Appendix

Basic Facts from Algebra and Probability Theory

A.1 Basic Preliminaries

For logarithms to various bases,

$$\log_a \alpha = \frac{\log_b \alpha}{\log_b a} = \frac{\ln \alpha}{\ln a}. \tag{A.1.1}$$

For the differentiation of logarithms (with respect to α),

$$(a^\alpha)' = a^\alpha \cdot \ln a \quad , \quad (\ln \alpha)' = \frac{1}{\alpha} \quad , \quad (\log_a \alpha)' = \frac{1}{\alpha \ln a}. \tag{A.1.2}$$

L'Hôspital's rule: let f and g be continuously differentiable functions. If both limits $\lim\limits_{\alpha\to\alpha_0} f(\alpha)$ and $\lim\limits_{\alpha\to\alpha_0} g(\alpha)$ are either zero or infinite then

$$\lim_{\alpha\to\alpha_0} \frac{f(\alpha)}{g(\alpha)} = \lim_{\alpha\to\alpha_0} \frac{f'(\alpha)}{g'(\alpha)}, \tag{A.1.3}$$

i.e., the limit of the quotient of the functions can be replaced by the quotient of the first derivatives.

Taylor's expansion: if the function f is $(n+1)$-times differentiable and the $(n+1)$-th derivative is continuous, then

$$f(\alpha_0 + \alpha) = \sum_{r=0}^{n} \frac{f^{(r)}(\alpha_0)}{r!}\alpha^r + \frac{f^{(n+1)}(\alpha_1)}{(n+1)!}\alpha^{n+1} \tag{A.1.4}$$

with α_1 between α_0 and α. For $\alpha \to 0$ the remainder disappears, so that in a neighbourhood of α_0 the function f can be approximated by a polynomial of degree n. For small α there are the following Taylor approximations with first

degree polynomials:

$$\log_2(1+\alpha) \approx \frac{\alpha}{\ln 2} \tag{A.1.5}$$

$$\log_2(2+\alpha) \approx 1 + \frac{\alpha}{2\ln 2} \tag{A.1.6}$$

$$e^{\alpha} \approx 1+\alpha \tag{A.1.7}$$

$$(1+\alpha)^a \approx 1+a\alpha. \tag{A.1.8}$$

Schwarz's inequality: For complex-valued functions $f(\alpha)$ and $g(\alpha)$ with $\int_{-\infty}^{\infty} |f(\alpha)|^2\, d\alpha < \infty$ and $\int_{-\infty}^{\infty} |g(\alpha)|^2\, d\alpha < \infty$, the inequality can be stated as

$$\left| \int_{-\infty}^{\infty} f(\alpha) g(\alpha)\, d\alpha \right|^2 \leq \int_{-\infty}^{\infty} |f(\alpha)|^2\, d\alpha \cdot \int_{-\infty}^{\infty} |g(\alpha)|^2\, d\alpha. \tag{A.1.9}$$

The equality holds if and only if

$$f(\alpha) = c g^*(\alpha) \tag{A.1.10}$$

where c is an arbitrary constant, and the asterisk denotes complex conjugation.

A.2 Binomial Coefficients and Entropy Function

The *binomial coefficients* are defined as

$$\binom{n}{r} = \frac{n!}{r!(n-r)!} = \binom{n}{n-r} \quad ; \quad \binom{n}{0} = \binom{n}{n} = 1 \tag{A.2.1}$$

and the *binomial formula* is

$$\sum_{r=0}^{n} \binom{n}{r} a^r b^{n-r} = (a+b)^n \quad ; \quad \sum_{r=0}^{n} \binom{n}{r} = 2^n. \tag{A.2.2}$$

The *binary entropy function* is defined as

$$\begin{aligned} H_2(\lambda) &= -\lambda \log_2 \lambda - (1-\lambda)\log_2(1-\lambda) \\ &= -\log_2 \left(\lambda^{\lambda} (1-\lambda)^{1-\lambda} \right). \end{aligned} \tag{A.2.3}$$

Figure A.1 shows the binary entropy function. Note the symmetry $H_2(1-\lambda) = H_2(\lambda)$ and the properties $H_2(0) = H_2(1) = 0$ and $H_2(0.5) = 1$. Furthermore

$$H'(0) = \lim_{\lambda \to 0} \frac{H_2(\lambda)}{\lambda} = \lim_{n \to \infty} n \cdot H_2\left(\frac{1}{n}\right) = +\infty \tag{A.2.4}$$

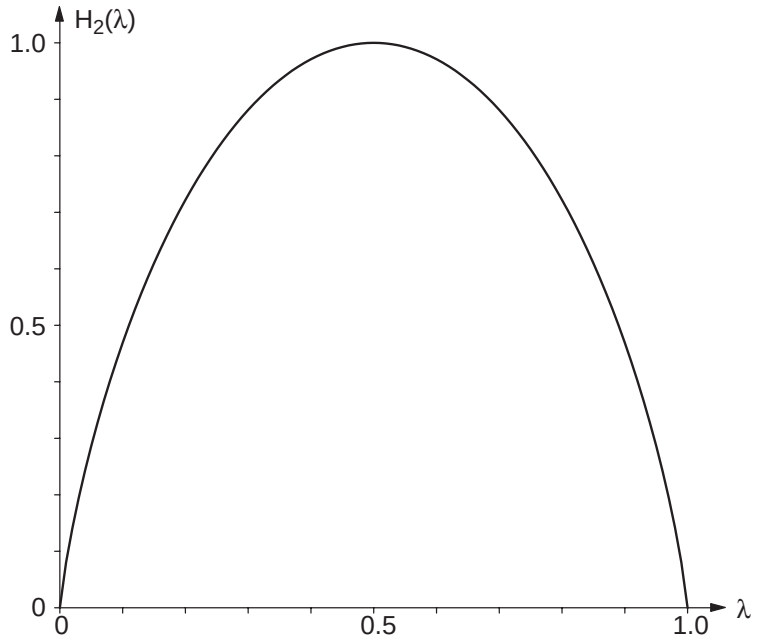

Figure A.1. The binary entropy function

and the Taylor approximation by a second degree polynomial in the neighbourhood of 0.5 gives us

$$H_2\left(\frac{1}{2}+\lambda\right) \approx 1 - \frac{2}{\ln 2}\lambda^2. \tag{A.2.5}$$

Theorem A.1. *Let $0 \le \lambda \le 1/2$. The partial sums of the binomial coefficients are upper bounded by the binary entropy function as follows:*

$$\sum_{r=0}^{\lambda n} \binom{n}{r} \le 2^{nH_2(\lambda)} = \left(\lambda^\lambda (1-\lambda)^{1-\lambda}\right)^{-n}, \tag{A.2.6}$$

where the sum is over all r with $0 \le r \le \lambda n$. Furthermore, asymptotically we have

$$\lim_{n\to\infty} \frac{1}{n} \log_2 \sum_{r=0}^{\lambda n} \binom{n}{r} = H_2(\lambda) = \lim_{n\to\infty} \frac{1}{n} \log_2 \binom{n}{\lfloor \lambda n \rfloor}. \tag{A.2.7}$$

Proof. According to the binomial formula,

$$\begin{aligned}
1 = (\lambda + 1 - \lambda)^n &= \sum_{r=0}^{n} \binom{n}{r} \lambda^r (1-\lambda)^{n-r} \\
&\ge \sum_{r=0}^{\lambda n} \binom{n}{r} \lambda^r (1-\lambda)^{n-r} = (1-\lambda)^n \sum_{r=0}^{\lambda n} \binom{n}{r} \left(\frac{\lambda}{1-\lambda}\right)^r \\
&\ge (1-\lambda)^n \sum_{r=0}^{\lambda n} \binom{n}{r} \left(\frac{\lambda}{1-\lambda}\right)^{\lambda n} \quad \text{since} \quad \frac{\lambda}{1-\lambda} \le 1 \quad \text{and} \quad r \le \lambda n
\end{aligned}$$

$$= \lambda^{\lambda n}(1-\lambda)^{n-\lambda n} \sum_{r=0}^{\lambda n} \binom{n}{r} = 2^{-nH_2(\lambda)} \sum_{r=0}^{\lambda n} \binom{n}{r},$$

proving (A.2.6). To easily describe asymptotic behaviour, the function $o(f(n))$ is used (read as: *small o of* $f(n)$), defined as $o(f(n))/f(n) \to 0$ as $n \to \infty$. In particular, $o(n)/n = o(1)$. Since $\log_2\lfloor\lambda n\rfloor - \log_2(\lambda n) = \log_2 \frac{\lfloor\lambda n\rfloor}{\lambda n} \to 0$ as $n \to \infty$,

$$\log_2\lfloor\lambda n\rfloor = \log_2(\lambda n) + o(1).$$

According to *Stirling's formula* [123],

$$n! = n^n e^{-n}\sqrt{2\pi n}\exp\left(\frac{1}{12n} - \frac{1}{360n^3} + \cdots\right), \tag{A.2.8}$$

thus

$$\ln n! = n\ln n - n + o(n).$$

So together with the definition of the binomial coefficient,

$$\begin{aligned}\ln\binom{n}{r} &= \Big[n\ln n - n + o(n)\Big] - \Big[r\ln r - r + o(r)\Big] \\ &\quad - \Big[(n-r)\ln(n-r) - (n-r) + o(n-r)\Big] \\ &= n\ln n - r\ln r - (n-r)\ln(n-r) + o(n).\end{aligned}$$

This is also valid for logarithms to the base 2, thus for $r = \lambda n$,

$$\begin{aligned}&\frac{1}{n}\log_2\binom{n}{\lfloor\lambda n\rfloor} \\ &\quad = \log_2 n - \frac{\lfloor\lambda n\rfloor}{n}\log_2\lfloor\lambda n\rfloor - \left(1 - \frac{\lfloor\lambda n\rfloor}{n}\right)\log_2(n - \lfloor\lambda n\rfloor) + \frac{o(n)}{n} \\ &\quad = \log_2 n - \lambda\log_2(\lambda n) - (1-\lambda)\log_2((1-\lambda)n) + o(1) \\ &\quad = -\lambda\log_2\lambda - (1-\lambda)\log_2(1-\lambda) + o(1) \\ &\quad = H_2(\lambda) + o(1).\end{aligned}$$

This implies the equality on the right hand side of (A.2.7) and

$$\binom{n}{\lfloor\lambda n\rfloor} \le \sum_{r=0}^{\lambda n}\binom{n}{r} \le 2^{nH_2(\lambda)}$$

implies the left hand side of (A.2.7). ■

The upper bound in Theorem A.1 is used in Section 2.7 for the proof of the channel coding theorem and the limit is used in Section 3.4 to derive the asymptotic bounds.

For $\lambda = 1/2$ (and for an even n), Theorem A.1 only gives us the trivial approximation $\binom{n}{n/2} \le 2^n = \sum_{r=0}^{n}\binom{n}{r}$. With elementary calculations we obtain

the following very precise approximation from Stirling's approximation $n! \approx n^n e^{-n}\sqrt{2\pi n}$ (as a special case of the DeMoivre-Laplace theorem [103]):

$$\binom{n}{n/2} \approx \sqrt{\frac{2}{\pi}}\frac{2^n}{\sqrt{n}}. \tag{A.2.9}$$

A.3 Basic Probability Theory

A.3.1 Bayes Theorem

The quotient $P(\mathcal{A}|\mathcal{B}) = P(\mathcal{A}\mathcal{B})/P(\mathcal{B})$ describes the *conditional probability* of the event $\mathcal{A}$ given the event $\mathcal{B}$. Two events $\mathcal{A}, \mathcal{B}$ are *statistically independent*, if $P(\mathcal{A}\mathcal{B}) = P(\mathcal{A})P(\mathcal{B})$ or $P(\mathcal{A}|\mathcal{B}) = P(\mathcal{A})$. For a complete disjunction of events $\mathcal{A}_i$ with $\mathcal{A}_i\mathcal{A}_j = \emptyset$, $i \neq j$ and $P(\bigcup_i \mathcal{A}_i) = 1$ we note the following *law of total probability*

$$P(\mathcal{B}) = \sum_i P(\mathcal{B}|\mathcal{A}_i)P(\mathcal{A}_i) \tag{A.3.1}$$

and the *Bayes' rule*

$$P(\mathcal{A}_k|\mathcal{B}) = \frac{P(\mathcal{A}_k\mathcal{B})}{P(\mathcal{B})} = \frac{P(\mathcal{B}|\mathcal{A}_k)P(\mathcal{A}_k)}{\sum_i P(\mathcal{B}|\mathcal{A}_i)P(\mathcal{A}_i)}. \tag{A.3.2}$$

For arbitrary events $\mathcal{A}_i$,

$$P\left(\bigcup_i \mathcal{A}_i\right) \leq \sum_i P(\mathcal{A}_i). \tag{A.3.3}$$

For disjunctive or independent events, we have equality in (A.3.3) which corresponds to the additivity of probability.

A.3.2 Discrete- and Real-Valued Random Variables, Mean and Variance

A random variable is a function from the set of experimental events onto the set of real numbers. For exact statements it may be necessary to distinguish between the random variable as such and the attained values (i.e., the possible results). The random variables are usually denoted $x, y, \ldots$ (small letters), and the values taken on by $\xi, \eta, \ldots$ (small greek letters). The denotation $P(x = \xi)$ or $P(\xi_a < x < \xi_b)$ describes the probability of the random variable attaining the exact value ξ or values between ξ_a and ξ_b. The outcome of a random variable is also called a sample of the random variable.

An essential property for distinguishing and classifying random variables is their range (i.e., the set of possible outcomes or attained values). A real-valued

(also called continuous-valued) random variable can take on all possible real numbers. In contrast, a discrete-valued random variable only takes on denumerably many values which includes only taking on a finite number of values. For a binary random variable there are only two possible outcomes. Examples of binary random variables are the input and output and the components of the error word of a binary symmetric channel.

An analog signal, for example the output of an AWGN channel, can be seen as a sample of a real-valued random variable. Quantization, technically realized by an analog-to-digital converter within the demodulator, transfers the analog voltage into a bit combination. This can be seen as a discrete-valued random variable with finite range which is determined by the wordlength of the analog-to-digital converter.

In this subsection we will see that the description of continuous random variables also contains discrete random variables and all other sorts of random variables as special cases.

Let the discrete-valued random variable x with finite range attain the q values ξ_i with the probabilities $p_i = P(x = \xi_i)$. Then the distribution has been described completely by the q values $p_1, \ldots, p_q$ and the range $\xi_1, \ldots, \xi_q$.

