathbf{g_k}^{[1]} \in C$.
Nach Konstruktion ist $\mathbf{g_l}^{1]} = \mathbf{g_{l+1}}$ für $l < k$, und daher bleibt nur noch zu zeigen, dass $\mathbf{g_k}^{[1]} \in C$. Es ist

$$\mathbf{g_k}^{[1]} = (g_{n-k}, 0, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1})$$

Nach Voraussetzung an die Polynome $G(X)$ und $H(X)$ gilt

$$\begin{array}{lcll} g_{n-k}\cdot h_k & = & 1 & \\ \sum\limits_{i+j=l} g_i h_j & = & 0 & \text{für} \quad 0 < l < n \\ g_0 \cdot h_0 & = & -1 & \end{array} \tag{4.1}$$

Es reicht zu zeigen, dass $h_k \cdot \mathbf{g_k}^{[1]} \in C$, da $h_k \neq 0$. Dabei ist

$$\begin{aligned} h_k \cdot \mathbf{g_k}^{[1]} &= (h_k g_{n-k}, 0, \ldots, 0, h_k g_0, \ldots, h_k g_{n-k-1}) \\ &= (1, 0, \ldots, 0, h_k g_0, \ldots, h_k g_{n-k-1}) \\ &= (-h_0 g_0, 0, \ldots, 0, -\sum_{i=1}^{k} g_i h_{k-i}, -\sum_{i=2}^{k} h_{k+1-i} g_i, \ldots, h_{k-1} g_{n-k}) \\ &= -h_0 \cdot \mathbf{g_1} - h_1 \cdot \mathbf{g_2} - \cdots - h_{k-1} \cdot \mathbf{g_k} \end{aligned}$$

und damit gilt die Behauptung.
Das H eine Paritätsprüfmatrix dieses Codes ist, erhalten wir ebenfalls aus den Beziehungen (4.1).
Die Konstruktion von $G(X)$ und $H(X)$ aus einem zyklischen Code erfordert einige Kenntnisse in Algebra, daher verzichten wir hier darauf.

Bemerkung 4.2.5. Der Satz besagt, dass die zyklischen $[n,k]_q$–Codes C durch Polynome $G(X)$ vom Grad $n-k$ definiert werden, die über $\mathbb{F}_q$ das Poylnom $X^n - 1$ teilen. Algebraisch gesprochen bedeutet das, dass die zyklischen q–adischen Codes der Länge n den Idealen des Rings $R = \mathbb{F}_q[X]/)X^n - 1)$ entsprechen.

Definition 4.2.3. Das Polynom $G(X)$ aus Satz 4.2.1 heißt **Erzeugerpolynom** des Codes C, das Polynom $H(X)$ heißt **Paritätsprüfpolynom** von C.

Bemerkung 4.2.6. Ist $G(X)$ Erzeugerpolynom des zyklischen $[n,k]_q$–Codes C, und ist $r \in \mathbb{F}_q \setminus \{0\}$, so ist auch $r \cdot G(X)$ ein Erzeugerpolynom von C (und $\frac{1}{r} \cdot H(X)$ ist das entsprechende Paritätsprüfpolynom). Das sieht man sofort daran, dass die aus $G(X)$ bzw. $r \cdot G(X)$ abgeleiteten Matrizen G (wie in Satz 4.2.1) sich nur um den Faktor r unterscheiden, ihre Zeilen also den gleichen Code erzeugen. Zwei Polynome, die $X^n - 1$ teilen erzeugen also denselben zyklischen Code, wenn sie sich nur um einen Faktor unterscheiden. Das ist allerdings auch die einzige Möglichkeit, wie zwei Polynome denselben zyklischen Code erzeugen. Fordern wir also zusätzlich, dass $g_{n-k} = 1$ (dass das Erzeugerpolynom also normiert ist), so ist das Erzeugerpolynom durch den zyklischen Code schon eindeutig bestimmt.
Ist speziell $q = 2$, so ist des Erzeugerpolynom automatisch eindeutig festgelegt.

Beispiel 4.2.6. Das Polynom $G_1(X) = X^2 + 5X + 6 \in \mathbb{F}_7[X]$ definiert einen zyklischen $[6,4]_7$–Code mit Paritätsprüfpolynom

$$H_1(X) = X^4 + 2X^3 + 5X^2 + 5X + 1$$

Derselbe Code wird definiert durch $G_2(X) = 5X^2 + 4X + 2$ $(= 5 \cdot G_1(X))$ mit Paritätsprüfpolynom $H_2(X) = 3X^4 + 6X^3 + X^2 + X + 3 = 3 \cdot H_1(X)$.

Beispiel 4.2.7. Die beiden Poylnome

$$G_1(X) = 3X^3 + X^2 + X + 5, \quad G_2(X) = 5X^3 + 4X^2 + 3X + 2 \in \mathbb{F}_7[X]$$

definieren zyklische $[6,3]_7$–Codes mit den Paritätsprüfpolynomen

$$H_1(X) = 5X^3 + 3X^2 + 2X + 4, \qquad H_2(X) = 3X^3 + 6X^2 + 6X + 3$$

diese beiden zyklischen Codes stimmen aber nicht überein, denn es gibt kein $r \in \mathbb{F}_7$ mit

$$G_2(X) = r \cdot G_1(X)$$

Dann müsste nämlich gelten

$$5 = r \cdot 3, \qquad 3 = r \cdot 1$$

(durch Vergleich der Faktoren vor X^3 und X). Aus der ersten Bedingung folgt aber $r = 4$ und aus der zweiten $r = 3$. Also können nicht beide Bedingungen gleichzeitig für ein r erfüllt sein.

Bemerkung 4.2.7. Ist $G(X) = g_0 + g_1X + \cdots + g_{n-k}X^{n-k}$ das Erzeugerpolynom eines zyklischen $[n, k]_q$–Codes, so gilt immer $g_0 \neq 0$. Andernfalls wäre nämlich $G(X) \cdot H(X)$ immer durch X teilbar, aber für das Paritätsprüfpolynom muss ja gelten $G(X) \cdot H(X) = X^n - 1$, und das ist nicht durch X teilbar.
Ist speziell $q = 2$, so muss $g_0 = 1$ gelten.

Beispiel 4.2.8. Über $\mathbb{F}_2$ gilt

$$X^n - 1 = X^n + 1$$

da hier $+1 = -1$. Ferner ist

$$(X^2 + X + 1) \cdot (X^4 + X^3 + X + 1) = X^6 + 1$$

Damit ist $G(X) = X^2 + X + 1$ das Erzeugerpolynom eines zyklischen $[6, 4]_2$–Codes mit Erzeugermatrix

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

Das Paritätsprüfpolynom dieses Codes ist $H(X) = X^4 + X^3 + X + 1$, und

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

ist eine Paritätsprüfmatrix.

Beispiel 4.2.9. Über $\mathbb{F}_2$ ist

$$(X^6 + X^3 + 1) \cdot (X^3 + 1) = X^9 + 1$$

Damit ist $G(X) = X^6 + X^3 + 1$ das Erzeugerpolynom eines zyklischen $[9, 3]_2$–Codes mit Erzeugermatrix

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

Das Paritätsprüfpolynom dieses Codes ist $H(X) = X^3 + 1$, und

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

ist eine Paritätsprüfmatrix.

Beispiel 4.2.10. Das Polynom $G(X) = X^2 + 2$ ist das Erzeugerpolynom eines zyklischen $[4, 2]_3$–Codes C. Über $\mathbb{F}_3$ ist $X^4 - 1 = X^4 + 2$, da $-1 = 2$, und

$$(X^2 + 2) \cdot (X^2 + 1) = X^4 + 2X^2 + X^2 + 2 = X^4 + 2$$

Das Paritätsprüfpolynom dieses Codes ist $H(X) = X^2 + 1$

Beispiel 4.2.11. In diesem Beispiel bestimmen wir die Anzahl der zyklischen $[6, 4]_2$–Codes. Nach den Bemerkungen 4.2.6 und 4.2.7 kommen als Erzeugerpolynome nur die folgenden beiden Polynome in Frage

$$g_1(X) = X^2 + X + 1, \qquad g_2(X) = X^2 + 1$$

Wir führen für beide Kandidaten Polynomdivision mit Rest (über $\mathbb{F}^2$) durch:

$$(X^6 + 1) \div (X^2 + 1) = X^4 + X^2 + 1$$

Die Polynomdivision geht also ohne Rest auf und damit ist $g_1(X)$ das Erzeugerpolynom eines zyklischen $[6,4]_2$–Codes.

$$(X^6+1) \div (X^2+X+1) = X^4+X^3+X+1$$

Auch diese Polynomdivision geht also ohne Rest auf und damit ist $g_2(X)$ ebenfalls das Erzeugerpolynom eines zyklischen $[6,4]_2$–Codes. Es handelt sich dabei um zwei unterschiedliche Codes, wie man in diesem Fall auch elementar nachrechnen kann.
Beachten Sie, dass über $\mathbb{R}$ zwar die erste Polynomdivision ohne Rest aufgeht, nicht aber die zweite. Dort bleibt ein Rest von 2.

Beispiel 4.2.12. In diesem Beispiel bestimmen wir die Anzahl der zyklischen $[6,4]_3$–Codes. Da über $\mathbb{F}_3$ gilt $X^4-1 = X^4+2$, sind dazu alle Teiler von X^4+2 über $\mathbb{F}_3$ zu finden. Wegen Bemerkungen 4.2.6 und 4.2.7 müssen nur die folgenden Kandidaten getestet werden

$$\begin{array}{lll} g_1(X) = X^2+1, & g_2(X) = X^2+X+1, & g_3(X) = X^2+2x+1, \\ g_4(X) = X^2+2, & g_5(X) = X^2+X+2, & g_6(X) = X^2+2X+2 \end{array}$$

Wir überprüfen diese Polynome explizit, indem wir Polynomdivision mit Rest durchführen:
Es ist

$$(X^4+2) \div (X^2+1) = X^2+2$$

also ist $g_1(X)$ Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes. Es ist

$$(X^4+2) \div (X^2+X+1) = X^2+2X \quad \text{Rest } 2X+2$$

also ist $g_2(X)$ nicht Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes. Es ist

$$(X^4+2) \div (X^2+2X+1) = X^2+X \quad \text{Rest } 2X+2$$

also ist $g_3(X)$ nicht Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes. Ferner ist

$$(X^4+2) \div (X^2+2) = X^2+1$$

also ist $g_4(X)$ Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes. Es ist

$$(X^4+2) \div (X^2+X+2) = X^2+2X+2 \quad \text{Rest } 1$$

also ist $g_5(X)$ nicht Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes. Es ist

$$(X^4+2) \div (X^2+2X+2) = X^2+X+2 \quad \text{Rest } 1$$

also ist $g_6(X)$ nicht Erzeugerpolynom eines zyklischen $[4,2]_3$–Codes.
Damit gibt es 2 zyklische $[4,2]_3$–Codes.
Dieses Beispiel zeigt bereits, dass es für große n und große q schwierig wird, alle zyklischen Codes der Länge n zu finden. Die Mathematik stellt hierzu gewisse Hilfsmittel bereit (Primfaktorzerlegung von Polynomen), aber damit bleibt das Problem komplex.