A real-valued random variable x is described by the *cumulative distribution function (CDF)*

$$F_x(\xi) = P(x < \xi). \tag{A.3.4}$$

From the basic axioms of probability the following properties of the CDF may be shown: $F_x(-\infty) = 0$, $F_x(+\infty) = 1$, $F_x(\xi_1) \leq F_x(\xi_2)$ if $\xi_1 \leq \xi_2$ (i.e., monotonically non-decreasing) and the function $F_x(\xi)$ is continuous from the left. The differentiation of the CDF leads to the *probability density function (PDF)*:

$$f_x(\xi) = \frac{d}{d\xi} F_x(\xi). \tag{A.3.5}$$

The properties of the CDF imply the following properties of the PDF: $f_x(\xi) \geq 0$ for all ξ and $\int_{-\infty}^{\infty} f_x(\xi)\, d\xi = 1$. Furthermore,

$$P(a \leq x < b) = F_x(b) - F_x(a) = \int_a^b f_x(\xi)\, d\xi. \tag{A.3.6}$$

By using the Dirac delta function $\delta(\xi)$ a discrete-valued random variable can be interpreted as a special case of a real-valued random variable:

$$f_x(\xi) = \sum_i p_i \cdot \delta(\xi - \xi_i), \qquad F_x(\xi) = \sum_{\substack{i \\ \xi_i < \xi}} p_i. \tag{A.3.7}$$

So the PDF of a discrete-valued random variable consists of a sequence of Dirac delta impulses and the CDF consists of a sequence of steps (also called staircase

function). The height of the steps at ξ_i corresponds to the probablities $p_i = P(x = \xi_i)$ of these values being attained:

$$p_i = F_x(\xi_i + 0) - F_x(\xi_i) = F_x(\xi_{i+1}) - F_x(\xi_i). \tag{A.3.8}$$

So all in all an explicit distinction between discrete- and real-valued random variables is not necessary for most situations. However, the PDF finds greater use in connection with continuous-valued random variables.

The two most important parameters characterizing a statistical distribution are the mean and the variance. The *mean* (also called *average value*, *expected value* or *expectation*) of the real- or discrete-valued random variable is defined as

$$\mu = E(x) = \int_{-\infty}^{\infty} \xi \cdot f_x(\xi)\, d\xi \tag{A.3.9}$$

$$= \sum_i \xi_i \cdot p_i \quad \text{for discrete } x \tag{A.3.10}$$

and the *variance* as

$$\sigma^2 = D^2(x) = \int_{-\infty}^{\infty} (\xi - \mu)^2 \cdot f_x(\xi)\, d\xi \tag{A.3.11}$$

$$= E((x - E(x))^2) \tag{A.3.12}$$

$$= E(x^2) - (E(x))^2 = \int_{-\infty}^{\infty} \xi^2 f_x(\xi)\, d\xi - \left(\int_{-\infty}^{\infty} \xi f_x(\xi)\, d\xi \right)^2 \tag{A.3.13}$$

$$= \sum_i (\xi_i - \mu)^2 \cdot p_i \quad \text{for discrete } x. \tag{A.3.14}$$

The square root $\sigma = D(x) = \sqrt{D^2(x)}$ of the variance is called the *standard deviation* or *dispersion* of the random variable.

The mean $E(x^k)$ is called the *k-th moment* and $E((x-\mu)^k)$ is called the *k-th central moment*, i.e., the mean $E(x)$ is the first moment, $E(x^2)$ is the second moment and the variance $D^2(x)$ proves to be the second central moment. All moments can be seen as special cases of the expected value of a function of a random variable:

$$E(h(x)) = \int_{-\infty}^{\infty} h(\xi) \cdot f_x(\xi)\, d\xi. \tag{A.3.15}$$

A.3.3 Joint and Conditional Distributions and Statistical Independence

In this subsection we consider relations between two or more random variables. The *joint cumulative probability function (joint CDF)* of two random variables

is defined as

$$F_{x,y}(\xi,\eta) = P(x<\xi, y<\eta) = \int_{-\infty}^{\xi}\int_{-\infty}^{\eta} f_{x,y}(\alpha,\beta)\, d\beta\, d\alpha \tag{A.3.16}$$

and the *joint probability distribution function (joint PDF)* is defined as

$$f_{x,y}(\xi,\eta) = \frac{d^2 F_{x,y}(\xi,\eta)}{d\xi\, d\eta}. \tag{A.3.17}$$

The *marginal CDF* and the *marginal PDF* can be obtained from the joint CDF and the joint PDF with

$$F_x(\xi) = F_{x,y}(\xi,\infty) \tag{A.3.18}$$

and

$$\begin{aligned} f_x(\xi) &= \frac{dF_x(\xi)}{d\xi} = \frac{dF_{x,y}(\xi,\infty)}{d\xi} \\ &= \frac{d}{d\xi}\int_{-\infty}^{\xi}\int_{-\infty}^{\infty} f_{x,y}(\alpha,\eta)\, d\eta\, d\alpha \\ &= \int_{-\infty}^{\infty} f_{x,y}(\xi,\eta)\, d\eta. \end{aligned} \tag{A.3.19}$$

The *conditional CDF* is defined as

$$\begin{aligned} F_{x|y}(\xi|\eta) &= P(x<\xi \mid y=\eta) \\ &= \lim_{\varepsilon\to 0}\frac{P(x<\xi,\ \eta\le y<\eta+\varepsilon)}{P(\eta\le y<\eta+\varepsilon)}, \end{aligned} \tag{A.3.20}$$

where $F_{x|y}(\xi|\eta)$ is assumed to be a continuous function in η. From this the corresponding *conditional PDF* can be easily derived:

$$\begin{aligned} f_{x|y}(\xi|\eta) &= \frac{dF_{x|y}(\xi|\eta)}{d\xi} \\ &= \lim_{\varepsilon\to 0}\frac{\dfrac{d}{d\xi}\displaystyle\int_{-\infty}^{\xi}\int_{\eta}^{\eta+\varepsilon} f_{x,y}(\alpha,\beta)\, d\beta\, d\alpha}{\displaystyle\int_{\eta}^{\eta+\varepsilon} f_y(\beta)\, d\beta} = \lim_{\varepsilon\to 0}\frac{\dfrac{1}{\varepsilon}\displaystyle\int_{\eta}^{\eta+\varepsilon} f_{x,y}(\xi,\beta)\, d\beta}{\dfrac{1}{\varepsilon}\displaystyle\int_{\eta}^{\eta+\varepsilon} f_y(\beta)\, d\beta} \\ &= \frac{f_{x,y}(\xi,\eta)}{f_y(\eta)}. \end{aligned} \tag{A.3.21}$$

The two random variables x and y are called *statistically independent* (or simply *independent*) if one of the following equivalent relations is valid for the CDFs or

PDFs (for all ξ and η):

$$\begin{aligned} & F_{x,y}(\xi,\eta) = F_x(\xi)\cdot F_y(\eta) && \text{(A.3.22)}\\ \Longleftrightarrow\quad & f_{x,y}(\xi,\eta) = f_x(\xi)\cdot f_y(\eta) && \text{(A.3.23)}\\ \Longleftrightarrow\quad & f_{x|y}(\xi|\eta) = f_x(\xi). && \text{(A.3.24)} \end{aligned}$$

The definition of statistical independence can be easily generalized to n random variables. The components of the random vector $\boldsymbol{x} = (x_1,\ldots,x_n)$ are said to be *mutually statistically independent* if $f_{\boldsymbol{x}}(\xi_1,\ldots,\xi_n) = f_{x_1}(\xi_1)\cdots f_{x_n}(\xi_n)$ for all $\boldsymbol{\xi} = (\xi_1,\ldots,\xi_n)$. The statistical independence of two or more random variables implies that

$$E(x\cdot y) = E(x)\cdot E(y), \tag{A.3.25}$$

$$D^2(x+y) = D^2(x) + D^2(y), \tag{A.3.26}$$

$$E(x|y=\eta) = E(x) \quad \text{for all } \eta, \tag{A.3.27}$$

for the means and variances. However, $E(x+y) = E(x) + E(y)$ is valid for dependent random variables, as well.

Regardless of the statistical independence or dependence, the *conditional mean* $E(x|y)$ is a random variable dependent on y and defined as

$$E(x|y) = \int_{-\infty}^{\infty} \xi\cdot f_{x|y}(\xi|y)\,d\xi. \tag{A.3.28}$$

For the mean of this function of y, we generally (including also the case of statistical dependence) have:

$$\begin{aligned} E(E(x|y)) &= \int_{-\infty}^{\infty}\left(\int_{-\infty}^{\infty}\xi\cdot f_{x|y}(\xi|\eta)\,d\xi\right)\cdot f_y(\eta)\,d\eta\\ &= \int_{-\infty}^{\infty}\xi\cdot\underbrace{\int_{-\infty}^{\infty} f_{x,y}(\xi,\eta)\,d\eta}_{=f_x(\xi)}\,d\xi\\ &= E(x). \end{aligned} \tag{A.3.29}$$

For the sum $z = x + y$ of two arbitrary random variables x and y, the PDF can

be easily derived:

$$f_z(\zeta) = \frac{d}{d\zeta} P(x+y<\zeta) = \frac{d}{d\zeta} \iint\limits_{\xi+\eta<\zeta} f_{x,y}(\xi,\eta)\, d\xi\, d\eta$$

$$\text{substitute } (\xi,\eta) \text{ by } (\xi, \alpha = \xi+\eta)$$

$$= \frac{d}{d\zeta} \int\limits_{-\infty}^{\zeta} \underbrace{\int\limits_{-\infty}^{\infty} f_{x,y}(\xi, \alpha-\xi)\, d\xi}_{=I(\alpha)}\, d\alpha = \underbrace{\int\limits_{-\infty}^{\infty} f_{x,y}(\xi, \zeta-\xi)\, d\xi}_{=I(\zeta)}. \qquad \text{(A.3.30)}$$

Above, the auxiliary function $I(.)$ is only used for simplification. If the random variables x and y are presupposed to be statistically independent, then the PDF of the sum $z = x+y$ is obtained by the convolution of the single (i.e., marginal) PDFs:

$$f_z(\zeta) = (f_x * f_y)(\zeta)$$

$$= \int\limits_{-\infty}^{\infty} f_x(\xi) \cdot f_y(\zeta-\xi)\, d\eta = \int\limits_{-\infty}^{\infty} f_x(\zeta-\eta) \cdot f_y(\eta)\, d\eta. \qquad \text{(A.3.31)}$$

A.3.4 Tchebycheff Inequality

The following bound for the probability of the linear deviation given by the quadratic deviation is used in Section 2.7 for the proof of the channel coding theorem:

Theorem A.2 (Tchebycheff Inequality). *Let the random variable x be discrete- or continuous-valued with the mean $\mu = E(x)$ and the variance $D^2(x)$. Then for every $\delta > 0$, the probability of $|x-\mu| > \delta$ is upper bounded as follows:*

$$P\big(|x-\mu| > \delta\big) \;\le\; \frac{D^2(x)}{\delta^2}. \qquad \text{(A.3.32)}$$

Proof.

$$D^2(x) = \int\limits_{-\infty}^{\infty} (\xi-\mu)^2 \cdot f_x(\xi)\, d\xi \;\ge \int\limits_{|\xi-\mu|>\delta} (\xi-\mu)^2 \cdot f_x(\xi)\, d\xi$$

$$\ge \int\limits_{|\xi-\mu|>\delta} \delta^2 \cdot f_x(\xi)\, d\xi \;=\; \delta^2 \cdot P(|\xi-\mu|>\delta).$$

The proof for discrete-valued random variables follows from the general case as well as from a similar direct calculation. ■

A.4 Some important Probability Distributions

First, we will consider the discrete binomial distribution which describes the number of errors in a received word for hard decisions. All further distributions are continuous and are described by their PDFs. The important Gaussian (or normal) distribution will be discussed thoroughly because the computations of the error probabilities for the AWGN channel are based on it. The two-dimensional Gaussian distribution is used to describe the complex-valued passband noise. Finally, the Rayleigh distribution characterizes the simplest form of fading channels.

A.4.1 The Binomial Distribution

The discrete-valued random variable x has a *binomial distribution* with the parameter p_e (let $0 \le p_e \le 1$), if

$$P(x = l) = \binom{n}{l} p_e^l (1 - p_e)^{n-l}, \quad l = 0, 1, \ldots, n \tag{A.4.1}$$

$$= b(n, l, p_e). \tag{A.4.2}$$

The value $P(x = l)$ is the probability of an event with probability p_e occurring l times during n independent trials. This probability is also denoted $b(n, l, p_e)$. So the binomial distribution is characterized by these $n + 1$ values $b(n, 0, p_e), \ldots, b(n, n, p_e)$. The mean is $E(x) = np_e$ and the variance is $D^2(x) = np_e(1 - p_e)$, which can be easily checked. An example for the binomial distribution is given by the number of errors in a received word after transmission over a binary symmetric channel with the bit-error probability p_e, see (1.3.9).

For better understanding, in Figure A.2 the values $b(n, l, p_e)$ are connected by a graph over l for different values of p_e and $n = 20$. Obviously $b(n, l, p_e = s/n)$ with fixed $s \in \mathbb{N}$ reaches its maximum for $l = s$ (see also Problem 1.9). Generally, we have the simple equation

$$b(n, l, p_e) = b(n, n - l, 1 - p_e). \tag{A.4.3}$$

For $p_e = 1/2$, $b(n, l, 1/2) = b(n, n - l, 1/2)$, i.e., in this specific case the distribution is symmetric.

A.4.2 The Gaussian (Normal) Distribution

The continuous-valued random variable x has a *Gaussian distribution* (also widely called *normal distribution*) with the mean μ and the variance σ^2, written

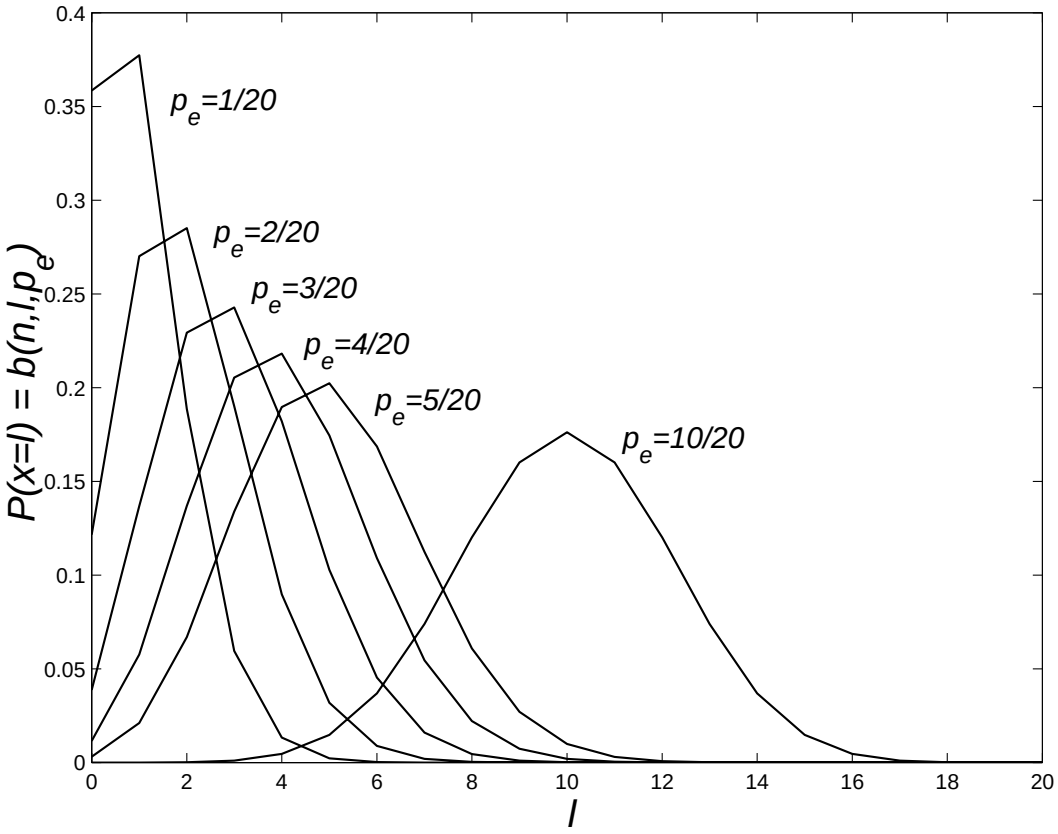

Figure A.2. The binomial distribution for $n = 20$

as $x \sim N(\mu, \sigma^2)$ and called x distributed according to $N(\mu, \sigma^2)$, if the PDF looks like

$$f(\xi) = \frac{1}{\sqrt{2\pi\sigma^2}} \exp\left(-\frac{(\xi-\mu)^2}{2\sigma^2}\right). \tag{A.4.4}$$

In Figure A.3, there are a few examples of PDFs with various combinations of the parameters μ and σ.

For the moments of order ≤ 2 of the Gaussian distribution we have the familiar properties

$$\int_{-\infty}^{\infty} f(\xi)d\xi \;=\; 1, \tag{A.4.5}$$

$$E(x) = \int_{-\infty}^{\infty} \xi f(\xi)d\xi \;=\; \mu, \tag{A.4.6}$$

$$E(x^2) = \int_{-\infty}^{\infty} \xi^2 f(\xi)d\xi \;=\; \sigma^2 + \mu^2. \tag{A.4.7}$$

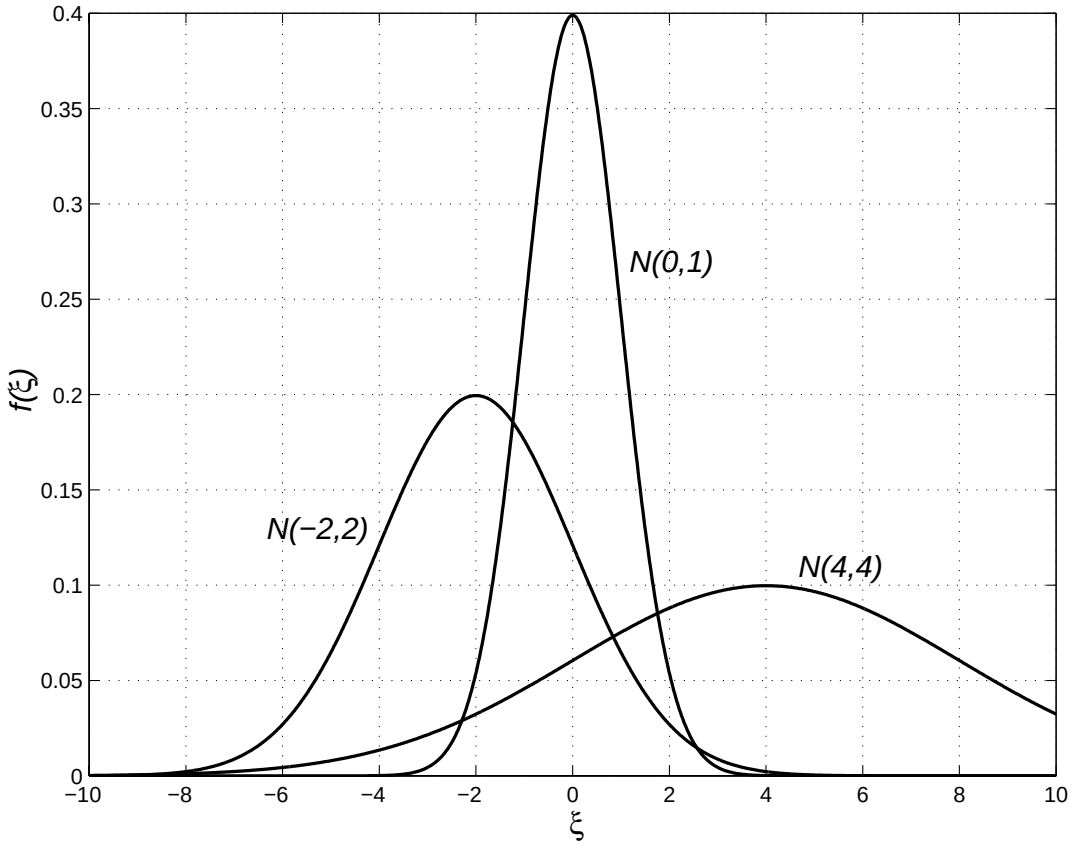

Figure A.3. PDF's of some Gaussian (normal) distributions

Proof. We apply two substitutions to the square of (A.4.5). First, we use polar coordinates $\xi_1 = r\cos\varphi$, $\xi_2 = r\sin\varphi$ with the Jacobian

$$\det\left(\frac{\partial(\xi_1,\xi_2)}{\partial(r,\varphi)}\right) = \det\begin{pmatrix}\cos\varphi & \sin\varphi\\ -r\sin\varphi & r\cos\varphi\end{pmatrix} = r,$$

implying that

$$\begin{aligned}\left(\int_{-\infty}^{\infty} f(\xi)\,d\xi\right)^2 &= \frac{1}{2\pi\sigma^2}\cdot\iint_{\mathbb{R}^2}\exp\left(-\frac{\xi_1^2+\xi_2^2}{2\sigma^2}\right)\,d\xi_1\,d\xi_2\\ &= \frac{1}{2\pi\sigma^2}\cdot\int_{r>0}\int_{\varphi=0\ldots2\pi} r\,e^{-r^2/2\sigma^2}\,d\varphi\,dr\\ &\qquad\text{second substitution } u = r^2/2\sigma^2\\ &= \int_0^{\infty} e^{-u}\,du = 1.\end{aligned}$$

So (A.4.5) is proved. The integral in

$$E(x-\mu) = \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \int_{-\infty}^{\infty} \xi \, e^{-\xi^2/2\sigma^2} \, d\xi = 0$$

is 0 due to symmetry, implying (A.4.6). On the one hand,

$$\begin{aligned} E((x-\mu)^2) &= \frac{1}{\sqrt{2\pi\sigma^2}} \cdot \int_{-\infty}^{\infty} \underbrace{\xi}_{u(\xi)} \cdot \underbrace{\xi e^{-\xi^2/2}}_{v'(\xi)} \, d\xi \\ &\qquad \text{apply integration by parts, } u'(\xi) = 1, v(\xi) = -\sigma^2 \cdot e^{-\xi^2/2\sigma^2} \\ &= \frac{\sigma^2}{\sqrt{2\pi\sigma^2}} \cdot \int_{-\infty}^{\infty} e^{-\xi^2/2\sigma^2} \, d\xi = \sigma^2 \quad \text{using (A.4.5)}, \end{aligned}$$

on the other hand $E((x-\mu)^2) = E(x^2) - 2E(x)\mu + \mu^2 = E(x^2) - \mu^2$, all in all implying (A.4.7). ■

For the probability of x attaining values between ξ_1 and ξ_2,

$$\begin{aligned} P(\xi_1 < x < \xi_2) &= P\left(\frac{\xi_1-\mu}{\sigma} < \frac{x-\mu}{\sigma} < \frac{\xi_2-\mu}{\sigma}\right) \\ &= P\left(\frac{x-\mu}{\sigma} < \frac{\xi_2-\mu}{\sigma}\right) - P\left(\frac{x-\mu}{\sigma} < \frac{\xi_1-\mu}{\sigma}\right) \\ &= Q\left(\frac{\xi_1-\mu}{\sigma}\right) - Q\left(\frac{\xi_2-\mu}{\sigma}\right). \end{aligned} \tag{A.4.8}$$

The standardized random variable $(x-\mu)/\sigma$ is also Gaussian distributed with the mean 0 and the variance 1, hence $(x-\mu)/\sigma \sim N(0,1)$. Note that

$$Q(\alpha) = P\left(\frac{x-\mu}{\sigma} > \alpha\right) = \frac{1}{\sqrt{2\pi}} \int_{\alpha}^{\infty} e^{-\eta^2/2} \, d\eta \tag{A.4.9}$$

$$= \frac{1}{2}\text{erfc}\left(\frac{\alpha}{\sqrt{2}}\right), \tag{A.4.10}$$

where $Q(\alpha)$ is the *complementary Gaussian error function*, whose graph is shown in Figure A.4. In communications engineering it is standard practice to use $Q(\alpha)$ rather than the CDF $F(\alpha) = Q(-\alpha)$. Instead of using the function $Q(\alpha)$ the function $\text{erfc}(\alpha)$, introduced in (A.4.8), is often used:

$$\text{erfc}(\alpha) = 2 \cdot Q(\alpha\sqrt{2}) = \frac{2}{\sqrt{\pi}} \int_{\alpha}^{\infty} e^{-\xi^2} \, d\xi \tag{A.4.11}$$

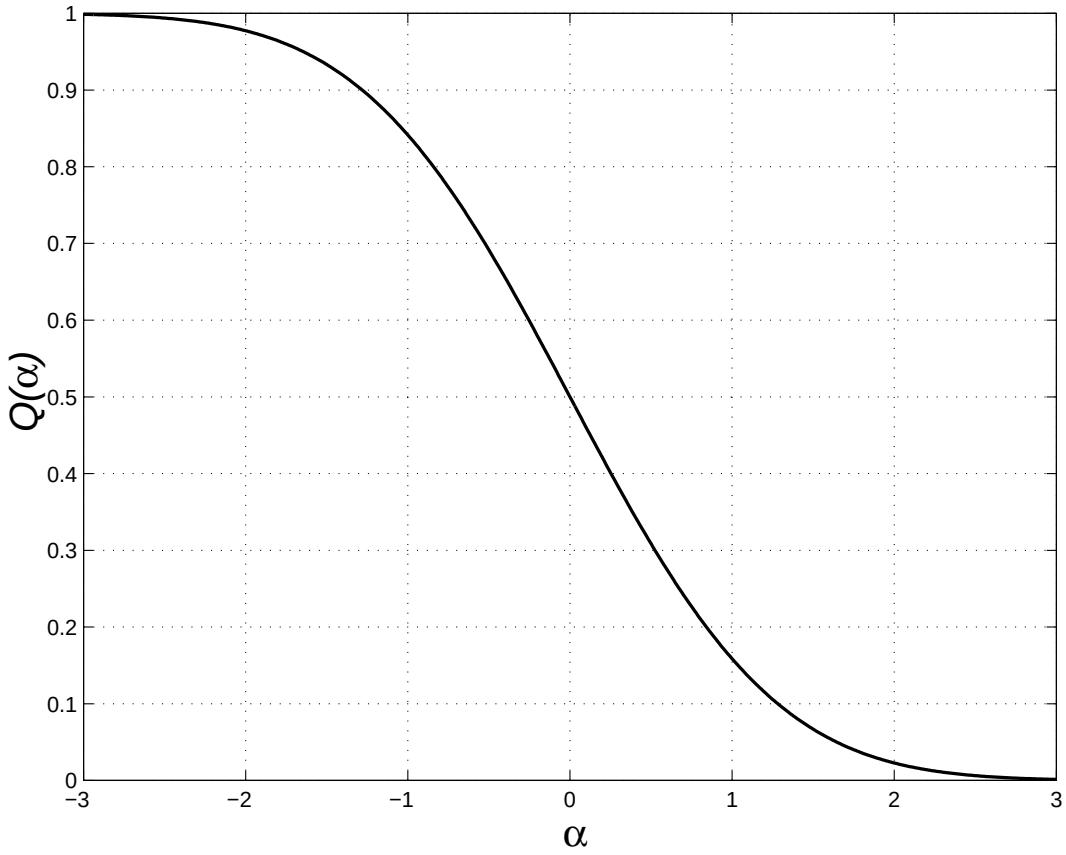

Figure A.4. The complementary Gaussian error function $Q(\alpha)$

Even if it is fairly simple, the following important relations are explicitly listed below:

$$P(x > \alpha) = Q\left(\frac{\alpha - \mu}{\sigma}\right), \tag{A.4.12}$$

$$P(x < \alpha) = 1 - Q\left(\frac{\alpha - \mu}{\sigma}\right) = Q\left(\frac{\mu - \alpha}{\sigma}\right). \tag{A.4.13}$$

The probability of a Gaussian random variable deviating by more than δ times the standard deviation σ from the mean μ is expressed by

$$P(|x - \mu| > \delta \cdot \sigma) = 2 \cdot Q(\delta) \tag{A.4.14}$$

and listed in Table A.1. In comparison, the Tchebycheff inequality only offers the very weak upper bound $P(|x - \mu| > \delta \cdot \sigma) \leq 1/\delta^2$.