Bemerkung 4.2.8. Die Codierung bei einem zyklischen $[n,k]_q$–Code kann natürlich (wie bei jedem linearen Code) mit Hilfe der Erzeugermatrix G erfolgen, sie kann aber auch direkt mit Hilfe des Erzeugerpolynoms $G(X) = g_0 + g_1X + \cdots + g_{n-k}X^{n-k}$ durchgeführt werden:
Dazu betrachten wir eine Nachricht $m = (m_0, \ldots, m_{k-1})$ aus dem Nachrichtenraum $\mathbb{F}_q^k$ und leiten daraus das Nachrichtenpolynom

$$m(X) = m_0 + m_1X + \cdots + m_{k-1}X^{k-1}$$

ab. Durch Polynommultiplikation erhalten wir daraus das Codepolynom

$$c(X) = m(X) \cdot G(X) = c_0 + c_1X + \cdots + c_{n-1}X^{n-1}$$

und leiten daraus das Codewort

$$c = (c_0, c_1, \ldots, c_{n-1})$$

ab. Es ist leicht zu überprüfen, dass das auch das Codewort ist, dass wir bei Codierung mit der Erzeugermatrix G erhalten.

Beispiel 4.2.13. Betrachten wir den zyklischen $[6,4]_2$–Code mit Erzeugerpolynom $G(X) = X^2+X+1$ und die Nachricht $m = (1,0,1,1)$, so erhalten wir

$$m(X) = 1 + X^2 + X^3$$

also

$$\begin{aligned} c(X) &= m(X) \cdot G(X) \\ &= (1+X^2+X^3) \cdot (1+X+X^2) \\ &= 1+X+X^5 \end{aligned}$$

und damit das Codewort

$$c = (1, 1, 0, 0, 0, 1)$$

Bemerkung 4.2.9. Zyklische Codes können über beliebigen endlichen Körpern $\mathbb{F}_q$ betrachtet werden, nicht nur über Primkörpern $\mathbb{F}_p$.

Beispiel 4.2.14. Wir betrachten den Körper $\mathbb{F}_4$, gegeben durch die Relation $\alpha^2 = \alpha + 1$.
Das Polynom $G(X) = X^3 + X^2 + \alpha \cdot X + \alpha$ definiert einen zyklischen $[6, 3]_4$–Code:
Es ist

$$(X^6 + 1) \div G(X) = X^3 + X^2 + (\alpha + 1) \cdot X + \alpha + 1 \qquad \text{Rest } 0$$

Damit ist also

$$H(X) = X^3 + X^2 + (\alpha + 1) \cdot X + \alpha + 1$$

das Paritätsprüfpolynom für diesen Code.

Beispiel 4.2.15. Wir betrachten den Körper $\mathbb{F}_8$, gegeben durch die Relation $\alpha^3 = \alpha + 1$. Dann können auch über $\mathbb{F}_8$ zyklische Codes betrachtet werden.
Das Polynom $G(X) = X^3 + (\alpha^2 + \alpha + 1) \cdot X^2 + (\alpha^2 + 1) \cdot X + \alpha + 1$ ist das Erzeugerpolynom eines zyklischen $[7, 4]_8$–Codes. Es ist

$$(X^7+1) \div G(X) = X^4 + (\alpha^2+\alpha+1) \cdot X^3 + (\alpha^2+\alpha) \cdot X^2 + X + \alpha^2 + \alpha \qquad \text{Rest } 0$$

Also ist

$$H(X) = X^4 + (\alpha^2 + \alpha + 1) \cdot X^3 + (\alpha^2 + \alpha) \cdot X^2 + X + \alpha^2 + \alpha$$

das zugehörige Paritätsprüfpolynom.

Bemerkung 4.2.10. Das Problem der Decodierung eines zyklischen $[n, k]_q$–Codes C kann ebenfalls mit Hilfe des Erzeugerpolynoms $G(X)$ angegangen werden:
Ist $a = (a_0, a_1, \ldots, a_{n-1})$ die empfangene Nachricht, so bilde das Nachrichtenpolynom

$$a(X) = a_0 + a_1 X + \cdots + a_{n-1} X^{n-1}$$

und für (über $\mathbb{F}_q$) Polynomdivision durch $G(X)$ mit Rest durch, also

$$a(X) \div G(X) = m(X) \quad \text{Rest } s(X)$$

mit einem Polynom $r(X) \in \mathbb{F}_q[X]$ vom Grad $\deg(r) \leq n-k-1$.
Falls $s(X) = 0$ und $m(X) = m_0 + m_1 X + \cdots m_{k-1} X^{k-1}$, so gilt

$$m = (m_0, m_1, \ldots, m_{k-1})$$

ist das zu a gehörige Nachrichtenwort. Falls $s(X) \neq 0$, so ist a kein Codewort von C.
Das Polynom $s(X)$ heißt **Syndrom** der Nachricht a. Im allgemeinen ist eine formelmäßige Korrektur von a aus $s(X)$ nicht möglich, für ausgewählte zyklische Codes kann diese jedoch über sogenannte Syndromtabellen erfolgen.

Beispiel 4.2.16. Wir betrachten den zyklischen $[6,4]_2$–Code C mit Erzeugerpolynom $G(X) = 1 + X + X^2$.
Ist $a = (1,1,1,1,1,1)$, so haben wir

$$a(X) = 1 + X + X^2 + X^3 + X^4 + X^5$$

und damit

$$a(X) \div G(X) = X^3 + 1 \quad \text{Rest } 0$$

Also ist a ein Codewort von C mit zugehöriger Nachricht

$$m = 1,0,0,1)$$

Ist $a = (1,1,0,0,1,1)$, so haben wir

$$a(X) = 1 + X + X^4 + X^5$$

und damit

$$a(X) \div G(X) = X^3 + X + 1 \quad \text{Rest } X$$

Also ist a kein Codewort von C

Beispiel 4.2.17. Wir betrachten den Körper $\mathbb{F}_8$ mit der Relation $\alpha^3 + 1$. Dann ist

$$G(X) = X^4 + (\alpha^2+1) \cdot X^3 + (\alpha^2+1) \cdot X^2 + (\alpha+1) \cdot X + \alpha$$

das Erzeugerpolynom eines zyklischen $[7,3]_8$–Code, denn

$$(X^7+1) \div G(X) = X^3 + (\alpha^2+1)\cdot X^2 + \alpha \cdot X^2 + \alpha^2 + 1 \qquad (\text{Rest } 0)$$

Für die empfangene Nachricht

$$a = (\alpha+1, 1, \alpha, \alpha^2, \alpha^2+\alpha, \alpha^2+1, \alpha^2+\alpha+1)$$

ist

$$\begin{aligned} a(X) &= \alpha + 1 + X + \alpha \cdot X^2 + \alpha^2 \cdot X^3 + (\alpha^2+\alpha)\cdot X^4 \\ &\quad +(\alpha^2+1)\cdot X^5 + (\alpha^2+\alpha+1)\cdot X^6 \end{aligned}$$

und es gilt

$$a(X) \div G(X) = \alpha^2 + (\alpha+1)\cdot X + (\alpha^2+\alpha+1)\cdot X^2 \quad \text{Rest } 0$$

Also ist a ein Codewort, das zur Nachricht

$$m = (\alpha^2, \alpha+1, \alpha^2+\alpha+1)$$

gehört.
Für die empfangene Nachricht

$$b = (\alpha, 1, \alpha, 1, \alpha+1, \alpha, \alpha)$$

ist

$$\begin{aligned} b(X) &= \alpha + X + \alpha \cdot X^2 + X^3 + (\alpha+1)\cdot X^4 \\ &\quad + \alpha \cdot X^5 + \alpha \cdot X^6 \end{aligned}$$

In diesem Fall gilt

$$\begin{aligned} b(X) \div G(X) &= \alpha^2 + \alpha + (\alpha+1)\cdot X + \alpha \cdot X^2 \\ &\qquad \text{Rest } (\alpha^2+\alpha)\cdot X + \alpha^2 + 1 \end{aligned}$$

Also ist b kein Codewort.

Mit Hilfe des Syndrompolynoms ist in vielen Fällen eine Fehlerkorrektur möglich.

Beispiel 4.2.18. Wir betrachten wieder den Körper $\mathbb{F}_8$ mit der Relation α^3+1 und den zyklischen $[7,3]_8$–Code mit Erzeugerpolynom

$$G(X) = X^4 + (\alpha^2+1)\cdot X^3 + (\alpha^2+1)\cdot X^2 + (\alpha+1)\cdot X + \alpha$$

In diesem Fall ist bekannt, dass C die Zuverlässigkeit $d = 5$ hat, also bis zu zwei Fehler korrigieren kann.
Wir betrachten wieder $b = (\alpha, 1, \alpha, 1, \alpha + 1, \alpha, \alpha)$, sodass also wieder

$$\begin{aligned} b(X) \div G(X) &= \alpha^2 + \alpha + (\alpha + 1) \cdot X + \alpha \cdot X^2 \\ &\quad \text{Rest } (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1 \end{aligned}$$

Also ist b kein Codewort, wie wir ja schon gesehen haben. Aus dem Syndrom $s(X) = (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1$, das nur an zwei Stellen Einträge hat, lesen wir ab, dass

$$\begin{aligned} c &= a - (\alpha^2 + 1, \alpha^2 + \alpha, 0, 0, 0, 0, 0) \\ &= (\alpha^2 + \alpha + 1, \alpha^2 + \alpha + 1, \alpha, 1, \alpha + 1, \alpha, \alpha) \end{aligned}$$

ein Codewort ist, dass sich an (höchstens) zwei Stellen von dem übertragenen Wort unterscheidet.
Das liegt in diesem Fall daran, dass das Syndrom nur so viele Terme hat wie durch die Fehlerkorrektur gegeben.
Wir betrachten dagegen $d = (\alpha^2, \alpha^2, 1, \alpha + 1, \alpha^2 + 1, \alpha + 1, \alpha + 1)$, so ist

$$\begin{aligned} d(X) \div G(X) &= \alpha^2 + \alpha + 1 + (\alpha^2 + \alpha + 1) \cdot X + (\alpha + 1) \cdot X^2 \\ &\quad \text{Rest } (\alpha^2 + \alpha) \cdot X^3 + (\alpha + 1) \cdot X^2 + (\alpha + 1) \cdot X + 1 \end{aligned}$$

Also ist auch hier d kein Codewort, aber aus dem Syndrom $s(X) = (\alpha^2 + \alpha) \cdot X^3 + (\alpha + 1) \cdot X^2 + (\alpha + 1) \cdot X + 1$ kann diesmal die Fehlerkorrektur nicht direkt abgelesen werden, da in dem Syndrom vier Terme auftreten, also mehr als die Fehlerkorrektur angibt.
Aber es gilt, dass

$$\begin{aligned} c &= a - (0, 0, 0, 0, 0, 0, \alpha^2 + \alpha + 1) \\ &= (\alpha^2, \alpha^2, 1, \alpha + 1, \alpha^2 + 1, \alpha + 1, \alpha^2) \end{aligned}$$

ein Codewort ist, dass sich an höchstens zwei Stellen (hier sogar nur an einer) von dem übertragenen Wort unterscheidet.
Das liegt daran, dass

$$\begin{aligned} (\alpha^2 + \alpha + 1) \cdot X^6 = &\left((\alpha^2 + \alpha + 1) \cdot X^2 + (\alpha^2 + \alpha) \cdot X + \alpha^2 + 1\right) \cdot G(X) \\ &+ s(X) \end{aligned}$$

Das Syndrom $s(X)$ kann also durch ein Vielfaches von $G(X)$ so abgeändert werden, dass das entstehende Polynom nur noch höchstens zwei Terme hat,

und mit dieser Abänderung kann die Fehlerkorrektur durchgeführt werden. Über Syndromtabellen kann allgemein festgestellt werden, ob für ein gegebenes Syndrom so eine Abänderung (und damit eine Fehlerkorrektur) möglich ist, und wie sie aussieht. Fehlerkorrektur

4.3 Reed–Solomon–Codes

Die für die Anwendung vielleicht wichtigste Klasse von Codes ist die der Reed–Solomon–Codes, die (teils auch in Abwandlungen und Varianten) bei der Speicherung digitalisierter Audio– oder Videodateien zum Einsatz kommen. Auch bei der Betrachtung dieser Codes spielen Polynome eine wichtige Rolle.
Ist $f(X) \in \mathbb{F}_q[X]$ ein Polynom, so können wir für die Unbekannte X ein Element $b \in \mathbb{F}_q$ einsetzen und erhalten ein Element $f(b) \in \mathbb{F}_q$.

Beispiel 4.3.1. Ist $f(X) = 3 + 2X + 4X^4 \in \mathbb{F}_7[X]$, so ist

$$F(2) = 3 + 2 \cdot 2 + 4 \cdot 2^4 = 3 + 4 + 1 = 1$$

Beispiel 4.3.2. Ist $\mathbb{F}_4$ der Körper mit 4 Elementen und definierender Relation $\alpha^2 = \alpha + 1$, und ist $f(X) = 1 + \alpha \cdot X^2 + (\alpha + 1) \cdot X^3 \in \mathbb{F}_4[X]$, so ist

$$\begin{aligned} f(\alpha) &= 1 + \alpha \cdot \alpha^2 + (\alpha + 1) \cdot \alpha^3 \\ &= 1 + \alpha^3 + \alpha^4 + \alpha^3 \\ &= 1 + \alpha^4 \\ &= 1 + \alpha^2 \cdot \alpha^2 \\ &= 1 + (\alpha + 1) \cdot (\alpha + 1) \\ &= 1 + \alpha^2 + 1 \\ &= \alpha^2 \\ &= \alpha + 1 \end{aligned}$$

Ein Polynom $f(X) \in \mathbb{F}_q[X]$ definiert also eine Abbildung

$$f : \mathbb{F}_q \longrightarrow \mathbb{F}_q, \quad b \mapsto f(b)$$

Wir betrachten nun

$$\mathscr{L}(k) = \{f(X) \in \mathbb{F}_q[X] | \deg(f) \leq k\}$$

den Raum der Polynome vom Grad $\leq k$ (über $\mathbb{F}_q$). Ferner betrachten wir n Punkte $b_1, \ldots, b_n \in \mathbb{F}_q$ (paarweise verschieden) und setzen

$$\mathscr{B} = \{b_1, \ldots, b_n\}$$

Mit der Menge $\mathscr{B}$ und dem Raum $\mathscr{L}(k)$ definieren wir die Auswertungsabbildung

$$\mathrm{Ev}_{\mathscr{B}}(k) : \mathscr{B} \longrightarrow \mathbb{F}_q^n$$

mit $\mathrm{Ev}_{\mathscr{B}}(k)(f) = (f(b_1), \ldots, f(b_n))$. Wir nehmen dabei an, dass $k < n$.

Satz 4.3.1. *Falls $k < n$, so ist die Teilmenge*

$$\begin{aligned} C &= \{\mathrm{Ev}_{\mathscr{B}}(k)(f) |\, f(X) \in \mathscr{L}\} \\ &= \{(f(b_1), \ldots, f(b_n)) |\, f(X) \in \mathscr{L}\} \quad \subseteq \quad \mathbb{F}_q^n \end{aligned}$$

ist ein linearer $[n, k+1]_q$–Code mit $d(C) = n - k$.

Beweis: Zunächst gilt für $\lambda, \mu \in \mathbb{F}_q$ und $f, g \in \mathscr{L}(k)$:

$$\begin{aligned} \mathrm{Ev}_{\mathscr{B}}(k)(\lambda f + \mu g) &= ((\lambda f + \mu g)(b_1), \ldots, (\lambda f + \mu g)(b_n)) \\ &= (\lambda f(b_1) + \mu g(b_1), \ldots, \lambda f(b_n) + \mu g(b_n)) \\ &= \lambda \cdot (f(b_1), \ldots, f(b_n)) + \mu \cdot (g(b_1), \ldots, g(b_n)) \\ &= \lambda \cdot \mathrm{Ev}_{\mathscr{B}}(k)(f) + \mu \cdot \mathrm{Ev}_{\mathscr{B}}(k)(g) \end{aligned}$$

also ist $\mathrm{Ev}_{\mathscr{B}}(k)$ eine lineare Abbildung, und damit ist $C = \mathrm{im}(\mathrm{Ev}_{\mathscr{B}}(k))$, das Bild von $\mathrm{Ev}_{\mathscr{B}}(k)$, ein Untervektorraum von $\mathbb{F}_q^n$.
Um zu zeigen, dass $\dim(C) = k+1$, reicht es, zu zeigen, dass $\mathrm{Ev}_{\mathscr{B}}(k)$ injektiv ist:
Ist dazu $f \in \mathscr{L}(k)$ mit $\mathrm{Ev}_{\mathscr{B}}(k)(f) = (0, \ldots, 0)$, so bedeutet das, dass

$$f(b_1) = 0, \ldots, f(b_n) = 0$$

und damit sind $b_1, \ldots, b_n$ Nullstellen von f. Wie über den reellen Zahlen gilt aber auch über $\mathbb{F}_q$, dass ein Polynom $f(X)$ vom Grad l (das nicht das Nullpolynom ist) höchstens l Nullstellen haben kann. Da alle Polynome in $\mathscr{L}(k)$ einen Grad $\leq k$ haben und $k < n$ ist, kann also $\mathrm{Ev}_{\mathscr{B}}(k)(f) = (0, \ldots, 0)$ nur dann gelten, wenn $f(X)$ das Nullpolynom ist.

Aufgrund der Singleton–Schranke ist klar, dass $d(C) \leq n-k$. Um zu zeigen, dass auch $d(C) \geq n-k$ gilt, ist zu zeigen, dass für $c = (c_1, \ldots, c_n) \in C \setminus \{0\}$ mindestens $n-k$ der c_i von Null verschieden sind. Dazu schreibe

$$c = \mathrm{Ev}_{\mathscr{B}}(k)(f) = f(b_1, \ldots, f(b_n))$$

Damit gilt für eine i:

$$c_i = 0 \iff f(b_i) = 0 \iff b_i \text{ ist Nullstelle von } f(X)$$

Da $c \neq 0$, kann $f(X)$ nicht das Nullpolynom sein, und da $\deg(f) \leq k$, kann $f(X)$ daher höchstens k Nullstellen haben. Deshalb muss für mindestens $n-k$ der b_i gelten $f(b_i) \neq 0$, und daraus folgt die Behauptung.

Definition 4.3.1. Der Code C heißt **dualer Reed–Solomon–Code** zu $k+1$ und $\mathscr{B}$ oder **dualer** $[n, k+1]_q$**–Reed–Solomon–Code** zu $\mathscr{B}$.

Bemerkung 4.3.1. Der duale $[n, k+1]_q$–Reed–Solomon–Code C zu $\mathscr{B}$ ist ein MDS–Code.

Die Basispolynome vom Grad $\leq k$ sind $1, X, \ldots, X^{k-1}, X^k$, und diese bilden eine Basis von $\mathscr{L}(k)$. Damit bilden ihre Bilder (unter $\mathrm{Ev}_{\mathscr{B}}(k)$) eine Basis von C, also ist eine Erzeugermatrix von C gegeben durch

$$G = \begin{pmatrix} \mathrm{Ev}_{\mathscr{B}}(k)(1) \\ \mathrm{Ev}_{\mathscr{B}}(k)(X) \\ \mathrm{Ev}_{\mathscr{B}}(k)(X^2) \\ \vdots \\ \mathrm{Ev}_{\mathscr{B}}(k)(X^k) \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & \ldots & 1 \\ b_1 & b_2 & b_3 & \ldots & b_n \\ b_1^2 & b_2^2 & b_3^2 & \ldots & b_n^2 \\ \vdots & & & \ddots & \vdots \\ b_1^k & b_2^k & b_3^k & \ldots & b_n^k \end{pmatrix}$$

Beispiel 4.3.3. Der dualen $[6,3]_{17}$–Reed–Solomon–Code C zu $\mathscr{B} = \{1,2,3,4,5,6\}$ hat die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 9 & 16 & 8 & 2 \end{pmatrix}$$

Beispiel 4.3.4. Der dualen $[6,4]_{17}$–Reed–Solomon–Code C zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat die Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 16 & 8 \\ 0 & 1 & 8 & 10 & 13 & 6 \end{pmatrix}$$

Die Zeilen $\mathbf{g_1}, \mathbf{g_2}, \mathbf{g_3}, \mathbf{g_4}$ dieser Matrix bilden eine Basis von C, und die Codierung kann durch folgende Vorschrift erfolgen

$$a = (a_1, a_2, a_3, a_4) \mapsto a_1 \cdot \mathbf{g_1} + a_2 \cdot \mathbf{g_2} + a_3 \cdot \mathbf{g_3} + a_4 \cdot \mathbf{g_4}$$

also etwa

$$\begin{aligned} (4,1,3,2) &\mapsto 4 \cdot (1,1,1,1,1,1) + 1 \cdot (0,1,2,3,4,5) \\ &\quad +3 \cdot (0,1,4,9,16,8) + 11 \cdot (0,1,8,10,13,6) \\ &= (4,10,0,3,14,11) \end{aligned}$$

Beispiel 4.3.5. Wir betrachten $\mathbb{F}_4$, gegeben durch die Relation $\alpha^2 = \alpha + 1$. Dann hat der duale $[4,2]_4$–Reed–Solomon–Code C zu $\mathscr{B} = \{0,1,\alpha,\alpha+1\}$ die Erzeugermatrix

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

Wir betrachten nun einen dualen $[n, n-k]_q$–Reed–Solomon–Code zu $\mathscr{B} = \{b_1, b_2, \ldots, b_n\}$ mit Erzeugermatrix

$$G = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_n \\ b_1^2 & b_2^2 & \ldots & b_n^2 \\ \vdots & & \ddots & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_n^{n-k-1} \end{pmatrix}$$

Beachten Sie, dass G eine Matrix vom Rang $n-k$ ist.

Definition 4.3.2. Der $[n,k]_q$–Reed–Solomon–Code C zu $\mathscr{B}$ ist der Code mit Paritätsprüfmatrix G.

Ein Code C ist also genau dann ein $[n,k]_q$–Reed–Solomon–Code, wenn es Elemente $b_1,\ldots,b_n \in \mathbb{F}_q$ gibt, so dass die Matrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_n \\ b_1^2 & b_2^2 & \ldots & b_n^2 \\ \vdots & & \ddots & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_n^{n-k-1} \end{pmatrix}$$

Paritätsprüfmatrix von C ist.