For the complementary Gaussian error function, note the following impor-

Table A.4. The probability that a Gaussian random variable is outside δ standard deviations of the mean

δ	$P(\|x-\mu\| > \delta \cdot \sigma)$
1	$3.17 \cdot 10^{-1}$
2	$4.56 \cdot 10^{-2}$
3	$2.70 \cdot 10^{-3}$
4	$6.33 \cdot 10^{-5}$
5	$5.73 \cdot 10^{-7}$
6	$1.97 \cdot 10^{-9}$
7	$2.56 \cdot 10^{-12}$
8	$1.24 \cdot 10^{-15}$

tant properties of which the first two are trivial:

$$Q(-\infty) = 1, \quad Q(0) = \frac{1}{2}, \quad Q(+\infty) = 0, \tag{A.4.15}$$

$$Q(\alpha) + Q(-\alpha) = 1, \tag{A.4.16}$$

$$Q(\alpha) \leq \frac{e^{-\alpha^2/2}}{2} \quad \text{for } \alpha \geq 0, \tag{A.4.17}$$

$$Q(\sqrt{\alpha+\beta}) \leq Q(\sqrt{\alpha}) \cdot e^{-\beta/2} \quad \text{for } \alpha, \beta \geq 0. \tag{A.4.18}$$

Proof. (A.4.15) and (A.4.16) are trivial. For the proof of (A.4.17), let x_1, x_2 be two statistically independent random variables with a $N(0,1)$ distribution. Let $\alpha \geq 0$. Then we obtain

$$\begin{aligned} Q^2(\alpha) &= P(x_1 > \alpha) \cdot P(x_2 > \alpha) = P(x_1 > \alpha \text{ and } x_2 > \alpha) \\ &\leq P(x_1^2 + x_2^2 > 2\alpha^2 \text{ and } x_1 > 0 \text{ and } x_2 > 0) \\ &= \frac{1}{4} \cdot P(x_1^2 + x_2^2 > 2\alpha^2), \end{aligned}$$

where the last equality can be seen by expanding the complement of a disk in one quadrant to all quadrants. Using the same substitution as for the proof of (A.4.5), it is simple to show that

$$P(x_1^2 + x_2^2 > 2\alpha^2) = e^{-\alpha^2},$$

which completes the proof of (A.4.17). Another proof of (A.4.17) can be found in [66]. Next, we will prove (A.4.18). With a simple shift we obtain

$$\begin{aligned} Q(\sqrt{\alpha+\beta}) &= \int_{\sqrt{\alpha+\beta}}^{\infty} e^{-\eta^2/2}\, d\eta \\ &= \int_{\sqrt{\alpha}}^{\infty} \exp(-\underbrace{(\eta + \sqrt{\alpha+\beta} - \sqrt{\alpha})^2/2}_{\geq\, \eta^2/2 + \beta/2})\, d\eta \\ &\leq e^{-\beta/2} \cdot Q(\sqrt{\alpha}), \end{aligned}$$

where the inequality below the brace is obtained as follows: by simply rearranging

$$\eta \geq \sqrt{\alpha} = \frac{\sqrt{\alpha(\alpha+\beta)} - \alpha}{\sqrt{\alpha+\beta} - \sqrt{\alpha}}$$

we obtain

$$\underbrace{\eta(\sqrt{\alpha+\beta} - \sqrt{\alpha}) - \sqrt{\alpha(\alpha+\beta)} + \alpha + \eta^2/2 + \beta/2}_{= (\eta + \sqrt{\alpha+\beta} - \sqrt{\alpha})^2/2} \geq \eta^2/2 + \beta/2.$$

Thus (A.4.18) is proved. This result is used in the proof of Theorem 11.1. ■

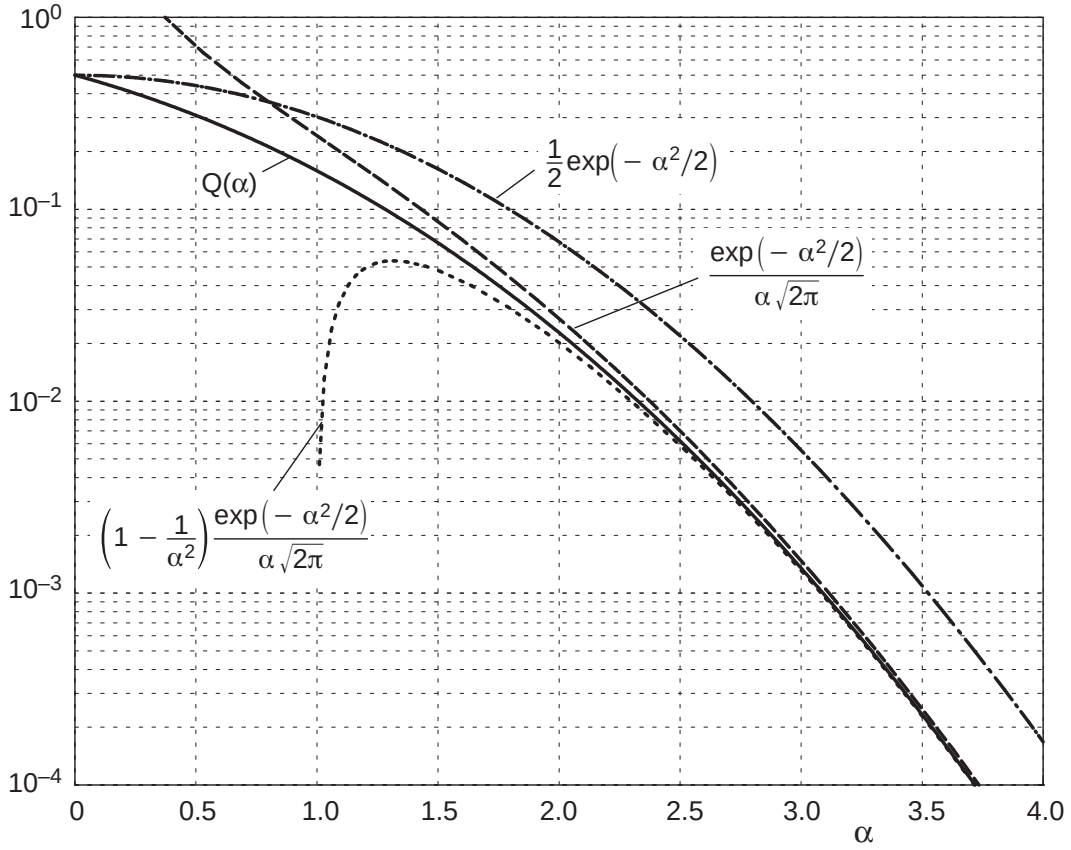

Figure A.5. Bounds for the complementary Gaussian error function $Q(\alpha)$

For large values of α there exists an extremely precise approximation [139, 149] which is not only of theoretical interest but also of great practical importance for numerical computations:

$$\left(1 - \frac{1}{\alpha^2}\right) \frac{e^{-\alpha^2/2}}{\alpha\sqrt{2\pi}} < Q(\alpha) < \frac{e^{-\alpha^2/2}}{\alpha\sqrt{2\pi}} \quad \text{for } \alpha > 0. \tag{A.4.19}$$

The bounds in (A.4.17) and (A.4.19) are shown in Figure A.5. The upper and lower bounds in (A.4.19) can be equivalently expressed by an error term ε_α:

$$Q(\alpha) = \frac{e^{-\alpha^2/2}}{\alpha\sqrt{2\pi}} \cdot (1 - \varepsilon_\alpha) \quad \text{with} \quad 0 < \varepsilon_\alpha < \frac{1}{\alpha^2} \tag{A.4.20}$$

Proof of (A.4.19).

$$Q(\alpha) = \frac{1}{\sqrt{2\pi}} \cdot \int_\alpha^\infty \underbrace{\eta^{-1}}_{u(\eta)} \cdot \underbrace{\eta e^{-\eta^2/2}}_{v'(\eta)} \, d\eta$$

apply integration by parts, $u'(\eta) = -\eta^{-2}, v(\eta) = -e^{-\eta^2/2}$

$$= \frac{1}{\sqrt{2\pi}} \left[\frac{1}{\alpha} e^{-\alpha^2/2} - \int_\alpha^\infty \underbrace{\frac{1}{\eta^2}}_{\leq \eta/\alpha^3} \cdot e^{-\eta^2/2} \, d\eta \right].$$

Since the above integrand is positive, we directly obtain the right hand side of (A.4.19). For the proof of the left hand side we will use the previously mentioned approximation:

$$Q(\alpha) \geq \frac{1}{\sqrt{2\pi}} \left[\frac{e^{-\alpha^2/2}}{\alpha} - \frac{1}{\alpha^3} \cdot \underbrace{\int_\alpha^\infty \eta \cdot e^{-\eta^2/2} \, d\eta}_{= e^{-\alpha^2/2}} \right] = \frac{1}{\sqrt{2\pi}} \left(\frac{1}{\alpha} - \frac{1}{\alpha^3} \right) e^{-\alpha^2/2}.$$

Therefore, the left hand hand side of (A.4.19) is also proved. ■

With $\alpha = \sqrt{2E_c/N_0} \to \infty$, (A.4.19) or (A.4.20) lead to the following result, which is the basis for the derivation of the asymptotic coding gain in Section 1.7:

$$Q\left(\sqrt{\frac{2E_c}{N_0}} \right) = e^{-E_c/N_0 (1 + o(1))}. \tag{A.4.21}$$

The series expansion $e^x = \sum_{r=0}^{\infty} \frac{x^r}{r!}$ for the exponential function can be used to

derive the corresponding series expansion for the Q function:

$$\begin{aligned} Q(\alpha) &= \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \cdot \int_0^\alpha e^{-\eta^2/2}\, d\eta \\ &= \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \sum_{r=0}^{\infty} \frac{(-1)^r}{2^r r!} \int_0^\alpha \eta^{2r}\, d\eta \\ &= \frac{1}{2} - \frac{1}{\sqrt{2\pi}} \sum_{r=0}^{\infty} \frac{(-1)^r}{2^r (2r+1) r!} \cdot \alpha^{2r+1}. \end{aligned} \tag{A.4.22}$$

In the neighbourhood of 0 we therefore have the following Taylor approximation with a first degree polynomial:

$$Q(\alpha) \;\approx\; \frac{1}{2} - \frac{\alpha}{\sqrt{2\pi}}. \tag{A.4.23}$$

A.4.3 The Multi-Dimensional Gaussian (Normal) Distribution

Let $\boldsymbol{x} = (x_1, \ldots, x_n)$ be an arbitrary n-dimensional random vector with the mean vector $\boldsymbol{\mu} = E(\boldsymbol{x}) = (E(x_1), \ldots, E(x_n)) \in \mathbb{R}^n$ and the (n,n)-dimensional *covariance matrix*

$$\boldsymbol{\Sigma} = E((\boldsymbol{x} - \boldsymbol{\mu})^T (\boldsymbol{x} - \boldsymbol{\mu})) = \Big((x_i - \mu_i)(x_j - \mu_j) \Big)_{i,j=1}^{n} \in \mathbb{R}^{n,n}. \tag{A.4.24}$$

All vectors are row vectors. For an arbitrary row vector $\boldsymbol{a} \in \mathbb{R}^n$ with $\boldsymbol{a} \neq \boldsymbol{0}$,

$$\begin{aligned} \boldsymbol{a}\boldsymbol{\Sigma}\boldsymbol{a}^T &= E(\boldsymbol{a}(\boldsymbol{x} - \boldsymbol{\mu})^T (\boldsymbol{x} - \boldsymbol{\mu})\boldsymbol{a}^T) \\ &= E(y^2) > 0 \quad \text{where} \quad y = \boldsymbol{a}(\boldsymbol{x} - \boldsymbol{\mu})^T = (\boldsymbol{x} - \boldsymbol{\mu})\boldsymbol{a}^T, \end{aligned}$$

excluding the case of a constant random vector $\boldsymbol{x} \equiv \boldsymbol{\mu}$. A square matrix $\boldsymbol{\Sigma} \in \mathbb{R}^{n,n}$ with the property $\boldsymbol{a}\boldsymbol{\Sigma}\boldsymbol{a}^T > 0$ for all $\boldsymbol{a} \neq \boldsymbol{0}$ is called *positive definite*. An equivalent characterization of positive definite matrices is that there exists a non-singular square matrix $\boldsymbol{C} \in \mathbb{R}^{n,n}$ such that $\boldsymbol{C}\boldsymbol{\Sigma}\boldsymbol{C}^T = \boldsymbol{I_n}$, where $\boldsymbol{I_n} \in \mathbb{R}^{n,n}$ denotes the identity matrix.

After these preparations, we can finally get to the actual definition: an n-dimensional random vector $\boldsymbol{x}$ has a *multi-dimensional Gaussian distribution* (also called *multivariate normal distribution*), written as $\boldsymbol{x} \sim N(\boldsymbol{\mu}, \boldsymbol{\Sigma})$, if

$$f_{\boldsymbol{x}}(\boldsymbol{\xi}) = \frac{(2\pi)^{-n/2}}{\sqrt{\det(\boldsymbol{\Sigma})}} \exp\left(-\frac{1}{2} (\boldsymbol{\xi} - \boldsymbol{\mu}) \boldsymbol{\Sigma}^{-1} (\boldsymbol{\xi} - \boldsymbol{\mu})^T \right) \tag{A.4.25}$$

for the n-dimensional PDF. Then

$$E(\boldsymbol{x}) = \boldsymbol{\mu}, \qquad E((\boldsymbol{x} - \boldsymbol{\mu})^T (\boldsymbol{x} - \boldsymbol{\mu})) = \boldsymbol{\Sigma}. \tag{A.4.26}$$

For $n = 1$, $\boldsymbol{\Sigma} = \sigma^2$ is valid, thus $n = 1$ is a special case of the general case. If the components of the random vector are mutually statistically independent, then $\boldsymbol{\Sigma} = \operatorname{diag}(\sigma_1^2, \ldots, \sigma_n^2)$ is a diagonal matrix with $\boldsymbol{\Sigma}^{-1} = \operatorname{diag}(\sigma_1^{-2}, \ldots, \sigma_n^{-2})$ for the inverse matrix and $\det(\boldsymbol{\Sigma}) = \sigma_1^2 \cdots \sigma_n^2$ for the determinant, thus we obtain a factorization of the n-dimensional PDF into the product of the n single (i.e., marginal) PDFs:

$$\begin{aligned} f_{\boldsymbol{x}}(\boldsymbol{\xi}) &= \frac{(2\pi)^{-n/2}}{\sqrt{\sigma_1^2 \cdots \sigma_n^2}} \exp\left(-\frac{1}{2}\sum_{i=1}^{n} \frac{(\xi_i - \mu_i)^2}{\sigma_i^2}\right) \\ &= \prod_{i=1}^{n} \frac{1}{\sqrt{2\pi\sigma_i^2}} \exp\left(-\frac{(\xi_i - \mu_i)^2}{2\sigma_i^2}\right). \end{aligned} \tag{A.4.27}$$

Proof that the multiple integral over the PDF actually attains the value 1. Let $\boldsymbol{C}\boldsymbol{\Sigma}\boldsymbol{C}^T = \boldsymbol{I_n}$ or $\boldsymbol{\Sigma} = \boldsymbol{C}^{-1}\boldsymbol{C}^{-T}$ (the power $-T$ denotes the transposition of the inverse matrix), then $\boldsymbol{\Sigma}^{-1} = \boldsymbol{C}^T\boldsymbol{C}$ and $\sqrt{\det(\boldsymbol{\Sigma})} = 1/\det(\boldsymbol{C})$. With the substitution $\boldsymbol{\eta} = (\boldsymbol{\xi} - \boldsymbol{\mu})\boldsymbol{C}^T$, the Jacobian $\det(\partial\boldsymbol{\eta}/\partial\boldsymbol{\xi}) = \det(\boldsymbol{C})$ and (A.4.25), we have:

$$\begin{aligned} \int_{\mathbb{R}^n} \cdots \int f_{\boldsymbol{x}}(\boldsymbol{\xi})\, d\boldsymbol{\xi} &= \frac{(2\pi)^{-n/2}}{\sqrt{\det(\boldsymbol{\Sigma})}} \int_{\mathbb{R}^n} \cdots \int \exp\left(-\frac{1}{2}(\boldsymbol{\xi} - \boldsymbol{\mu})\boldsymbol{C}^T\boldsymbol{C}(\boldsymbol{\xi} - \boldsymbol{\mu})^T\right) d\boldsymbol{\xi} \\ &= \frac{(2\pi)^{-n/2}}{\sqrt{\det(\boldsymbol{\Sigma})}} \cdot \frac{1}{\det(\boldsymbol{C})} \cdot \int_{\mathbb{R}^n} \cdots \int \exp\left(-\frac{1}{2}\boldsymbol{\eta}\boldsymbol{\eta}^T\right) d\boldsymbol{\eta} \\ &= \prod_{i=1}^{n} \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\infty} \exp\left(-\frac{1}{2}\eta_i^2\right) d\eta_i = 1, \end{aligned}$$

because every single factor is 1 according to (A.4.5). ■

We will now consider linear transformations (i.e., linear combinations) of Gaussian distributed random vectors. Let $\boldsymbol{x}$ be an n-dimensional random row vector and $\boldsymbol{A} \in \mathbb{R}^{n,l}$ be a transformation matrix with $n \geq l = \operatorname{rank}(\boldsymbol{A})$, then $\boldsymbol{x}\boldsymbol{A}$ is a shorter or equally long l-dimensional random vector. The Gaussian distribution is invariant to linear transformations and additive shifts:

$$\boldsymbol{x} \sim N(\boldsymbol{\mu}, \boldsymbol{\Sigma}) \quad \Longrightarrow \quad \boldsymbol{y} = \boldsymbol{x}\boldsymbol{A} + \boldsymbol{b} \sim N(\boldsymbol{\mu}\boldsymbol{A} + \boldsymbol{b}, \boldsymbol{A}^T\boldsymbol{\Sigma}\boldsymbol{A}). \tag{A.4.28}$$

Proof. The equation $E(\boldsymbol{y}) = E(\boldsymbol{x}\boldsymbol{A}+\boldsymbol{b}) = E(\boldsymbol{x})\boldsymbol{A}+\boldsymbol{b} = \boldsymbol{\mu}\boldsymbol{A}+\boldsymbol{b}$ is trivial for the mean vector. The precondition $n \geq l = \operatorname{rank}(\boldsymbol{A})$ guarantees that $\boldsymbol{A}^T\boldsymbol{\Sigma}\boldsymbol{A} \in \mathbb{R}^{l,l}$ is a non-singular matrix. With

$$\begin{aligned} E([\boldsymbol{y} - E(\boldsymbol{y})]^T[\boldsymbol{y} - E(\boldsymbol{y})]) &= E([(\boldsymbol{x} - \boldsymbol{\mu})\boldsymbol{A}]^T[(\boldsymbol{x} - \boldsymbol{\mu})\boldsymbol{A}]) \\ &= E(\boldsymbol{A}^T(\boldsymbol{x} - \boldsymbol{\mu})^T(\boldsymbol{x} - \boldsymbol{\mu})\boldsymbol{A}) \\ &= \boldsymbol{A}^T\boldsymbol{\Sigma}\boldsymbol{A} \end{aligned}$$

we obtain the covariance matrix in (A.4.28). ■

Another interesting property of the multi-dimensional Gaussian distribution is that all marginal and all conditional distributions derived from a Gaussian distribution are again Gaussian distributions. A more detailed study of this theory can be found in [2].

The sum of two arbitrary statistically dependent or independent Gaussian random variables is again Gaussian distributed, which follows directly from (A.4.28) for $n = 2$ and $l = 1$ and $\boldsymbol{A} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$ and $\boldsymbol{b} = \boldsymbol{0}$.

We will now discuss the case of an arbitrary Gaussian random vector of length $n = 2$ (also called *bivariate Gaussian distribution*) in detail. The equation $E((x_i - \mu_i)^2/\sigma_i^2) = 1$ is apparent and the *correlation coefficient* between x_1 and x_2 is defined as

$$\rho = E\left(\left(\frac{x_1 - \mu_1}{\sigma_1}\right)\left(\frac{x_2 - \mu_2}{\sigma_2}\right)\right). \tag{A.4.29}$$

Then we have the following for the covariance matrix

$$\boldsymbol{\Sigma} = \begin{pmatrix} \sigma_1^2 & \rho\sigma_1\sigma_2 \\ \rho\sigma_1\sigma_2 & \sigma_2^2 \end{pmatrix}, \qquad \boldsymbol{\Sigma}^{-1} = \frac{1}{1-\rho^2}\begin{pmatrix} \frac{1}{\sigma_1^2} & \frac{-\rho}{\sigma_1\sigma_2} \\ \frac{-\rho}{\sigma_1\sigma_2} & \frac{1}{\sigma_2^2} \end{pmatrix},$$

$$\det(\boldsymbol{\Sigma}) = \sigma_1^2\sigma_2^2(1-\rho^2),$$

thus

$$f_{\boldsymbol{x}}(\xi_1, \xi_2) = \frac{1}{2\pi\sigma_1\sigma_2\sqrt{1-\rho^2}} \tag{A.4.30}$$
$$\cdot \exp\left(-\frac{1}{2(1-\rho^2)}\left(\frac{(\xi_1-\mu_1)^2}{\sigma_1^2} - 2\rho\frac{(\xi_1-\mu_1)(\xi_2-\mu_2)}{\sigma_1\sigma_2} + \frac{(\xi_2-\mu_2)^2}{\sigma_2^2}\right)\right).$$

Obviously the non-correlation, $\rho = 0$ or $E((\xi_1 - \mu_1)(\xi_2 - \mu_2)) = 0$, is equivalent to the statistical independence, but this only applies for random variables with Gaussian distributions and not for other distributions!

A geometric interpretation of the 2-dimensional Gaussian PDF is enlightening. The density $f_{\boldsymbol{x}}(\xi_1, \xi_2)$ can be thought of as a surface over the (ξ_1, ξ_2)-plane. The special case of two statistically independent components with the same variance is shown in Figure 2.1, so $\boldsymbol{\Sigma} = E(\boldsymbol{x}^T\boldsymbol{x}) = \sigma^2 \cdot \boldsymbol{I}_2$ as well as $E(\boldsymbol{x}) = \boldsymbol{0}$ are presupposed. This describes the 2-dimensional or complex-valued passband noise of the AWGN channel, and so the notation $\boldsymbol{\nu} = (\nu_I, \nu_Q)$ is used in Figure 2.1 as well as in Chapters 2, 3 and 11. The energy of the noise components $E(\nu_I^2) = E(\nu_Q^2) = \sigma^2 = N_0/2$ corresponds to the variances.

From Figure 2.1 it is obvious that the 2-dimensional PDF is *rotationally invariant* (also addressed as *circular symmetry*), in other words, on circles with

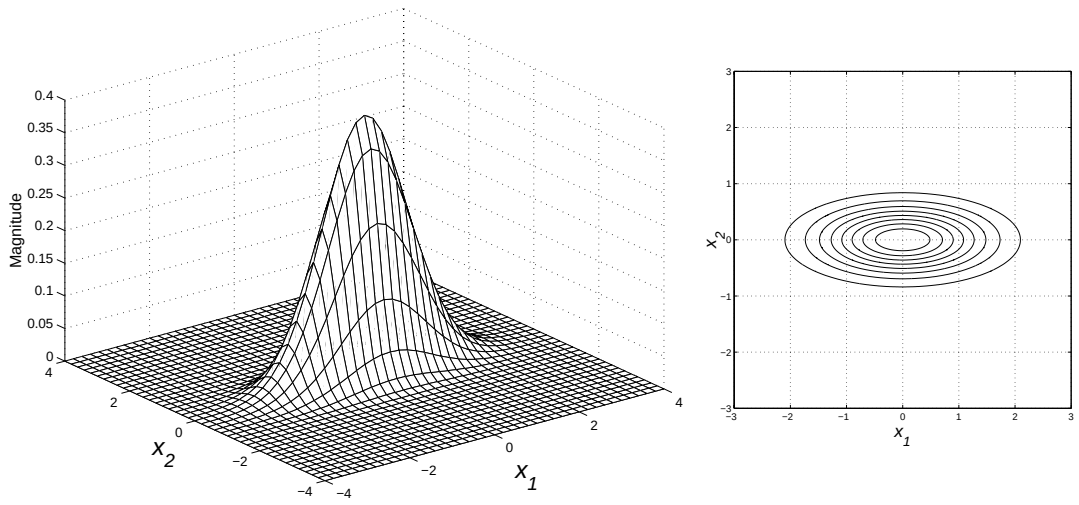

Figure A.6. Bivariate Gaussian PDF and associated contour plot for $\sigma_1 = 1$, $\sigma_2 = 0.4$ and $\rho = 0$

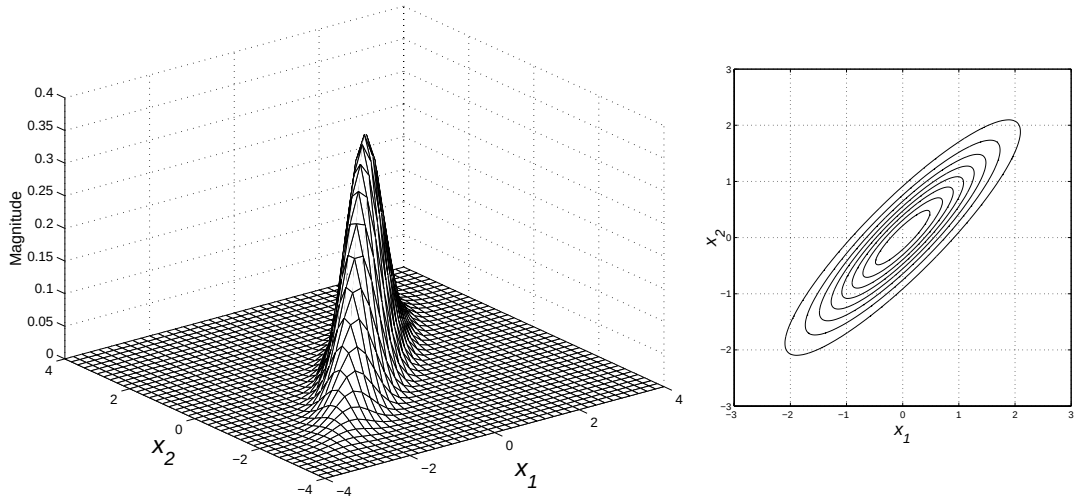

Figure A.7. Bivariate Gaussian PDF and associated contour plot for $\sigma_1 = 1$, $\sigma_2 = 1$ and $\rho = 0.9$

centers at the origin the Gaussian PDF assumes constant values (presupposing the case of $\sigma_1 = \sigma_2$ and $\rho = 0$).

The Figures A.6 and A.7 illustrate the bivariate Gaussian PDF and the corresponding contour plots, as the parameters σ_1, σ_2, and ρ are varied (where no generality is lost in assuming zero means). In Figure A.6, the two components are still statistically independent (uncorrelated, $\rho = 0$) but with unequal variances ($\sigma_1 \neq \sigma_2$). As a result, of course, the spread of the PDF is greater in the x_1 direction than in the x_2 direction. The lines in the contour plots denoting a constant value of the PDF have now the shape of an ellipse (instead of a circle as for uncorrelated components with equal variances). Figure A.7 shows correlated components with equal variances. Obviously, the PDF and the contour plot are

symmetrical about the line $x_1 = x_2$ in the (x_1, x_2) plane, indicating the strong linear relationship between x_1 and x_2 for a correlation coefficient of $\rho = 0.9$. For $\rho = -0.9$, the plots are symmetrical about the line $x_1 = -x_2$.

We again presuppose the previous special case with equal variances in both components. The statistical independence is now maintained under rotations, which is easy to show: a rotation by the angle φ is described in $\mathbb{C}$ by $(y_1 + jy_2) = (x_1 + jx_2) \cdot e^{j\varphi}$ or in the 2-dimensional space $\mathbb{R}^2$ by

$$(y_1, y_2) = (x_1, x_2) \cdot \boldsymbol{R} \quad \text{where} \quad \boldsymbol{R} = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix}. \tag{A.4.31}$$

The equation $\boldsymbol{\Sigma}_x = E(\boldsymbol{x}^T \boldsymbol{x}) = \sigma^2 \cdot \boldsymbol{I}_2$ then implies that

$$\begin{aligned} \boldsymbol{\Sigma}_y &= E(\boldsymbol{y}^T \boldsymbol{y}) = E(\boldsymbol{R}^T \boldsymbol{x}^T \boldsymbol{x} \boldsymbol{R}) = \sigma^2 \cdot \boldsymbol{R}^T \boldsymbol{R} \\ &= \sigma^2 \cdot \boldsymbol{I}_2. \end{aligned} \tag{A.4.32}$$

Hence, after a rotation the components of the 2-dimensional or the complex-valued noise are still statistically independent, however, only if both components have the same variance.

A.4.4 The Rayleigh Distribution

The random variable amplitude of a fading channel can sometimes only be represented by very difficult models. For the simplest case, the fading amplitude can be described by the Rayleigh distribution discussed in this subsection.