Satz 4.3.2. *Der $[n,k]_q$–Reed–Solomon–Code C zu $\mathscr{B}$ ist dual zum dualen $[n,n-k]_q$–Reed–Solomon–Code zu $\mathscr{B}$.*
Es gilt $d(C) = n-k+1$, C ist also ein MDS–Code.

Beweis: Der $[n,k]_q$–Reed–Solomon–Code C zu $\mathscr{B}$ ist nach Konstruktion dual zum dualen $[n,n-k]_q$–Reed–Solomon–Code zu $\mathscr{B}$, da eine Erzeugermatrix das dualen Codes seine Paritätsprüfmatrix ist.
Um zu zeigen, dass $d(C) = n-k+1$ ist, reicht es (aufgrund der Singleton–Schranke), zu zeigen, dass je $n-k$ Spalten der Matrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_n \\ b_1^2 & b_2^2 & \ldots & b_n^2 \\ \vdots & & \ddots & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_n^{n-k-1} \end{pmatrix}$$

linear unabhängig sind. Wir betrachten dazu beispielshaft die ersten $n-k$ Spalten. Um zu zeigen, dass diese linear unabhängig sind, reicht es zu zeigen, dass

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_{n-k} \\ b_1^2 & b_2^2 & \ldots & b_{n-k}^2 \\ \vdots & & \ddots & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_{n-k}^{n-k-1} \end{pmatrix} \neq 0$$

Das ist aber genau die Aussage der folgenden Übungsaufgabe.

Aufgabe 4.3.1. Beweisen Sie mit vollständiger Induktion, dass für einen beliebigen Körper k und für $r_1, \ldots, r_t \in k$ gilt

$$\det \begin{pmatrix} 1 & 1 & \ldots & 1 \\ r_1 & r_2 & \ldots & r_t \\ r_1^2 & r_2^2 & \ldots & r_t^2 \\ \vdots & & \ddots & \vdots \\ r_1^{t-1} & r_2^{t-1} & \ldots & r_t^{t-1} \end{pmatrix} = \prod_{i<j} (r_j - r_i)$$

Speziell ist diese Determinante also von Null verschieden, wenn die $r_1, \ldots, r_t$ paarweise verschieden sind.

Beispiel 4.3.6. Der $[6,2]_{17}$–Reed–Solomon–Code C zu $\mathscr{B} = \{0,1,2,3,4,5\}$ hat die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 9 & 16 & 8 \\ 0 & 1 & 8 & 10 & 13 & 6 \end{pmatrix}$$

Der Code C selbst ist also der Lösungsraum des zugehörigen homogenen Gleichungssystems,

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot c^\top = 0\}$$

Dieses Gleichungssystem lösen wir wie in der linearen Algebra durch Betrachtung und Umformung der zugehörigen augmentierten Matrix $(H|0)$, also von

$$A_1 = \left(\begin{array}{cccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 1 & 4 & 9 & 16 & 8 & 0 \\ 0 & 1 & 8 & 10 & 13 & 6 & 0 \end{array}\right)$$

und dadurch, dass wir diese Matrix auf Zeilen–Stufen–Form bringen.
Durch Subtraktion der zweiten Zeile von der dritten und der vierten erhalten wir

$$A_2 = \left(\begin{array}{cccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 2 & 6 & 12 & 3 & 0 \\ 0 & 0 & 6 & 7 & 9 & 1 & 0 \end{array}\right)$$

Nun dividieren wir die dritte Zeile durch 2. Beachten Sie dabei, dass $\frac{1}{2} = 9$ in $\mathbb{F}_{17}$, d.h. wir erhalten

$$A_3 = \left(\begin{array}{cccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 1 & 3 & 6 & 10 & 0 \\ 0 & 0 & 6 & 7 & 9 & 1 & 0 \end{array}\right)$$

Nun ziehen wir von der vierten Zeile das sechsfache der dritten ab und erhalten

$$A_4 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 1 & 3 & 6 & 10 & 0 \\ 0 & 0 & 0 & 6 & 7 & 9 & 0 \end{pmatrix}$$

Schließlich dividieren wir die vierte Zeile noch durch 6. Beachten Sie dabei, dass $\frac{1}{6} = 3$ in $\mathbb{F}_{17}$, wir haben also mit 3 zu multiplizieren und erhalten

$$A_5 = \left(\begin{array}{cccccc|c} 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 0 \\ 0 & 0 & 1 & 3 & 6 & 10 & 0 \\ 0 & 0 & 0 & 1 & 4 & 10 & 0 \end{array}\right)$$

Es reicht nun, das Gleichungssystem zu betrachten, dessen augmentierte Matrix A_5 ist. Wir sehen, dass x_5 und x_6 die freien Variablen sind, und wie in der linearen Algebra finden wir eine Basis des Lösungsraums, indem wir es für $x_5 = 1, x_6 = 0$ und für $x_5 = 0$, $x_6 = 1$ lösen. Dadurch erhalten wir die beiden Basislösungen

$$\mathbf{g_1} = \begin{pmatrix} 1 \\ 13 \\ 6 \\ 13 \\ 1 \\ 0 \end{pmatrix}, \quad \mathbf{g_2} = \begin{pmatrix} 4 \\ 2 \\ 3 \\ 7 \\ 0 \\ 1 \end{pmatrix}$$

Die Codierungsvorschrift ist nun gegeben durch

$$\begin{aligned} m = (m_1, m_2) &\mapsto m_1 \cdot \mathbf{g_1}^\top + m_2 \cdot \mathbf{g_2}^\top \\ &= (m_1 + 4m_2,\ 13m_1 + 2m_2,\ 6m_1 + 3m_2,\ 13m_1 + 7m_2,\ m_1,\ m_2) \end{aligned}$$

also etwa ganz konkret

$$\begin{aligned}(5,3) &\mapsto 5\cdot \mathbf{g_1}^\top + 3\cdot \mathbf{g_2}^\top \\ &= 5\cdot(1,\,13,\,6,\,13,\,1,\,0) + 3\cdot(4,\,2,\,3,\,7,\,0,\,1) \\ &= (5,\,14,\,13,\,14,\,5,\,0) + (12,\,6,\,9,\,4,\,0,\,3) \\ &= (0,\,3,\,5,\,1,\,5,\,3)\end{aligned}$$

Beachten Sie, dass bei diesem Vorgehen (bei jedem Reed–Solomon–Code) das Nachrichtenwort $m = (m_1, \ldots, m_k)$ immer in den letzten k–Stellen des Codeworts auftritt und in den ersten $n-k$ Stellen durch Redundanzen ergänzt wird.

Wir betrachten nun einen $[n,k]_q$–Reed–Solomon–Code mit Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ b_1 & b_2 & \ldots & b_n \\ b_1^2 & b_2^2 & \ldots & b_n^2 \\ \vdots & & \ddots & \vdots \\ b_1^{n-k-1} & b_2^{n-k-1} & \ldots & b_n^{n-k-1} \end{pmatrix}$$

und wir setzen

$$d = d(C) = n+1-k, \quad t = \lfloor \frac{d-1}{2} \rfloor$$

Dann ist C ein t–Fehler–korrigierender Code, d.h. zu jedem Codewort c, bei dessen Übertragung höchstens t Fehler auftreten ist c (im Sinne der Hamming–Metrik) das eindeutig bestimmte nächstliegende Codewort zum empfangenen Wort a. Im Falle des Reed–Solomon–Codes kann aus a das Wort c mit einem einfachen algebraischen Algorithmus rekonstruiert werden. Dazu betrachen wir ein $a = (a_1, \ldots, a_n) \in \mathbb{F}_q^n$.

Definition 4.3.3. Für $0 \leq l \leq n-k-1$ heißt

$$[a, X^l] = \sum_{i=1}^{n} a_i \cdot b_i^l$$

das l–**te Syndrom** von a.

Bemerkung 4.3.2. Es ist $[a, X^l]$ die $(l+1)$–te Komponente von $H \cdot a^\top$. Speziell gilt also

$$a \in C \iff [a, X^l] = 0 \quad \text{für alle } l \in \{0, \ldots, n-k-1\}$$

Ist nun a ein n–Tupel, dass aus einem Codewort c durch möglicherweise fehlerhafte Übertragung entstanden ist, so schreiben wir

$$a = c + e = (c_1, \ldots, c_n) + (e_1, \ldots, e_n)$$

mit einem Fehlerterm $e = (e_1, \ldots, e_n)$. Wir nehmen an, dass $w(e) \leq t$, dass die Anzahl der Fehler bei der Übertragung die Fehlerkorrekturschranke also nicht übersteigt.

Bemerkung 4.3.3. für alle $0 \leq l \leq n - k - 1$ gilt

$$[a, X^l] = [c, X^l] + [e, X^l] = [e, X^l]$$

Mit Hilfe der Syndrome bilden wir nur ein Gleichungssystem

$$\begin{array}{rcrcrcl} [a, X^0] \cdot Y_0 & + & [a, X^1] \cdot Y_1 & + \ldots + & [a, X^t] \cdot Y_t & = & 0 \\ [a, X^1] \cdot Y_0 & + & [a, X^2] \cdot Y_1 & + \ldots + & [a, X^{t+1}] \cdot Y_t & = & 0 \\ \vdots & & & & & & \vdots \\ [a, X^{n-k-t-1}] \cdot Y_0 & + & [a, X^{n-k-t}] \cdot Y_1 & + \ldots + & [a, X^{n-k-1}] \cdot Y_t & = & 0 \end{array} \tag{4.2}$$

mit $n - k - t$ Gleichungen und $t + 1$ Unbekannten $Y_0, Y_1, \ldots, Y_t$.

Hilfssatz 4.3.3. *Falls $w(e) \leq t$, so hat das Gleichungssystem (4.2) immer eine nicht–triviale Lösung $\eta = (\eta_0, \ldots, \eta_t)$. Setzen wir*

$$L(X) = \eta_0 + \eta_1 \cdot X + \eta_2 \cdot X^2 + \cdots + \eta_t \cdot X^t$$

und ist $r \in \{1, \ldots, n\}$ mit $e_r \neq 0$ (ist also r ein Fehlerstelle von a), so gilt

$$L(b_r) = 0$$

Definition 4.3.4. Das Polynom $L(X)$ heißt **fehlerlokalisierendes Polynom** von a.

Bemerkung 4.3.4. Das Gleichungssystem (4.2) kann viele nicht–triviale Lösungen haben (auch nicht linear abhängige). Daher kann es viele verschiedene fehlerlokalisierende Polynome geben. Neben den fehlerhaften Stellen können diese auch noch an anderen der $b_1, \ldots, b_n$ (an denen a nicht fehlerhaft ist) verschwinden. Die Fehlerstellen von a gehören jedoch immer zu den Nullstellen.

Bemerkung 4.3.5. Das Gleichungssystem (4.2) kann auch im Fall $w(e) > t$ nicht–triviale Lösungen haben. Allerdings führen sie in diesem Fall nicht zu einem fehlerlokalisierendem Polynom.