In the generalized case, the Rayleigh distribution is typically written with a parameter λ. The PDF then looks like

$$f_\lambda(\xi) = \left\{ \begin{array}{ll} \dfrac{\xi}{\lambda} \cdot e^{-\xi^2/2\lambda} & \text{if } \xi \geq 0 \\ \\ 0 & \text{if } \xi < 0 \end{array} \right\}. \tag{A.4.33}$$

In Figure A.6 the PDF for the special case of $\lambda = 1/2$ is shown, which was also presupposed for (11.2.4). For the general case, note that

$$E(x) = \sqrt{\frac{\pi\lambda}{2}}, \quad E(x^2) = 2\lambda, \quad D^2(x) = 2\lambda \left(1 - \frac{\pi}{4}\right). \tag{A.4.34}$$

The maximum of the PDF is $1/\sqrt{e\lambda}$ and is taken on at $\xi = \sqrt{\lambda}$. If y has a Rayleigh distribution with $\lambda = 1$, then $x = y \cdot \sqrt{\lambda}$ has a PDF like (A.4.33).

If x_1 and x_2 are two statistically independent $N(0, 1/2)$ distributed Gaussian random variables, then it is easy to prove (by using polar coordinates as in the proof of (A.4.5)) that the random variable $\sqrt{x_1^2 + x_2^2} = |x_1 + jx_2|$, which obviously corresponds to the absolute value of the complex-valued or 2-dimensional Gaussian noise, is Rayleigh distributed with $\lambda = 1/2$.

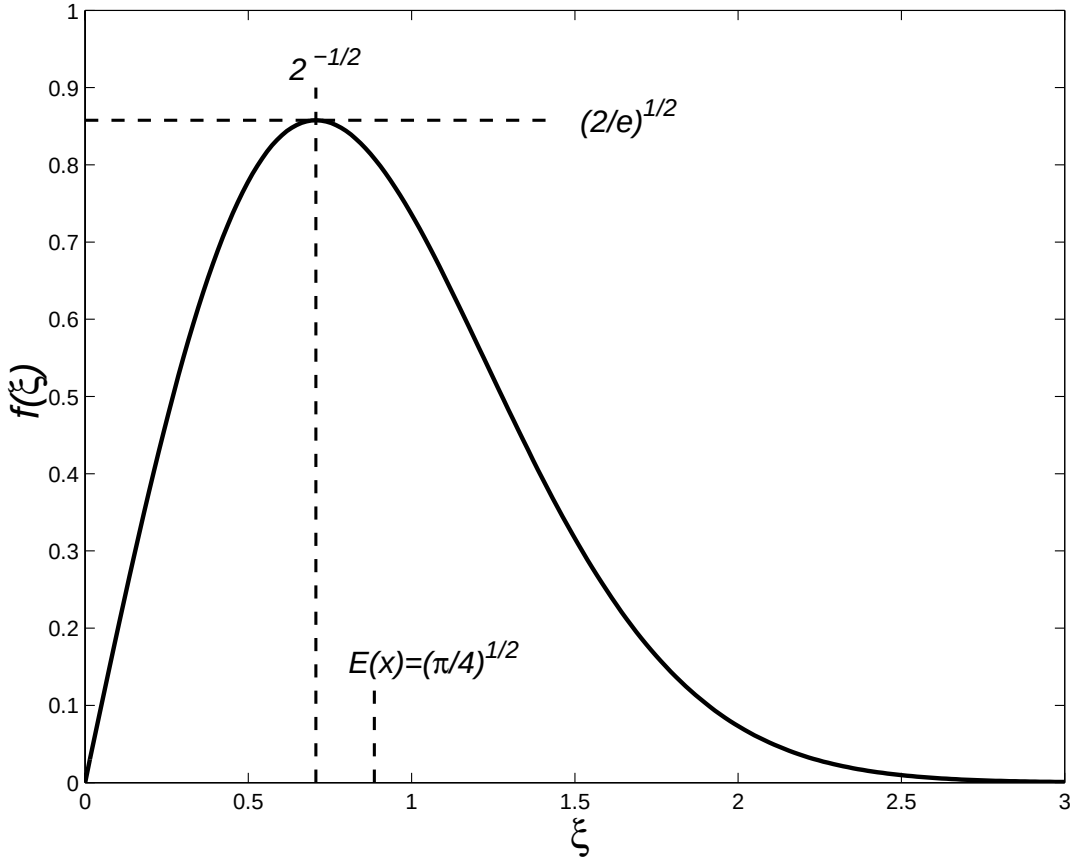

Figure A.8. The Rayleigh PDF for $\lambda = 1/2$

A.4.5 Further Distributions

For the *uniform distribution* all possible values are attained with the same probability. A real-valued uniform distribution is characterized by two parameters ξ_a, ξ_b with $\xi_a < \xi_b$:

$$f_x(\xi) = \left\{ \begin{array}{ll} 1/(\xi_b - \xi_a) & \xi_a < \xi < \xi_b \\ 0 & \text{otherwise} \end{array} \right\}. \tag{A.4.35}$$

Note that $E(x) = (\xi_a + \xi_b)/2$ and $D^2(x) = (\xi_b - \xi_a)^2/12$. A discrete-valued uniform distribution with the range $\xi_1, \ldots, \xi_q$ is defined by $P(x = \xi_i) = 1/q$.

A.5 The Entropy of a Discrete Random Variable

Let x be a discrete-valued random variable which attains q possible values $\xi_1, \ldots, \xi_q$ with the probabilities $p_i = P(x = \xi_i)$. When we receive a sample of x, how much information do we get? For example, if $p_1 = 1$ (and thus

$p_2 = \cdots = p_q = 0$), then there is no surprise, no information, since we know what the message must be. On the other hand, if the p_i are all very different, then when a symbol with a low p_i is received, we feel more surprised, get more information, than when a symbol with large probability p_i arrives. Thus information is somewhat inversely related to the probability of occurrence. It turns out that $-\log_2 p_i$ is a useful measure for the amount of information of an outcome with probability p_i.

As a measure of the amount of information (or uncertainty) of a random variable we define the *entropy* as

$$H(x) = E(-\log_2 P(x)) \tag{A.5.1}$$

$$= -\sum_{i=1}^{q} p_i \log_2 p_i = \sum_{i=1}^{q} p_i \log_2 \frac{1}{p_i} \tag{A.5.2}$$

$$= H(p_1, \ldots, p_q). \tag{A.5.3}$$

For completeness we mention the alternative denotations

$$H(x) = -\sum_{i=1}^{q} P(x = \xi_i) \log_2 P(x = \xi_i) = -\sum_{x} P(x) \log_2 P(x).$$

The entropy is measured in units of bits because of the use of the logarithm to the base 2. Since the entropy only depends on the distribution, i.e., only depends on the p_i and not on the ξ_i, we also speak of the entropy of the distribution and use the denotation $H(p_1, \ldots, p_q)$ for it. Formally, we set $0 \cdot \log_2 0 = 0$ which matches $\lim_{\alpha \to 0} \alpha \log_2 \alpha = 0$. So the p_i could be extended by an arbitrary number of zeros, i.e., $H(p_1, \ldots, p_q) = H(p_1, \ldots, p_q, 0, \ldots, 0)$.

For a binary random variable x, for which the two values occur with the probabilities λ and $1-\lambda$, we obtain the entropy from the binary entropy function as $H(x) = H_2(\lambda)$. For $\lambda = 1/2$ we have a uniform distributed binary random variable (corresponding to the definition of equal a priori probabilities in Section 1.6) with $H(x) = 1$. The entropy of the binomial distribution is discussed in Problem 3.6.

Generally, the entropy is bounded as follows:

$$0 \leq H(x) \leq \log_2 q. \tag{A.5.4}$$

The inequality $p_i \leq 1$ trivially implies that $H(x) \geq 0$. Obviously the entropy $H(x)$ attains the minimum value 0 if and only if a value ξ_i occurs with a probability of 1 and the other $q - 1$ values occur with a probability of 0, i.e., the random variable x is constant (also called *single-point distribution*). The entropy attains its maximum, when all values are taken on with the same probability of $p_i = 1/q$, which will be proved below in (A.5.8).

The entropy is only defined for discrete-valued random variables, for a continuous-valued random variable the previous definition would result in an

infinitely large entropy. A different entropy definition for continuous-valued random variables is given in (3.5.2).

Let p'_i be a another discrete probability distribution. Trivially, the following relationship between two arbitrary probability distributions is valid:

$$-\sum_{i=1}^{q} p_i \log_2 p'_i \geq 0. \tag{A.5.5}$$

The following extended relation between two arbitrary probability distributions is called the *fundamental inequality* and is valid for arbitrary bases a:

$$\sum_{i=1}^{q} p_i \log_a \frac{p'_i}{p_i} \leq 0 \tag{A.5.6}$$

$$= 0 \quad \text{if and only if } p_i = p'_i \text{ for all } i. \tag{A.5.7}$$

Proof of the fundamental inequality. We will use the inequality $\ln x \leq x - 1$ for all $x > 0$, where the equality $\ln x = x - 1$ is only valid for $x = 1$:

$$\sum_{i=1}^{q} p_i \log_a \frac{p'_i}{p_i} = \frac{1}{\ln a} \sum_{i=1}^{q} p_i \ln \frac{p'_i}{p_i} \leq \frac{1}{\ln a} \sum_{i=1}^{q} p_i \left(\frac{p'_i}{p_i} - 1 \right)$$

$$= \frac{1}{\ln a} \left(\sum_{i=1}^{q} p'_i - \sum_{i=1}^{q} p_i \right) = 0$$

Thus (A.5.6) and (A.5.7) are proved. ■

With $p'_i = 1/q$ we now have $0 \geq \sum_{i=1}^{q} p_i \log_2 \frac{1/q}{p_i} = -\log_2 q + H(x)$ and therefore the right hand side of (A.5.4). So the entropy attains its maximum for the discrete uniform distribution and its minimum for a constant random variable:

$$\underbrace{H(1, 0, \ldots, 0)}_{=0} \leq H(p_1, \ldots, p_q) \leq \underbrace{H\left(\frac{1}{q}, \ldots, \frac{1}{q}\right)}_{=\log_2 q}. \tag{A.5.8}$$

Therefore it is clear that the entropy actually describes the uncertainty of the output of a discrete-valued random variable.

The definition of the entropy can be directly extended to the joint distribution of several random variables. For two statistically independent random

variables x and x' with the distributions p_i and p'_i, we have

$$H(x,x') = -\sum_{i,j} P(x=\xi_i, x'=\xi'_j)\cdot \log_2 P(x=\xi_i, x'=\xi'_j) \tag{A.5.9}$$

$$\begin{aligned} &= -\sum_{i,j} p_i p'_j \log_2(p_i p'_j) \\ &= -\sum_{i,j} p_i p'_j \log_2 p_i - \sum_{i,j} p_i p'_j \log_2 p'_j \\ &= -\sum_{i=1}^{q} p_i \log_2 p_i - \sum_{j} p'_j \log_2 p'_j \\ &= H(x) + H(x'). \end{aligned} \tag{A.5.10}$$

Thus for a word $\boldsymbol{x}$ of length k with statistically independent and identically distributed components $x_1, \ldots, x_k$,

$$H(\boldsymbol{x}) = k \cdot \log_2 q. \tag{A.5.11}$$

Very often we are interested in the behaviour of one random variable when another random variable is specified, for example in the DMC output y when the input x is given or in x when y is given. The latter describes the actual task of information transmission, i.e., to decide from the output y with a minimum of uncertainty on the input x (which is extensively discussed in Chapter 3). The definition of entropy can be generalized to the *conditional entropy* of the discrete-valued random variable x given knowledge of the discrete-valued random variable y:

$$H(x|y) = E(-\log P(x|y)) \tag{A.5.12}$$

$$= -\sum_{x,y} P(x,y)\log_2 P(x|y), \quad \geq 0. \tag{A.5.13}$$

Note that we do not define $H(x|y) = -\sum_{x,y} P(x|y)\log_2 P(x|y)$. The definition above corresponds to the general formula $E(h(x,y)) = \sum_{x,y} P(x,y)h(x,y)$ for the mean of the random variable $h(x,y)$. Observing

$$\begin{aligned} H(x|y) - H(x) &= -\sum_{x,y} P(x,y)\log_2 P(x|y) + \sum_{x,y} P(x,y)\log_2 P(x) \\ &= \sum_{x,y} P(x,y)\log_2 \frac{P(x)}{P(x|y)} \\ &= \sum_{x,y} P(x,y)\log_2 \frac{P(x)\cdot P(y)}{P(x,y)} \\ &\leq 0 \quad \text{according to (A.5.6)}, \end{aligned}$$

we conclude that

$$H(x) \geq H(x|y) \tag{A.5.14}$$

with equality for statistically independent random variables x and y. So if there is a dependence between x and y, the uncertainty of x is reduced by the knowledge of y, i.e., conditioning on random variables can never increase uncertainty.

A.6 Algebraic Foundations

This section contains a survey of some basic algebraic structures like equivalence classes, groups, cosets, rings, ideals, and fields. Elementary algebra uses the binary operations of arithmetic such as addition and multiplication on sets of numbers. Important simple examples are the set $\mathbb{N}$ of natural numbers (non-negative integers), the set $\mathbb{Z}$ of integers, the set $\mathbb{Q}$ of rational numbers, the set $\mathbb{R}$ of real numbers, and the set $\mathbb{C}$ of complex numbers. Die für die Codierungstheorie erforderliche Spezialisierung auf finite fields erfolgt in Abschnitt A.8 sowie in Kapitel 6. Als weitere Beispiele betrachten wir sets of matrices, or sets of vectors, wobei die coefficients Werte aus den vorangehend genannten sets annehmen können.

In modern algebra the level of abstraction is raised further by considering general operations (processes of combining two or more elements to yield another element) in general sets. Wir beschränken uns hierbei jedoch auf das für uns unbedingt Notwendige.

Eine Einführung in die algebraischen Grundbegriffe findet sich beispielsweise in [17, 144]. Ausführliche Darstellungen der Theorie der Galois fields bieten [24, 68, 78, 89, 92].

A.6.1 Equivalence Relations

Definition A.1 (Equivalence Relation). *Eine auf einer Menge $\mathcal{M}$ definierte Relation $\sim$ heißt* equivalence relation*, if it fulfills the following three axioms:*

1. *For all $a \in \mathcal{M}$: $a \sim a$ (reflexivity).*
2. *For all $a, b \in \mathcal{M}$: if $a \sim b$, then $b \sim a$ (symmetry).*
3. *For all $a, b, c \in \mathcal{M}$: if $a \sim b$ and $b \sim c$, then $a \sim c$ (transitivity).*

Als equivalence class $[a] = \{b \in \mathcal{M} \,|\, b \sim a\}$ *wird die Menge aller zu a äquivalenten Elemente bezeichnet. Jedes Element aus $[a]$ kann die equivalence class repräsentieren since $[b] = [a]$ for $b \in [a]$. Since $[b] \cap [a] = \emptyset$ for $b \notin [a]$, eqivalence classes are either identical or mutually disjoint. Hence, the collection of all distinct equivalence classes forms a* partition *of $\mathcal{M}$ into subsets.*

Rein formal ist die equivalence relation ein specific subset $\mathcal{S}$ of $\mathcal{M} \times \mathcal{M}$ (where $\times$ is used to denotes the set of ordered pairs), indem wir $(a, b) \in \mathcal{S} \subseteq \mathcal{M} \times \mathcal{M}$ für $a \sim b$ schreiben. Wir werden es aber bei der einfachen Schreibweise $a \sim b$ belassen.

Example A.1. Für $\mathcal{M} = \mathbb{Z}$ wird bei festem $p \in \mathbb{Z}$ durch

$$a \sim b \quad \Longleftrightarrow \quad a - b \text{ is a multiple of } p \tag{A.6.1}$$

eine equivalence relation auf $\mathbb{Z}$ definiert mit $[a] = \{a + rp | r \in \mathbb{Z}\}$, also

$$\begin{aligned} [0] &= \{\ldots, -2p, -p, 0, p, 2p, \ldots\}, \\ [1] &= \{\ldots, -2p+1, -p+1, 1, p+1, 2p+1, \ldots\}, \\ [p-1] &= \{\ldots, -p-1, -1, p-1, 2p-1, 3p-1, \ldots\}. \end{aligned}$$

Somit ergibt sich die partition $\mathbb{Z} = [0] \cup [1] \cup \ldots \cup [p-1]$. Für diesen Fall ist die Schreibweise

$$a = b \mod p \tag{A.6.2}$$

gebräuchlich and we say that a is *congruent* to b modulo p. We define on the equivalence classes an addition (denoted with + although it is certainly not the ordinary addition) by

$$[a] + [b] = [a + b]. \tag{A.6.3}$$

Similarly,

$$[a] \cdot [b] = [a \cdot b]. \tag{A.6.4}$$

These operations are well-defined, i.e., they are uniquely determined by the sets $[a]$ and $[b]$ alone and do not depend in any way on the representatives of the equivalence classes. This follows immediately from $[a' + b'] = [a + b]$ and $[a' \cdot b'] = [a \cdot b]$ for all $a' \in [a]$ and $b' \in [b]$.

The set of equivalence classes $\mathbb{Z}_p = \{[0], [1], [2], \ldots, [p-1]\}$ is called the *set of integers modulo p*. Abkürzend wird dafür üblicherweise

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\} \tag{A.6.5}$$

geschrieben mit der Vereinbarung daß die arithmetic operations modulo p gemeint sind. ■

A.6.2 Groups

Definition A.2 (Group). *A* group $(\mathcal{G}, *)$ *is a set* $\mathcal{G}$ *together with a binary operation* $*$ *on* $\mathcal{G}$ *such that the following axioms (1-4) are satisfied. The group is called* commutative *or* abelian *if axiom (5) is also satisfied.*

1. Closed*: $a * b \in \mathcal{G}$ for all $a, b \in \mathcal{G}$.*

2. Associative law*:* $(a * b) * c = a * (b * c)$ *for all* $a, b, c \in \mathcal{G}$*.*

3. Neutral element *(also called* identity*): there exists an* $e \in \mathcal{G}$ *such that* $a * e = e * a = a$ *for all* $a \in \mathcal{G}$*.*

4. Inverse element*: for each* $a \in \mathcal{G}$ *there exists an* $\bar{a} \in \mathcal{G}$ *such that* $a * \bar{a} = \bar{a} * a = e$ *.*

5. Commutative law*:* $a * b = b * a$ *for all* $a, b \in \mathcal{G}$*.*

Die Anzahl der Elemente von $\mathcal{G}$*, also die cardinality* $|\mathcal{G}|$*, wird auch als* order *bezeichnet.*

Falls die Operation $*$ *der Addition entspricht, so wird das neutral element als 0 und das inverse Element zu* a *als* $-a$ *geschrieben mit der Vereinbarung* $a + (-b) = a - b$*.*

Falls die Operation $*$ *dagegen der Multiplikation entspricht, so wird das neutral element als 1 und das inverse Element zu* a *als* a^{-1} *geschrieben mit den Vereinbarungen* $a \cdot b = ab$*,* $a^n = a \cdots a$ *(n times) und* $a \cdot b^{-1} = \dfrac{a}{b}$*.*

Generell ist das neutrale Element eindeutig bestimmt, denn wenn e und e' jeweils neutrale Elemente wären, so folgt aus $e = e * e' = e'$ ihre Gleichheit. Auch das inverse Element ist stets eindeutig bestimmt, denn wenn $\bar{a}$ und $\tilde{a}$ jeweils inverse Elemente zu a wären, so folgt aus $\bar{a} = \bar{a} * e = \bar{a} * (a * \tilde{a}) = (\bar{a} * a) * \tilde{a} = e * \tilde{a} = \tilde{a}$ ihre Gleichheit.

Example A.2. (1) Durch $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sowie $(\mathbb{Q}\backslash\{0\}, \cdot)$ werden kommutative Gruppen erklärt. Dagegen existieren in $(\mathbb{N}, +)$ und $(\mathbb{Z}\backslash\{0\}, \cdot)$ die inversen Elemente nicht.

(2) Die Menge aller (k, n)-dimensional matrices mit Koeffizienten aus $\mathbb{Q}$ oder $\mathbb{R}$ oder $\mathbb{C}$ bildet eine additive kommutative Gruppe.

Wenn wir nun die multiplication of matrices betrachten, so sind zunächst square matrices vorauszusetzen um die Abgeschlossenheit zu garantieren. Ohne weitere Einschränkungen existieren auch in der Menge aller quadratischen Matrizen die multiplikativen Inversen nicht generell. Erst bei der Beschränkung auf non-singular Matrizen ergibt sich eine nicht-kommutative multiplikative Gruppe mit der identity matrix als multiplicative neutral element.

(3) Die Menge $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ ist bezüglich der Addition modulo p eine Gruppe.

Die Menge $\mathcal{G} = \{1, 2, \ldots, p-1\} = \mathbb{Z}_p\backslash\{0\}$ ist bezüglich der Multiplikation modulo p genau dann eine Gruppe, wenn p prime ist. Denn wenn $p = sr$ keine Primzahl ist, so würde aus der Existenz von r^{-1} wegen $s = s \cdot 1 = s \cdot rr^{-1} = pr^{-1} = 0r^{-1} = 0$ ein Widerspruch folgen. Wenn p dagegen eine Primzahl ist, so existieren für $a \in \mathcal{G}$ nach dem Euclidean algorithm (siehe (A.7.4)) integers s und t mit $\mathrm{GCD}(a, p) = 1 = sa + tp$ und somit existiert $a^{-1} = s \in \mathcal{G}$. ■

Wenn $\mathcal{U}$ und $\mathcal{G}$ jeweils Gruppen sind mit $\mathcal{U} \subseteq \mathcal{G}$, so heißt $\mathcal{U}$ *subgroup* von $\mathcal{G}$. Sei nun $\mathcal{G}$ eine additive Gruppe. Für $a, b \in \mathcal{G}$ wird durch

$$a \sim b \quad \Longleftrightarrow \quad a - b \in \mathcal{U} \tag{A.6.6}$$

eine equivalence relation erklärt und die equivalence classes sind von der Form

$$[a] \;=\; a + \mathcal{U} \;=\; \{a + u \,|\, u \in \mathcal{U}\}. \tag{A.6.7}$$

In diesem Fall werden die equivalence classes als *cosets*, die partition als *standard array* und die representatives auch als *coset leader* bezeichnet.

Für $a \in \mathcal{U}$ gilt $[a] = \mathcal{U}$ und für alle $a \in \mathcal{G}$ gilt $|[a]| = |\mathcal{U}|$. Somit bilden die verschiedenen equivalence classes eine partition von $\mathcal{G}$ mit der Eigenschaft

$$(\text{number of distinct cosets}) \cdot |\mathcal{U}| = |\mathcal{G}|. \tag{A.6.8}$$

Falls die Ordnung von $\mathcal{G}$ endlich ist, muß $|\mathcal{U}|$ folglich ein Teiler von $|\mathcal{G}|$ sein – dies gilt nicht nur wie hier gezeigt für the addition als spezielle arithmetic operation sondern sogar für jede beliebige operation $*$ auf $\mathcal{G}$. Ein Beispiel zum standard array wird in Abschnitt 4.6 für lineare Codes gegeben. Der folgende Satz ist für Chapter 7 wichtig:

Theorem A.3. *Es sei $\mathcal{G}$ eine endliche multiplikative Gruppe der Ordnung n. Für $a \in \mathcal{G}$ ist*

$$\langle a \rangle \;=\; \{a^i \,|\, i \in \mathbb{Z}\} \;=\; \{a^1, a^2, a^3, \ldots, a^r\} \tag{A.6.9}$$

eine Untergruppe von $\mathcal{G}$, die aus den powers von a besteht. Als order *of the element a wird $r = |\langle a \rangle|$ bezeichnet und r is a divisor of n. Furthermore, $a^n = 1$ for all $a \in \mathcal{G}$.*

Falls ein Element $a \in \mathcal{G}$ mit $\langle a \rangle = \mathcal{G}$ existiert, so heißt $\mathcal{G}$ cyclic group *und a wird als* generator *für $\mathcal{G}$ bezeichnet. Für weitere generators gibt es ein einfaches Kriterium:*

$$\langle a^k \rangle = \mathcal{G} \quad \Longleftrightarrow \quad \mathrm{GCD}(k, n) = 1. \tag{A.6.10}$$

Proof. Offensichtlich ist $\{a^i \,|\, i \in \mathbb{Z}\}$ eine multiplicative group mit $a^0 = 1$ als neutral element und a^{-i} ist invers zu a^i. Da $\mathcal{G}$ endlich ist, gibt es in der enumeration $a^1, a^2, a^3, \ldots$ nur endlich viele verschiedene Elemente. Somit existiert ein minimales $r > 0$ mit $a^r = 1$ (denn wenn $a^r = a^l$ mit $l < r$ wäre, so würde ein $r' = r - l$ mit $a^{r'} = 1$ existieren, was einen Widerspruch zur Minimalität von r bedeuten würde).

The order $r = |\langle a \rangle|$ divides n according to (A.4.4). Also existiert ein $s \in \mathbb{Z}$ mit $rs = n$ und somit gilt $a^n = (a^r)^s = 1^s = 1$.

"(A.4.6)⇒": Sei $\langle a^k \rangle = \mathcal{G}$. Aus der Annahme $\mathrm{GCD}(k, n) = s > 1$ folgt $(a^k)^{n/s} = (a^n)^{k/s} = 1^{k/s} = 1$. Wegen $n/s < n$ kann a^k also nicht $\mathcal{G}$ erzeugen, was der Voraussetzung widerspricht. Somit folgt $s = 1$.

"(A.4.6)⇐": Sei $\mathrm{GCD}(k, n) = 1$. Aus der Annahme $\langle a^k \rangle \subset \mathcal{G}$ folgt die Existenz von s mit $s < n$ und $(a^k)^s = 1$. Wegen $\langle a \rangle = \mathcal{G}$ ist $ks < n$ ausgeschlossen

bzw. n muß sogar ein Teiler von ks sein. Da n und k nach Voraussetzung relatively prime sind, muß n ein Teiler von s sein und damit ergibt sich ein Widerspruch. Also folgt $\langle a^k \rangle = \mathcal{G}$. ■

Example A.3. Es wird eine Gruppe betrachtet, die aus den complex n-th *roots of unity* besteht, also aus den n complex numbers on the unit circle:

$$\mathcal{G} \;=\; \{e^{j2\pi r/n} \,|\, r = 0, 1, \ldots, n-1\} \;\subset\; \mathbb{C}. \tag{A.6.11}$$

Für $n = 3$ ergibt sich $\mathcal{G} = \{1, e^{j2\pi/3}, e^{j2\pi 2/3}\}$ mit:

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle e^{j2\pi/3} \rangle \;=\; \langle e^{j2\pi 2/3} \rangle &= \mathcal{G}. \end{aligned}$$

Für $n = 6$ ergibt sich $\mathcal{G} = \{1, e^{j2\pi/6}, e^{j2\pi 2/6}, \ldots, e^{j2\pi 5/6}\}$ mit:

$$\begin{aligned} \langle 1 \rangle &= \{1\} \\ \langle e^{j2\pi/6} \rangle \;=\; \langle e^{j2\pi 5/6} \rangle &= \mathcal{G} \\ \langle e^{j2\pi 2/6} \rangle \;=\; \langle e^{j2\pi 4/6} \rangle &= \{1, e^{j2\pi 2/6}, e^{j2\pi 4/6}\} \\ \langle e^{j2\pi 3/6} \rangle &= \{1, e^{j2\pi 3/6}\}. \end{aligned}$$

Natürlich kann eine Gruppe der Ordnung 6 nur Untergruppen der Ordnungen 1, 2, 3, 6 haben. ■

A.6.3 Rings

Definition A.3 (Ring). *A* ring $(\mathcal{R}, +, \cdot)$ *is a set* $\mathcal{R}$ *together with two binary operations* $+$ *and* $\cdot$ *on* $\mathcal{R}$ *such that the following three properties are satisfied:*

1. $(\mathcal{R}, +)$ *is a commutative group.*
2. $(\mathcal{R}\backslash\{0\}, \cdot)$ *is closed and the associative law is satisfied, that is,* $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ *for all* $a, b, c \in \mathcal{R}$.
3. *The* distributive law *holds, that is,* $a(b + c) = ab + ac$ *for all* $a, b, c \in \mathcal{R}$.

The ring is called ring with identity *if there exists a neutral element with respect to the multiplication. The neutral elements for addition and multiplication are called* zero element *and* identity element *(or simply* identity*), respectively. The ring is said to be* commutative *if the multiplication is commutative.*

The ring is called integral domain *if it is a commutative ring with identity in which* $ab = 0$ *implies* $a = 0$ *oder* $b = 0$. *In contrast, elements* $a \neq 0$ *and* $b \neq 0$ *with* $ab = 0$ *are called* zero divisors. *Nebenbei bemerkt wird gelegentlich bei der Definition eines integral domains die Existenz der identity nicht gefordert.*

In einem integral domain darf gekürzt werden, that is,

$$au = bu, \quad u \neq 0 \quad \Longrightarrow \quad a = b. \tag{A.6.12}$$

Example A.4. (1) The set of integers $\mathbb{Z}$ forms an integral domain. The set of even integers, often denoted as $2\mathbb{Z}$, forms a commutative ring without identity.