Wir nehmen nun an, dass wir mit Hilfe von Gleichungssystem (4.2) ein fehlerlokalsierendes Polynom $L(X)$ gefunden haben und setzen

$$N(L) = \{i = \{1, \ldots, n\} | \, L(b_i) = 0\}$$

Dann enthält $N(L)$ alle Fehlerstellen von a. Wir schreiben

$$N(L) = \{i_1, \ldots, i_\tau\}$$

(für ein $\tau \leq t$) und betrachten das lineare Gleichungssystem

$$\begin{array}{rcrcrcl} 1 \cdot E_{i_1} & + & 1 \cdot E_{i_2} & + \ldots + & 1 \cdot E_{i_\tau} & = & [a, X^0] \\ b_{i_1} \cdot E_{i_1} & + & b_{i_2} \cdot E_{i_2} & + \ldots + & b_{i_{tau}} \cdot E_{i_\tau} & = & [a, X^1] \\ \vdots & & & & & & \vdots \\ b_{i_1}^{n-k-1} \cdot E_{i_1} & + & b_{i_2}^{n-k-1} \cdot E_{i_2} & + \ldots + & b_{i_{tau}}^{n-k-1} \cdot E_{i_\tau} & = & [a, X^{n-k-1}] \end{array} \tag{4.3}$$

mit $n - k$ Gleichungen in den Unbekannten $E_{i_1}, \ldots, E_{i_\tau}$.

Hilfssatz 4.3.4. *Falls $w(e) \leq t$, so hat das Gleichungssystem (4.3) immer eine eindeutige nicht–triviale Lösung $(\varepsilon_{i_1}, \ldots, \varepsilon_{i_\tau})$. Setzen wir $\varepsilon_i = 0$ für $i \in \{1, \ldots, n\} \setminus N(L)$, so ist*

$$e = (\varepsilon_1, \ldots, \varepsilon_n)$$

der Fehlerterm von a und

$$c = a - e$$

ist das Codewort c, das zu a gehört.

Bemerkung 4.3.6. Das Gleichungssystem (4.3) kann auch für $w(e) > t$ Lösungen haben. In diesem Fall ist

$$\widetilde{c} = a - (\varepsilon_1, \ldots, \varepsilon_n)$$

ebenfalls ein Codewort von C, allerdings ist es nicht das Codewort aus dem a durch fehlerhafte Übertragung entstanden ist. In diesem Fall sind bei der

Übertragung so viele Fehler aufgetreten, dass das übertragene Wort näher an einem anderen Codewort liegt als an dem Ausgangswort. Dieser Fall tritt aber (im Sinne des Maximum–Likelihood–Decodings) selten auf und kann in der Praxis ignoriert werden.

Die Decodierung eines $[n,k]_q$–Reed–Solomon–Codes bei einer empfangenen Nachricht $a \in \mathbb{F}_q^n$ kann nun wie folgt beschreiben werden:

1. Bestimme den Minimalabstand $d = n - k + 1$ und die Fehlerkorrekturschranke $t = \lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{n-k}{2} \rfloor$.

2. Bestimme die Syndrome $[a,1], [a,X], \ldots, [a,X^{n-k-1}]$.

   Falls alle Syndrome verschwinden, so ist a ein Codewort und eine Fehlerkorrektur ist nicht erforderlich. STOPP.

3. Bestimme eine nicht–triviale Lösung des linearen Gleichungssystems

$$\begin{array}{rcrcrcl} [a,X^0]\cdot Y_0 & + & [a,X^1]\cdot Y_1 & + \ldots + & [a,X^t]\cdot Y_t & = & 0 \\ [a,X^1]\cdot Y_0 & + & [a,X^2]\cdot Y_1 & + \ldots + & [a,X^{t+1}]\cdot Y_t & = & 0 \\ \vdots & & & & & & \vdots \\ [a,X^{n-k-t-1}]\cdot Y_0 & + & [a,X^{n-k-t}]\cdot Y_1 & + \ldots + & [a,X^{n-k-1}]\cdot Y_t & = & 0 \end{array} \tag{4.4}$$

   Falls Gleichungssystem 4.4 keine nicht–triviale Lösung hat, so kann das Wort a nicht korrigiert werden. STOPP

4. Ist $\eta = (\eta_0, \ldots, \eta_t)$ eine nicht–triviale Lösung des Gleichungssystems 4.4, so bestimme das fehlerlokalisierende Polynom $L(X) = \eta_0 + \eta_1 X + \cdots + \eta_t X^t$, bestimme

$$N(L) = \{i = \{1, \ldots, n\} |\, L(b_i) = 0\}$$

   und schreibe

$$N(L) = \{i_1, \ldots, i_\tau\}$$

5. Bestimme eine Lösung des linearen Gleichungssystems

$$\begin{array}{rcrcrcl} 1 \cdot E_{i_1} & + & 1 \cdot E_{i_2} & + \ldots + & 1 \cdot E_{i_\tau} & = & [a, X^0] \\ b_{i_1} \cdot E_{i_1} & + & b_{i_2} \cdot E_{i_2} & + \ldots + & b_{i_{tau}} \cdot E_{i_\tau} & = & [a, X^1] \\ \vdots & & & & & & \vdots \\ b_{i_1}^{n-k-1} \cdot E_{i_1} & + & b_{i_2}^{n-k-1} \cdot E_{i_2} & + \ldots + & b_{i_{tau}}^{n-k-1} \cdot E_{i_\tau} & = & [a, X^{n-k-1}] \end{array} \tag{4.5}$$

   Falls Gleichungssystem 4.5 keine Lösung hat, so kann das Wort a nicht korrigiert werden. STOPP

6. Ist $(\varepsilon_{i_1}, \ldots, \varepsilon_{i_\tau})$ eine Lösung von Gleichungssystem 4.5, so setze $\varepsilon_i = 0$ für $i \in \{1, \ldots, n\} \setminus N(L)$ und

$$c = a - (\varepsilon_1, \ldots, \varepsilon_n)$$

   und gebe c als gesuchtes Codewort aus.

Beispiel 4.3.7. Wir betrachten den $[6, 2]_{11}$–Reed–Solomon–Code C bezüglich der Punkte $b_1 = 1$, $b_2 = 2$, $b_3 = 3$, $b_4 = 4$, $b_5 = 5$, $b_6 = 6$. Wir wollen überprüfen, ob das Wort $a = (10, 8, 10, 2, 4, 1)$ decodiert werden kann undgegebenenfalls das zugehörige Codewort c bestimmen.

Zunächst ist die Paritätsprüfmatrix von C gegeben als:

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 9 & 5 & 3 & 3 \\ 1 & 8 & 5 & 9 & 4 & 7 \end{pmatrix}$$

1. Der Code C hat Zuverlässigkeit $d(C) = 5$ und die Fehlerkorrekturschranke $t = 2$.

2. Die Syndrome von a sind gegeben als

$$\begin{array}{rcl} [a, X^0] & = & 2 \\ [a, X^1] & = & 2 \\ [a, X^2] & = & 3 \\ [a, X^3] & = & 0 \end{array}$$

   Damit ist das Wort a sicherlich kein Codewort.

3. Zur Bestimmung des fehlerlokalisierenden Polynoms betrachten wir zunächst das lineare Gleichungssystem

$$\begin{array}{rcrcrcl} 2Y_0 & + & 2Y_1 & + & 3Y_2 & = & 0 \\ 2Y_0 & + & 3Y_1 & & & = & 0 \end{array}$$

über $\mathbb{F}_{11}$. Die zugehörige Koeffizientenmatrix ist

$$A = \begin{pmatrix} 2 & 2 & 3 \\ 2 & 3 & 0 \end{pmatrix}$$

mit Normalform

$$B = \begin{pmatrix} 1 & 1 & 7 \\ 0 & 1 & 8 \end{pmatrix}$$

und Grundlösung des zugehörigen homogenen Gleichungssystems

$$l = (1, 3, 1)$$

Insbesondere hat dieses Gleichungssystem nicht–triviale Lösungen.

4. Aus l erhalten wir als fehlerlokalisierendes Polynom

$$L(x) = 1 + 3X + X^2$$

Einsetzen (in $\mathbb{F}_{11}$) ergibt

$$\begin{array}{rcrcl} L(b_1) & = & L(1) & = & 5 \\ L(b_2) & = & L(2) & = & 0 \\ L(b_3) & = & L(3) & = & 8 \\ L(b_4) & = & L(4) & = & 7 \\ L(b_5) & = & L(5) & = & 8 \\ L(b_6) & = & L(6) & = & 0 \end{array}$$

Also gilt $L(b_2) = 0$ und $L(b_6) = 0$, und damit können Fehler an den Stellen 2 und 6 vorliegen.

5. Zur Fehlerbestimming betrachten wir das Gleichungssystem

$$\begin{array}{rcrcl} E_2 & + & E_6 & = & 2 \\ 2E_2 & + & 6E_6 & = & 2 \\ 4E_2 & + & 3E_6 & = & 3 \\ 8E_2 & + & 7E_6 & = & 0 \end{array}$$

über $\mathbb{F}_{11}$. Dieses System hat augmentierte Koeffizientenmatrix

$$A = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 2 & 6 & 2 \\ 4 & 3 & 3 \\ 8 & 7 & 0 \end{array}\right)$$

mit Normalform

$$B = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 5 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Wir erhalten die eindeutige Lösung $e_2 = 8$ und $e_6 = 5$.

6. Setzen wir $e_1 = e_3 = e_4 = e_5 = 0$, so erhalten wir als Fehlerterm

$$e = (0,\, 8,\, 0,\, 0,\, 0,\, 5)$$

und als korrigiertes Wort

$$c = (10,\, 8,\, 10,\, 2,\, 4,\, 1) - (0,\, 8,\, 0,\, 0,\, 0,\, 5) = (10,\, 0,\, 10,\, 2,\, 4,\, 7)$$

Die gesendete Nachricht war also

$$m = (4,\, 7)$$

Kapitel 5

Beispiele und Anwendungen

Im Zuge der zunehmenden Digitalisierung aller Lebensbereiche wird die Codierungstheorie zur Absicherung der Zuverlässigkeit der Speicherung und Übertragung von Daten immer aktueller. In neuerer Zeit gewinnt die Codierungstheorie jedoch auch unter dem Gesichtspunkt von Sicherheitsüberlegungen immer mehr Bedeutung.

5.1 Das Bespiel der CD–Codierung

Der Durchbruch der Codierungstheorie begann mit dem Aufkommen der CD zu Beginn der 1980–iger Jahre. Hier wurde erstmals in großem Umfang und im industriellen Maßstab Codierungstheorie eingesetzt, um digitalisierte Audiodaten zuverlässig abzuspeichern und wieder auszulesen.
Um Musik auf einer CD abzuspeichern, wird diese zunächst digitalisiert. Nach dem Shannon–Nyquist Sampling Theorem sind für die diskrete Speicherung von Musik im Rahmen des menschlichen Hörbereichs (5 Hertz bis 20 000 Hertz) 44 100 Messwerte (**Abtastungen**) pro Sekunde erforderlich. Jede Messwert wird in Form eines **Audiobits**, also in 16 Bits abgelegt. Bei Stereowiedergabe bedeutet das, dass pro Sekunde ein Datenstrom von

$$d = 44\,100 \cdot 16 \cdot 2 = 1\,411\,200$$

Binärdaten erforderlich ist.
Der entstandene Datenstrom wird durch winzigste Einkerbungen auf der CD dargestellt.

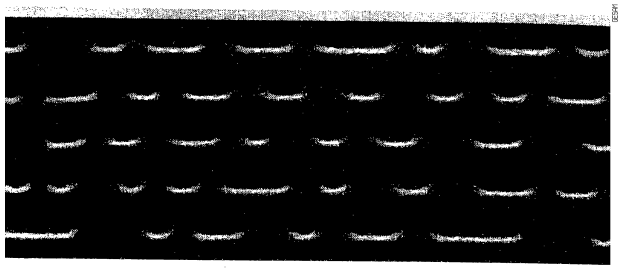


Abbildung 5.1: Vergrößerter Ausschnitt einer CD

Die Datenspur auf einer CD haben eine Breite von 1.6 μm. Eine Einkerbung (ein **Pit**) ist dabei 0.12 μm tief, 0.6 μm breit und mindestens 0.9 μm lang (maximal 3.3 μm). Der Bereich zwischen zwei Pits (das sogenannte **land**) hat ebenfalls eine Länge zwischen 0.9 μm und 3.3 μm. Fehler treten schon durch kleinste Kratzer und Verunreinigungen auf
Bei der Entwicklung der Codierung der CD wurden den beteiligten Ingenieuren und Mathematikern die folgendne Anforderungen gegeben, die berücksichtigt werden mussten:

1. Vereinzelt (aber regelmäßig) auftretende Lesefehler müssen korrigiert werden können (**sporadic error correction**).

2. Selten auftretende Kratzer bis zu einer Breite von 0.2 mm müssen fehlerfrei korrigiert werden können (**burst error correction**).

3. Selten auftretende Kratzer bis zu einer Breite von 0.7 mm müssen näherungsweise korrigiert werden können.

Der letzte Punkt ist eine Frage von Interpolationstechniken und hat nichts mit der Codierungstheorie zu tun. Die anderen beiden Punkte müssen jedoch mit Methoden der Codierungstheorie behandelt werden.
Die Technik, die bei der Nachrichtencodierung auf einer CD benutzt wird, ist die der **cross interleaved Reed–Solomon**–Codes (CIRS–Codes). Das Alphabet, über dem gearbeitet wird, ist dabei $\mathbb{A} = \mathbb{F}_{2^8} = \mathbb{F}_{256}$, der Raum der Bytes.
Für den CD–Spieler benutzt man dabei zwei solche Codes, einen $[28, 24]$–Reed–Solomon Code C_1 der Zuverlässigkeit 5 und ein $[32, 28]$–Reed–Solomon

Code C_2, ebenfalls mit Zuverlässigkeit 5. Diese beiden Codes werden nicht einfach hintereinandergeschaltet sondern in geeigneter Weise miteinander (zur Tiefe 28) verflochten (**interleaving**).
Der Körper $\mathbb{F}_{256}$ wird durch die Relation $\alpha^8 = \alpha^4 + \alpha^3 + \alpha^2 + 1$ definiert. Der $[28, 24]$–Reed–Solomon Code C_1 wird gebildet bezüglich der Punkte $\alpha^{27}, \alpha^{26}, \ldots, \alpha^2, \alpha, 1$, hat also die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ \alpha^{27} & \alpha^{26} & \ldots & \alpha^2 & \alpha & 1 \\ \alpha^{54} & \alpha^{52} & \ldots & \alpha^4 & \alpha^2 & 1 \\ \alpha^{81} & \alpha^{78} & \ldots & \alpha^6 & \alpha^3 & 1 \end{pmatrix}$$

Dieser Code C_1 hat die Zuverlässigkeit $d = 5$ und die Fehlerkorrekturschranke $t = 2$.
Der $[32, 28]$–Reed–Solomon Code C_2 wird gebildet bezüglich der Punkte $\alpha^{31}, \alpha^{30}, \ldots, \alpha^2, \alpha, 1$, hat also die Paritätsprüfmatrix

$$H = \begin{pmatrix} 1 & 1 & \ldots & 1 & 1 & 1 \\ \alpha^{31} & \alpha^{30} & \ldots & \alpha^2 & \alpha & 1 \\ \alpha^{62} & \alpha^{60} & \ldots & \alpha^4 & \alpha^2 & 1 \\ \alpha^{93} & \alpha^{90} & \ldots & \alpha^6 & \alpha^3 & 1 \end{pmatrix}$$

Dieser Code C_2 hat ebenfalls die Zuverlässigkeit $d = 5$ und die Fehlerkorrekturschranke $t = 2$.
Wir betrachten zunächst einen Block von 28 Nachrichtenwörter $m_1, \ldots, m_{28}$ und benutzen den Code C_1 um diese 28 Nachrichtenwörter $m_1, \ldots, m_{28} \in \mathbb{F}_{256}^{24}$ zu Codewörtern $c_1, \ldots, c_{28}$ zu codieren. Wir schreiben

$$c_i = (c_{i,1}, \ldots c_{i,28})$$

und notieren diese c_i als die Zeilen einer 28×28–Matrix,

$$A = \begin{pmatrix} c_{1,1} & c_{1,2} & \ldots & c_{1,27} & c_{1,28} \\ c_{2,1} & c_{2,2} & \ldots & c_{2,27} & c_{2,28} \\ \vdots & & \ddots & & \vdots \\ c_{28,1} & c_{28,2} & \ldots & c_{28,27} & c_{28,28} \end{pmatrix}$$

Diese Matrix A wird jetzt transponiert,

$$B = A^\top = \begin{pmatrix} c_{1,1} & c_{2,1} & \dots & c_{27,1} & c_{28,1} \\ c_{1,2} & c_{2,2} & \dots & c_{27,2} & c_{28,2} \\ \vdots & & \ddots & & \vdots \\ c_{1,28} & c_{2,28} & \dots & c_{27,28} & c_{28,28} \end{pmatrix}$$

Aus den Zeilen von B werden neue Nachrichtenwörter $d_1, \dots, d_{28}$, jetzt der Länge 28, gebildet, wobei

$$d_j = (c_{1,j}, c_{2,j}, \dots, c_{27,j}, c_{28,j})$$

Jedes dieser neuen Nachrichtenwörter d_j enthält also aus den ursprünglichen Codewörtern genau einen Buchstaben, und zwar an der Stelle i den j–ten Buchstaben des i–ten Codeworts c_i.
Diese Wörter d_j werden nun mit C_2 zu neuen Codewörtern $\widetilde{c_j}$ codiert, und diese Wörter $\widetilde{c_1}, \dots, \widetilde{c_{28}}$ werden gespeichert und auf der CD abgelegt.
Es soll ein Block von 28 gespeicherten Wörtern $a_1, \dots, a_{28}$ decodiert werden. Dabei nehmen wir an, dass dieser Block durch einen Kratzer beschädigt wurde und darüberhinaus beim Auslesen vereinzelte Fehler auftreten. Zur Vereinfachung der Notation wollen wir annehmen, dass die beiden ersten Wörter a_1 und a_2 von dem Kratzer betroffen sind und dadurch zu einem großen Teil zerstört wurden. Die sporadischen Fehler erstrecken sich über die Wörter a_3 bis a_{28}.
Die sporadischen Fehler in den Wörtern a_3 bis a_{28} können durch den Code C_2 korrigiert werden. Dadurch können die Nachrichten $d_3, \dots, d_{28}$ korrekt wieder hergestellt werden. Die Wörter a_1 und a_2 sind so stark durch Fehler betroffen, dass sie als zerstört markiert werden. Damit können d_1 und d_2 nicht rekonstruiert werden.
Die Matrix B kann also nur teilweise wiederhergestellt werden und wir erhalten:

$$\widetilde{B} = \begin{pmatrix} — & — & \cdots & — & — \\ — & — & \cdots & — & — \\ c_{1,3} & c_{2,3} & \dots & c_{27,3} & c_{28,3} \\ c_{1,4} & c_{2,4} & \dots & c_{27,4} & c_{28,4} \\ \vdots & & \ddots & & \vdots \\ c_{1,28} & c_{2,28} & \dots & c_{27,28} & c_{28,28} \end{pmatrix}$$

Die ersten beiden Zeilen können nicht rekonstruiert werden, der Rest ist allerdings korrekt.
Zum Rückgängigmachen des Transponierens muss die Matrix wieder transponiert werden,

$$\widetilde{A} = \widetilde{B}^{\top} = \begin{pmatrix} \_ & \_ & c_{1,3} & c_{1,4} & \dots & c_{1,27} & c_{1,28} \\ \_ & \_ & c_{2,3} & c_{2,4} & \dots & c_{2,27} & c_{1,28} \\ \vdots & & \vdots & & \ddots & & \vdots \\ \_ & \_ & c_{28,3} & c_{28,4} & \dots & c_{28,27} & c_{28,28} \end{pmatrix}$$

Auch A kann also nicht wiederhergestellt werden. Die ersten beiden Spalten von A fehlen in $\widetilde{A}$, der Rest von $\widetilde{A}$ stimmt allerdings schon komplett mit A überein.
Wir verarbeiten jetzt die **Zeilen** von $\widetilde{A}$, also

$$\widetilde{c_j} = (\_, \_, c_{j,3}, c_{j,4}, \dots, c_{j,27}, c_{j,28})$$

wobei die Stellen $c_{j,3}$ bis $c_{j,28}$ korrekte Buchstaben des ursprünglichen Codewortes c_j sind.
Da der Code C_1 zwei Fehler korrigieren kann, kann aus $\widetilde{c_j}$ das Wort c_j zurückgewonnen werden. Zu beachten ist hierbei, dass der aufwendige Schritt der Bestimmung der Fehlerstellen hier entfällt. Die potentiellen Fehlerstellen sind schon aus dem ersten Schritt der Decodierung übergeben worden. Dieser Schritt hat auch nicht mehr die Aufgabe, sporadische Fehler zu erkennen und zu korrigieren, das geschieht einzig und allein im ersten Schritt. Aus c_j schließlich kann m_j rekonstruiert werden.

Beispiel 5.1.1. Die Technik des cross–interleavings von Reed–Solomon–Codes soll hier an einem vereinfachten Beispiel erläutert werden. Wir betrachten dazu einen $[5,3]_{29}$–Reed–Solomon–Code C_1, gegeben durch $0,1,2,3,4$, und einen $[7,3]_{29}$–Reed–Solomon–Code C_2, gegeben durch die Punkte $0,1,2,3,4,5,6$. Jeder dieser Codes kann also einen Fehler korrigieren. Die beiden Codes haben die Paritätsprüfmatrizen

$$H_1 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \end{pmatrix}$$

und

$$H_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$

und Erzeugermatrizen hierzu sind

$$G_1 = \begin{pmatrix} 1 & 27 & 1 & 0 & 0 \\ 2 & 26 & 0 & 1 & 0 \\ 3 & 25 & 0 & 0 & 1 \end{pmatrix}$$

und

$$G_2 = \begin{pmatrix} 1 & 27 & 1 & 0 & 0 & 0 & 0 \\ 2 & 26 & 0 & 1 & 0 & 0 & 0 \\ 3 & 25 & 0 & 0 & 1 & 0 & 0 \\ 4 & 24 & 0 & 0 & 0 & 1 & 0 \\ 5 & 25 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Das Alphabet mit 29 Buchstaben haben wir gewählt, weil dadurch die Buchstaben des Alphabets, einschließlich der Umlaute, abgebildet werden können (wobei A mit 0, B mit 1, usw. bis Z mit 25, mit 26, mit 27 und mit 28 identifiziert wird). Damit soll der Text

$$m = \text{Rat und Tat vor Ort}$$

codiert und nach einer fehlerhaften Übertragung wieder decodiert werden. Dieser Satz übersetzt sich in die folgenden 5 Nachrichtenwörter,

$m_1 = (17, 0, 19)$, $m_2 = (20, 13, 3)$, $m_3 = (19, 0, 19)$, $m_4 = (21, 14, 17)$, $m_5 = (14, 17, 19)$

Codierung mit dem Code C_1 macht daraus die folgenden Codewörter

$$\begin{aligned} c_1 &= (16, 6, 17, 0, 19) \\ c_2 &= (26, 25, 20, 13, 3) \\ c_3 &= (18, 2, 19, 0, 19) \\ c_4 &= (13, 22, 21, 14, 17) \\ c_5 &= (18, 19, 14, 17, 19) \end{aligned}$$

also die Matrix

$$A = \begin{pmatrix} 16 & 6 & 17 & 0 & 19 \\ 26 & 25 & 20 & 13 & 3 \\ 18 & 2 & 19 & 0 & 19 \\ 13 & 22 & 21 & 14 & 17 \\ 18 & 19 & 14 & 17 & 19 \end{pmatrix}$$

Transponieren liefert dann die Matrix

$$B = A^\top = \begin{pmatrix} 16 & 26 & 18 & 13 & 18 \\ 6 & 25 & 2 & 22 & 19 \\ 17 & 20 & 19 & 21 & 14 \\ 0 & 13 & 0 & 14 & 17 \\ 19 & 3 & 19 & 17 & 19 \end{pmatrix}$$

Daraus erhalten wir die neuen Nachrichtenwörter

$$\begin{aligned} d_1 &= (16, 26, 18, 13, 18) \\ d_2 &= (6, 25, 2, 22, 19) \\ d_3 &= (17, 20, 19, 21, 14) \\ d_4 &= (0, 13, 0, 14, 17) \\ d_5 &= (19, 3, 19, 17, 19) \end{aligned}$$

Wenn wir diese mit C_2 codieren, so erhalten wir schließlich die Codewörter

$$\begin{aligned} \widetilde{c_1} &= (3, 22, 16, 26, 18, 13, 18) \\ \widetilde{c_2} &= (13, 0, 6, 25, 2, 22, 19) \\ \widetilde{c_3} &= (7, 18, 17, 20, 19, 21, 14) \\ \widetilde{c_4} &= (22, 21, 0, 13, 0, 14, 17) \\ \widetilde{c_5} &= (13, 26, 19, 3, 19, 17, 19) \end{aligned}$$

In dieser Form wird der ursprüngliche Text jetzt abgelegt.
Beim Wiederauslesen dieses Blocks treten sporadische Fehler und Blockfehler auf, und wir erhalten

$$\begin{aligned} \widetilde{a_1} &= (3, 22, 16, 26, 18, 3, 18) \\ \widetilde{a_2} &= (13, 0, 6, 25, 2, 22, 19 \\ \widetilde{a_3} &= (7, 18, 17, 20, 24, 21, 14) \\ \widetilde{a_4} &= (22, \_, \_, \_, \_, \_, 17) \\ \widetilde{a_5} &= (13, 26, 19, 3, 19, 17, 1) \end{aligned}$$

Wir haben also drei sporadische Auslesefehler und eine zum großen Teil zerstörten Block im Wort a_4. Dieses Wort kann aus seinen Resten mit C_2 nicht mehr rekonstruiert werden, die sporadischen Fehler lassen sich dagegen damit beheben, da hier immer maximal einer pro Wort auftritt. Nutzen wir

also des Fehlerkorrekturpotential von C_2 aus, so erhalten wir daraus vier Nachrichtenwörter und ein nicht lesbares Wort,

$$\begin{aligned}
\widetilde{d_1} &= (16, 26, 18, 13, 18) \\
\widetilde{d_2} &= (6, 25, 2, 22, 19) \\
\widetilde{d_3} &= (17, 20, 19, 21, 14) \\
\widetilde{d_4} &= (_, _, _, _, _) \\
\widetilde{d_5} &= (19, 3, 19, 17, 19)
\end{aligned}$$

also in Matrizenschreibweise

$$\widetilde{B} = \begin{pmatrix} 16 & 26 & 18 & 13 & 18 \\ 6 & 25 & 2 & 22 & 19 \\ 17 & 20 & 19 & 21 & 14 \\ \_ & \_ & \_ & \_ & \_ \\ 19 & 3 & 19 & 17 & 19 \end{pmatrix}$$

bzw. nach Transponieren

$$\widetilde{A} = \begin{pmatrix} 16 & 6 & 17 & \_ & 19 \\ 26 & 25 & 20 & \_ & 3 \\ 18 & 2 & 19 & \_ & 19 \\ 13 & 22 & 21 & \_ & 17 \\ 18 & 19 & 14 & \_ & 19 \end{pmatrix}$$

also als Input für die Decodierung mit Code C_1 die Wörter

$$\begin{aligned}
a_1 &= (16, 6, 17, _, 19) \\
a_2 &= (26, 25, 20, _, 3) \\
a_3 &= (18, 2, 19, _, 19) \\
a_4 &= (13, 22, 21, _, 17) \\
a_5 &= (18, 19, 14, _, 19)
\end{aligned}$$

Es ist bereits klar, dass der Fehler an der Position 4 aufgetreten ist, die Bestimmung der Fehlerstelle entfällt also hier. Für die Fehlerbestimmung werden aber trotzdem die Syndrome benötigt. Dazu setzen wir für die feh-

lerhaften Stellen einfach den Wert 0 ein, arbeiten also mit

$$\begin{aligned} a_1 &= (16, 6, 17, 0, 19) \\ a_2 &= (26, 25, 20, 0, 3) \\ a_3 &= (18, 2, 19, 0, 19) \\ a_4 &= (13, 22, 21, 0, 17) \\ a_5 &= (18, 19, 14, 0, 19) \end{aligned}$$

Damit erhalten wir für a_1 die Syndrome

$$[a_1, X^0] = 0, \quad [a_1, X^1] = 0$$

Wir haben also mit der 0 zufällig schon den korrekten Wert eingesetzt, a_1 wird dadurch fehlerfrei, und nach Entfernung der Redundanzen bleibt

$$m_1 = (17, 0, 19)$$

Zur Korrektur von a_2 berechnen wir dessen Syndrome und erhalten

$$[a_2, X^0] = 16, \quad [a_1, X^1] = 19$$

Damit ist nun das lineare Gleichungssystem

$$\begin{aligned} 1 \cdot E_4 &= 16 \\ 3 \cdot E_4 &= 19 \end{aligned}$$

und dieses Gleichungssystem hat die eindeutige Lösung $e_4 = 16$. Dadurch erhalten wir

$$c_2 = (26, 25, 20, 0, 3) - (0, 0, 0, 16, 0) = (26, 25, 20, 13, 3)$$

also nach Entfernung der Redundanzen

$$m_2 = (20, 13, 3)$$

Der Umweg über die Syndrome wäre in dieser Situation jedoch nicht nötig. Da wir schon wissen, dass in jedem Wort alle vorhandenen Einträge (also alle Buchstaben mit Ausnahme des vierten) korrekt sind, können wir gleich

mit den Paritätsprüfgleichungen arbeiten und erhalten etwa für das erste Codewort das Gleichungssystem

$$\begin{array}{rcrcrcrcrcr} 1\cdot 16 & + & 1\cdot 6 & + & 1\cdot 17 & + & 1\cdot c_{1,4} & + & 1\cdot 19 & = & 0 \\ 0\cdot 16 & + & 1\cdot 6 & + & 2\cdot 17 & + & 3\cdot c_{1,4} & + & 4\cdot 19 & = & 0 \end{array}$$

Daraus wird (in $\mathbb{F}_{19}$)

$$\begin{array}{rcrcr} c_{1,4} & + & 0 & = & 0 \\ 3\cdot c_{1,4} & + & 0 & = & 0 \end{array}$$

mit der eindeutigen Lösung $c_{1,4} = 0$, sodass wir also wieder

$$c_1 = (16, 6, 17, 0, 19), \quad m_1 = (27, 0, 29)$$

erhalten. Entsprechend ergibt sich für c_2 das Gleichungssystem

$$\begin{array}{rcrcrcrcrcr} 1\cdot 26 & + & 1\cdot 25 & + & 1\cdot 20 & + & 1\cdot c_{2,4} & + & 1\cdot 3 & = & 0 \\ 0\cdot 26 & + & 1\cdot 25 & + & 2\cdot 20 & + & 3\cdot c_{2,4} & + & 4\cdot 3 & = & 0 \end{array}$$

Daraus wird (in $\mathbb{F}_{19}$)

$$\begin{array}{rcrcr} c_{2,4} & + & 16 & = & 0 \\ 3\cdot c_{2,4} & + & 19 & = & 0 \end{array}$$

mit der eindeutigen Lösung $c_{2,4} = 13$, sodass wir also auch hier wieder

$$c_2 = (26, 25, 20, 13, 3), \quad m_2 = (20, 13, 3)$$

erhalten.
Genauso verfahren wir mit a_3, a_4 und a_5 und erhalten

$$m_3 = (19, 0, 19), \quad m_4 = (21, 14, 17), \quad m_5 = (14, 17, 19)$$

also in der Tat die Ausgangsnachricht.

Bemerkung 5.1.1. Der Durchbruch der Reed–Solomon–Codes kam sicherlich 1982 mit Einführung der CD. Sie kamen und kommen jedoch auch in vielen anderen Anwendungen zum Einsatz:

- Die NASA benutzte Reed–Solomon–Codes 1977 im Voyager–Programm.
- Die QR–Codes nutzen Reed–Solomon–Codes zur Fehlerkorrektur.
- Der DAB–Standard nutzt Reed–Solomon–Codes.
- Diverse Mobilfunkstandards benutzen Reed–Solomon–Codes.

5.2 Code–basierte Kryptosysteme

Für allgemeine lineare Codes ist die Fehlerkorrektur und Decodierung ein sehr hartes Problem. Im wesentlichen gibt es (nach heutigem Wissen) nichts besseres als eine vollständige Suche durch alle Codewörter, um das mit dem geringsten Abstand zu finden. Bei größeren Codes ist das naturgemäß extrem aufwendig und selbst mit Computerhilfe nicht in akzeptabler Zeit lösbar. Nur bei ausgewählten Verfahren ist es aufgrund zusätzlicher Kenntnisse möglich, die Decodierung zu beschleunigen und in akzeptabler Zeit durchzuführen. Bei den Reed–Solomon–Codes etwa ist die Kenntnis der Punkte, die in der Konstruktion benutzt wurden, notwendig, um daraus einen schnellen Decodierer zu konstruieren. Sind diese Punkte nicht bekannt, so ist das nicht möglich. Das hat den Mathematiker und Kryptographen Robert J. Eliece schon 1978 inspiriert, kryptographische Protokolle vorzuschlagen, die auf linearen Codes basieren. Dieser Ansatz wurde lange Zeit wenig beachtet, da er sehr viel aufwendiger ist als etwa das RSA–Verfahren, in letzter Zeit steigt aber das Interesse daran, da diese Verfahren im Gegensatz zu dem RSA–Verfahren oder zu Diffie–Hellman durch Quantenalgorithmen (aktuell) nicht kompromittiert werden können.
Die prinzipielle Vorgehensweise zur Bestimmung eines code–basierten public key Kryptosystems ist wie folgt:

Schlüsselerzeugung:
Bob erzeugt ein Schlüsselpaar wie folgt:

1. Bob wählt ein t–fehlerkorrigierendes $[n,k]_q$–Codierungsverfahren C mit bekanntem Decodierungsverfahren, das sich nicht direkt aus einer Erzeugermatrix ergibt, aus.

2. Bob bestimmt eine Erzeugermatrix G von C.

3. Bob bestimmt das Decodierungsverfahren D von C.

Der öffentliche Schlüssel von Bob ist des paar (G,t), bestehend aus der Erzeugermatrix G und der Fehlerkorrekturschranke t,

$$k_{\text{pub}} = (G,t)$$

Der private Schlüssel von Bob ist das Decodierungsverfahren D,

$$k_{\text{priv}} = D$$

Beispiel 5.2.1. Bob wählt als Codierungsverfahren den $[7,3]_{17}$–Reed–Solomon–Code bezüglich der Punkte $b_1 = 6$, $b_2 = 5$, $b_3 = 4$, $b_4 = 3$, $b_5 = 2$, $b_6 = 1$ und $b_7 = 0$ aus. Die Paritätsprüfmatrix, die Bob für die Decodierung benutzt, ist daher

$$H = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 6 & 5 & 4 & 3 & 2 & 1 & 0 \\ 2 & 8 & 16 & 9 & 4 & 1 & 0 \\ 12 & 6 & 13 & 10 & 8 & 1 & 0 \end{pmatrix}$$

Die Erzeugermatrix, die Bob aus dem Gauß–Algorithmus für C ableitet ist

$$G_1 = \begin{pmatrix} 1 & 0 & 0 & 14 & 11 & 15 & 10 \\ 0 & 1 & 0 & 7 & 3 & 2 & 4 \\ 0 & 0 & 1 & 13 & 6 & 13 & 1 \end{pmatrix}$$

Für kryptographische Zwecke ist diese Matrix allerdings weniger gut geeignet. Eine Codierung damit enthält nämlich den Nachrichtentext zunächst unverfälscht (in den ersten drei Positionen). Selbst nach Störung um einen Fehlerterm kann der Angreifer Catherine daraus möglicherweise Schlüsse über die Nachricht ableiten. Deshalb stört Bob diese Erezugermatrix mit der Matrix

$$U = \begin{pmatrix} 1 & 2 & 16 \\ 2 & 5 & 1 \\ 2 & 6 & 5 \end{pmatrix}$$

(die über $\mathbb{F}_{17}$ invertierbar ist) und benutzt

$$G = U \cdot G_1 = \begin{pmatrix} 1 & 2 & 16 & 15 & 11 & 6 & 0 \\ 2 & 5 & 1 & 8 & 9 & 2 & 7 \\ 2 & 6 & 5 & 16 & 2 & 5 & 15 \end{pmatrix}$$

Der öffentliche Schlüssel von Bob ist die Matrix G und die Fehlerkorrekturschranke $t = 2$ (und die Primzahl $p = 17$ bzw. der Körper $\mathbb{F}_{17}$, über dem gearbeitet wird) ,

$$k_{\text{pub},B} = (G, t = 2, \mathbb{F}_{17})$$

sein privater Schlüssel ist die Paritätsprüfamtrix H (bzw. die Punktmenge $\{b_1, b_2, \ldots, b_7\}$, die für die Konstruktion verwendet wurde,

$$k_{\text{priv},B} = H$$

Verschlüsselung:
Bob hat seine öffentlichen Schlüssel (G, t) veröffentlicht und Alice ist daher im Besitz dieser Daten. Um einen Klartext m (aufgefasst als k–Tupel in $\mathbb{F}_q^k$) zu verschlüsseln, geht Alice nun vor wie folgt:

1. Alice benutzt den öffentlichen Schlüssel (G, t) und berechnet $c = m \cdot G$.
2. Alice wählt zufällig einen Fehlervektor $e \in \mathbb{F}_q^n$ mit Gewicht $w(e) \leq t$ aus.
3. Alice setzt $b = c + e$.
4. Alice schickt b über einen öffentlichen Kanal an Bob.

Beispiel 5.2.2. Alice benutzt das von Bob in Beispiel 5.2.1 aufgesetzte asymmetrische Vrschlüsselungsverfahren, um Bob die Nachricht

$$m = (12, 9, 15)$$

geheim zukommen zu lassen. Dazu codiert sie die Nachricht m zu

$$b = 12 \cdot g_1 + 9 \cdot g_2 + 15 \cdot g_3 = (9, 6, 4, 16, 5, 12, 16)$$

(wobei g_1, g_2 und g_3 die Zeilen vo G sind). Sie wählt zufällig den Fehlervektor

$$e = (0, 7, 12, 0, 0, 0, 0)$$

mit Gewicht $w(e) \leq 2$ und erzeugt damit das Chiffrat

$$c = b + e = (9, 13, 16, 16, 5, 12, 16)$$

Dieses Chiffrat c schickt sie an Bob.

Entschlüsselung:
Bob nutzt seinen privaten Schlüssel D, um das von Alice empfangene Chiffrat d wie folgt zu entschlüsseln:

1. Bob benutzt seinen privaten Schlüssel D, um den Fehlerterm e zu bestimmen und $c = b - e$ zurückzugewinnen.

2. Bob beseitigt die Redundanzen in c und erhält den Klartext m zurück.

Beispiel 5.2.3. Bob hat in Beispiel 5.2.2 das Chiffrat $c = (9, 13, 16, 16, 5, 12, 16)$ von Alice erhalten.

1. Bob berechnet mithilfe von H die Syndrome von c und erhält

$$\begin{aligned} [c, X^0] &= 2 \\ [c, X^1] &= 15 \\ [c, X^2] &= 10 \\ [c, X^3] &= 11 \end{aligned}$$

   Damit ist das Chiffrat c sicherlich kein Codewort.

2. Zur Bestimmung des fehlerlokalisierenden Polynoms betrachtet Bob zunächst das lineare Gleichungssystem

$$\begin{aligned} 2 \cdot Y_0 + 15 \cdot Y_1 + 10 \cdot Y_2 &= 0 \\ 15 \cdot Y_0 + 10 \cdot Y_1 + 11 \cdot Y_2 &= 0 \end{aligned}$$

   über $\mathbb{F}_{17}$. Die zugehörige Koeffizientenmatrix ist

$$A = \begin{pmatrix} 2 & 15 & 10 \\ 15 & 10 & 11 \end{pmatrix}$$

   mit Normalform

$$B = \begin{pmatrix} 1 & 16 & 5 \\ 0 & 1 & 9 \end{pmatrix}$$

   bzw. reduzierter Normalform

$$B' = \begin{pmatrix} 1 & 0 & 14 \\ 0 & 1 & 9 \end{pmatrix}$$

und Grundlösung des zugehörigen homogenen Gleichungssystems

$$l = (3,\ 8,\ 1)$$

Insbesondere hat dieses Gleichungssystem nicht–triviale Lösungen.

3. Aus l erhalten wir als fehlerlokalisierendes Polynom

$$L(x) = 3 + 8 \cdot X + X^2$$

Einsetzen (in $\mathbb{F}_{11}$) ergibt

$$\begin{array}{rcl} L(b_1) = L(6) & = & 2 \\ L(b_2) = L(5) & = & 0 \\ L(b_3) = L(4) & = & 0 \\ L(b_4) = L(3) & = & 2 \\ L(b_5) = L(2) & = & 6 \\ L(b_6) = L(1) & = & 12 \\ L(b_7) = L(0) & = & 3 \end{array}$$

Also gilt $L(b_2) = 0$ und $L(b_3) = 0$, und damit können Fehler an den Stellen 2 und 3 vorliegen.

4. Zur Fehlerbestimming betrachten wir das Gleichungssystem

$$\begin{array}{rcrcl} E_2 & + & E_3 & = & 2 \\ 5 \cdot E_2 & + & 4 \cdot E_3 & = & 15 \\ 8 \cdot E_2 & + & 16 \cdot E_3 & = & 10 \\ 6 \cdot E_2 & + & 13 \cdot E_3 & = & 11 \end{array}$$

über $\mathbb{F}_{17}$. Dieses System hat Koeffizientenmatrix

$$A = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 5 & 4 & 15 \\ 8 & 16 & 10 \\ 6 & 13 & 11 \end{array}\right)$$

mit Normalform

$$B = \left(\begin{array}{cc|c} 1 & 1 & 2 \\ 0 & 1 & 12 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right)$$

Wir erhalten die eindeutige Lösung $e_2 = 7$ und $e_3 = 12$.

5. Setzen wir $e_1 = e_4 = e_5 = e_6 = e_7 = 0$, so erhalten wir als Fehlerterm

$$e = (0,\ 7,\ 12,\ 0,\ 0,\ 0,\ 0)$$

und als korrigiertes Wort

$$b = (9,\ 13,\ 16,\ 16,\ 5,\ 12,\ 16) - (0,\ 7,\ 12,\ 0,\ 0,\ 0,\ 0) = (9,\ 6,\ 4,\ 16,\ 5,\ 12,\ 16)$$

Zur Bestimmung des Klartextes löst Bob nun das lineare Gleichungssystem

$$m_1 \cdot g_1 + m_2 \cdot g_2 + m_3 \cdot g_3 = b$$

und erhält als eindeutige Lösung $m_1 = 12$, $m_2 = 9$ und $m_3 = 15$, also den Klartext

$$m = (12,\ 9,\ 15)$$

Bemerkung 5.2.1. Die Sicherheit des Verfahrens der code–basierten Kryptographie beruht darauf, dass die Erzeugermatrix eines Codes im Allgemeinen keine Rückschlüsse auf möglicher Decodierungsalgorithmen zulässt.
Die Verwendung von Reed–Solomon–Codes (bzw. verallgemeinerten Reed–Solomon–Codes) für kryptographische Protokolle wurde 1986 von Niederreiter vorgeschlagen. Allerdings entwickelten Sidelnikov und Shestakov 1992 einen Angriff auf dieses Verfahren, der es erlaubt, aus einer Erzeugermatrix die in der Konstruktion verwendeten Punkte zu berechnen. Bis heute nicht gebrochen ist der ursprüngliche Vorschlag von McEliece, für die code–basierte Verschlüsselung sogenannte binäre Goppa–Codes zu verwenden. Das Arbeiten mit diesen Codes ist aber sehr viel aufwendiger und zeitintensiver. Die Suche nach Klassen linearer Codes mit einfachen Decodierungsverfahren, die auch gute kryptographische Eigenschaften haben, ist noch im vollen Gange.

Index