(2) Die Menge der quadratischen Matrizen mit Koeffizienten aus $\mathbb{Q}$ oder $\mathbb{R}$ oder $\mathbb{C}$ bildet einen ring with identity (given by the identity matrix). The example

$$\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} = \begin{pmatrix} 2 & -2 \\ 2 & -2 \end{pmatrix},$$
$$\begin{pmatrix} 1 & -1 \\ 1 & -1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

shows a violation of the commutative law and the existence of zero divisors. So, this ring is not an integral domain.

(3) Die Menge $\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$ mit arithmetic operations modulo p bildet einen commutative ring with mit identity, aber nur dann einen integral domain, wenn p eine Primzahl ist. Denn wenn $p = sr$ non-prime ist, erweisen sich r and s sofort als zero divisors wegen $p = sr = 0 \mod p$. ■

Definition A.4 (Isomorphic Rings). *Zwei Ringe $(\mathcal{R}, +, \cdot)$ und $(\mathcal{R}', +, \cdot)$ of equal cardinality werden als* isomorphic *bezeichnet, wenn eine bijective mapping (also called one-to-one mapping) $\varphi : \mathcal{R} \to \mathcal{R}'$ mit*

$$\varphi(a + b) = \varphi(a) + \varphi(b) \quad \textit{and} \quad \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

existiert. The mapping φ is called isomorphism *and it preserves both operations $+$ and $\cdot$. In other words, die Elemente von $\mathcal{R}'$ ergeben sich durch Umbenennung aus den Elementen von $\mathcal{R}$. Formal wird dafür $\mathcal{R} \cong \mathcal{R}'$ geschrieben.*

If $|\mathcal{R}| \leq |\mathcal{R}'|$ and φ is a injective mapping (also addressed as mapping from $\mathcal{R}$ into $\mathcal{R}'$) then φ is called homomorphism.

A.6.4 Ideals

Definition A.5 (Ideal). *A subset $\mathcal{I}$ of a commutative ring $\mathcal{R}$ is called an* ideal *if the following two axioms are satisfied:*

1. *$\mathcal{I}$ is a ring.*

2. *For all $a \in \mathcal{I}$ and all $b \in \mathcal{R}$: $ab \in \mathcal{I}$.*

In other words, the ideal is a subring of $\mathcal{R}$ and the ideal is closed against multiplications with ring elements. Falls $\mathcal{I}$ das identity element enthält, so gilt natürlich $\mathcal{I} = \mathcal{R}$.

The ideal $\mathcal{I}$ is called principal ideal*, if it is generated by a single element, that is, if there is an $a \in \mathcal{R}$ such that $\mathcal{I} = \langle a \rangle = \{ab \,|\, b \in \mathcal{R}\}$.*

The ring $\mathcal{R}$ is said to be principal ideal domain *if each ideal is a principal ideal.*

Example A.5. (1) Let $n \in \mathbb{Z}$. The set $\mathcal{I} = \langle n \rangle = \{\ldots, -2n, -n, 0, n, 2n, \ldots\}$ is a principal ideal in $\mathbb{Z}$. he same set $\mathcal{I}$ is a subring of $\mathbb{Q}$ but not an ideal in $\mathbb{Q}$, since $n \cdot \frac{1}{2} \notin \mathcal{I}$. Oftmals wird auch die Kurzschreibweise $\langle n \rangle = n\mathbb{Z}$ verwendet.

(2) The set of integers $\mathbb{Z}$ is an principal ideal ring, since each ideal containing n muß zwangsläufig von der Form $\langle n \rangle$ sein und therefore each ideal is principal.

(3) The set of rational numbers $\mathbb{Q}$ contains only two ideals, nämlich $\langle 0 \rangle = \{0\}$ und $\langle 1 \rangle = \mathbb{Q}$ selber. Folglich ist damit auch $\mathbb{Q}$ ein principal ideal ring. Das gleiche gilt für $\mathbb{R}$ und $\mathbb{C}$. ■

Noch interessantere Beispiele for ideals, die auf polynomials basieren, werden in Section A.10 betrachtet.

Definition A.6 (Residue Classes). *Since the ideal $\mathcal{I}$ is also a subgroup of $\mathcal{R}$ with respect to the addition, there exists automatically a partition of $\mathcal{R}$ into equivalence classes or cosets of the form $[r] = r + \mathcal{I} = \{r + a \,|\, a \in \mathcal{I}\}$ according to (A.6.7) with $r \in \mathcal{R}$, wobei in diesem Fall für $[r]$ der term* residue classes *modulo $\mathcal{I}$ verwendet wird.*

Two elements r and r' are called congruent*, denoted by $r \equiv r' \mod \mathcal{I}$, if they are in the same residue class, or equivalently, if $r - r' \in \mathcal{I}$.*

As for (A.6.3) and (A.6.4), we introduce well-defined operations between the residue classes

$$[r] + [s] = [r + s], \qquad [r] \cdot [s] = [r \cdot s]. \tag{A.6.13}$$

The set of residue classes forms a ring that is called residue class ring *or* factor ring *of $\mathcal{R}$ modulo $\mathcal{I}$ and is denoted by*

$$\mathcal{R}\Big/_{\mathcal{I}} \;=\; \{\,[r] \mid r \in \mathcal{R}\}. \tag{A.6.14}$$

Example A.6. Im integer domain $\mathcal{R} = \mathbb{Z}$ erzeugt eine beliebige Zahl $p \in \mathcal{R}$ mit $p \geq 1$ das principal ideal

$$\mathcal{I} \;=\; \langle p \rangle \;=\; \{\ldots, -2p, -p, 0, +p, +2p, \ldots\}. \tag{A.6.15}$$

Die residue classes (or equivalence classes or cosets) sind wie bei Beispiel A.1 von der Form

$$[r] \;=\; r + \langle p \rangle \;=\; \{\ldots, r - 2p, r - p, r, r + p, r + 2p, \ldots\}. \tag{A.6.16}$$

Folglich besteht $[r]$ aus allen ganzen Zahlen, die bei Division durch p den Rest r haben. Also gilt $a \in [r]$, wenn $r - a$ ein Vielfaches von p ist bzw. wenn $a \bmod p$ gleich r ist. Weiter gilt $[r + p] = [r]$. Der factor ring von $\mathbb{Z}$ nach $\langle p \rangle$ besteht aus den residue classes

$$\mathbb{Z}\Big/\langle p\rangle \;=\; \{\,[r]\,|\,r \in \mathbb{Z}\} \;=\; \{[0],[1],\ldots,[p-1]\} \tag{A.6.17}$$

und das standard array $\mathbb{Z}$ lautet wie bei Beispiel A.1

$$\mathbb{Z} \;=\; [0] \cup [1] \cup \ldots \cup [p-1]. \tag{A.6.18}$$

Das Rechnen modulo p entspricht also dem Rechnen im factor ring, also sind formal der ring $\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$ mit addition and multiplication modulo p und der factor ring von $\mathbb{Z}$ nach $\langle p \rangle$ isomorph zueinander:

$$\mathbb{Z}_p \;\cong\; \mathbb{Z}\Big/\langle p\rangle. \tag{A.6.19}$$

Gemäß Definition A.4 wird dabei $\varphi : \mathbb{Z}_p \to \mathbb{Z}\Big/\langle p\rangle$ mit $\varphi(r) = [r]$ gesetzt. Speziell für $p = 0$ gilt $\langle 0 \rangle = \{0\}$ sowie $[r] = \{r\}$ und für $p = 1$ gilt $\langle 1 \rangle = \mathbb{Z}$ sowie $[r] = [0] = \mathbb{Z}$, d.h.:

$$\mathbb{Z}\Big/\langle 0\rangle \cong \mathbb{Z} \quad , \quad \mathbb{Z}\Big/\mathbb{Z} \cong \{0\}. \tag{A.6.20}$$

Für $p = 1$ besteht der factor ring also nur aus einem Element, und in diesem Fall sind das zero element und das identity element kurioserweise identisch. ■

A.6.5 Fields

Definition A.7 (Field). *Als* field $(\mathbb{K}, +, \cdot)$ *wird ein integral domain bezeichnet, in dem die multiplikativen Inversen existieren. Zusammenfassend müssen also die folgenden properties erfüllt sein:*

1. $(\mathbb{K}, +)$ *is a commutative group.*
2. $(\mathbb{K} \setminus \{0\}, \cdot)$ *is a commutative group, die auch als* multiplicative group *of the field bezeichnet wird.*
3. *The* distributive law *holds, that is,* $a(b + c) = ab + ac$ *for all* $a, b, c \in \mathbb{K}$.

A finite field with q elements is usually addressed as Galois field $\mathbb{F}_q$.

Example A.7. (1) Sowohl die rationalen Zahlen $\mathbb{Q}$ wie die reellen Zahlen $\mathbb{R}$ wie auch die komplexen Zahlen $\mathbb{C}$ bilden jeweils einen Körper.

(2) Die Menge aller quadratischen (n,n)-dimensional non-singular Matrizen mit Koeffizienten aus einem Körper bildet offensichtlich keinen Körper, da sie additiv nicht abgeschlossen ist und auch das zero element nicht enthält.

(3) The set $\mathbb{Z}_p$ with addition and multiplication modulo p is a field, if and only if p is prime (das wurde schon in Example A.2(3) gezeigt). ■

Alle endlichen Körper gleicher Mächtigkeit sind isomorph zueinander, also kann man nur von *dem* endlichen Körper der Mächtigkeit q oder von *dem* Galois field $\mathbb{F}_q$ sprechen. Wenn $q = p$ eine Primzahl ist, so folgt also

$$\mathbb{F}_p = \mathbb{Z}_p. \tag{A.6.21}$$

Insbesondere gilt also $1 + 1 + \cdots + 1 = 0$ für die p-fache Addition in $\mathbb{F}_p$ bzw. $1 + 1 = 0$ und $-1 = 1$ in $\mathbb{F}_2$.

Nicht bewiesen wird hier, daß Galois fields nur für $q = p^m$ existieren, wobei p eine Primzahl und m eine natürliche Zahl ist. Um so wichtiger für die Codierungstheorie ist aber die Konstruktion von $\mathbb{F}_{p^m}$ aus $\mathbb{F}_p$, die in Abschnitt A.8 und detailliert in Kapitel 6 erfolgt.

Über ideals in a field gewinnt man sofort einen vollständigen Überblick. Denn in einem finite or infinite field $\mathbb{K}$ sind $\{0\}$ und $\mathbb{K}$ die einzigen Ideale, wie wir schnell einsehen können. Denn wenn $\mathcal{I}$ ein Ideal mit $0 \neq a \in \mathcal{I}$ ist, so gilt mit $r = a^{-1} \in \mathbb{K}$ natürlich $1 = ar \in \mathcal{I}$ und somit $r = 1 \cdot r \in \mathcal{I}$ für alle $r \in \mathbb{K}$. Diese beiden Ideale sind wegen $\{0\} = \langle 0 \rangle$ und $\mathbb{K} = \langle 1 \rangle$ zugleich principal ideals. Ein field ist also formal auch ein principal ideal domain.

A.7 Vector Spaces

Definition A.8 (Vector Space). *Ein* Vektorraum *oder* linearer Raum V *über einem Körper* $\mathbb{K}$ *ist eine Menge von Vektoren, für die eine Addition und eine Skalarmultiplikation erklärt sind. Für* $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in V$ *und* $\alpha \in \mathbb{K}$ *sollen* $\boldsymbol{a} + \boldsymbol{b} \in V$ *und* $\alpha \cdot \boldsymbol{a} \in V$ *erfüllt sein sowie folgende Gesetze gelten:*

1. $\boldsymbol{a} + \boldsymbol{b} = \boldsymbol{b} + \boldsymbol{a}$
2. $(\boldsymbol{a} + \boldsymbol{b}) + \boldsymbol{c} = \boldsymbol{a} + (\boldsymbol{b} + \boldsymbol{c})$
3. $\boldsymbol{a} + \boldsymbol{0} = \boldsymbol{a} \quad mit \quad \boldsymbol{0} = (0, \ldots, 0)$
4. $\boldsymbol{a} + (-\boldsymbol{a}) = \boldsymbol{0} \quad mit \quad -(a_0, \ldots, a_{n-1}) = (-a_0, \ldots, -a_{n-1})$
5. $\alpha(\boldsymbol{a} + \boldsymbol{b}) = \alpha\boldsymbol{a} + \alpha\boldsymbol{b}$
6. $(\alpha + \beta)\boldsymbol{a} = \alpha\boldsymbol{a} + \beta\boldsymbol{a}$
7. $(\alpha\beta)\boldsymbol{a} = \alpha(\beta\boldsymbol{a})$

8. $1\boldsymbol{a} = \boldsymbol{a}$.

Insbesondere ist V bezüglich der Vektoraddition eine kommutative Gruppe. Das Zeichen $+$ steht sowohl für die Addition von Skalaren in $\mathbb{K}$ wie für die Addition von Vektoren in V. Entsprechend steht $\cdot$ sowohl für die Multiplikation von Skalaren wie für die Multiplikation von Skalaren mit Vektoren. Eine Multiplikation von Vektoren wird nicht erklärt.

Es seien $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ beliebige Vektoren mit Koeffizienten aus $\mathbb{K}$. Der hiervon *erzeugte* oder *aufgespannte* Vektorraum V ist als der kleinste Vektorraum über $\mathbb{K}$ definiert, der diese l Vektoren enthält. Er besteht offensichtlich genau aus den *Linearkombinationen* der erzeugenden Vektoren:

$$V = \left\{ \sum_{i=1}^{l} \alpha_i \boldsymbol{a}_i \,\middle|\, \alpha_1, \ldots, \alpha_l \in \mathbb{K} \right\}. \tag{A.7.1}$$

Die Vektoren $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ aus einem beliebigen Vektorraum heißen *linear unabhängig*, wenn gilt:

$$\sum_{i=1}^{l} \alpha_i \boldsymbol{a}_i = \boldsymbol{0} \quad \Longrightarrow \quad \alpha_1 = \ldots = \alpha_l = 0. \tag{A.7.2}$$

Wenn es umgekehrt eine Kombination von Skalaren gibt, die nicht alle Null sind, so daß die Linearkombination den Nullvektor ergibt, dann sind die $\boldsymbol{a}_1, \ldots, \boldsymbol{a}_l$ *linear abhängig*. Wenn speziell $\boldsymbol{b}$ eine Linearkombination der $\boldsymbol{a}_i$ ist, dann ist $\boldsymbol{b}$ von den $\boldsymbol{a}_i$ linear abhängig bzw. $\boldsymbol{b}$ und die $\boldsymbol{a}_i$ sind zusammen linear abhängig.

Die maximale Anzahl der linear unabhängigen Vektoren heißt *Dimension* des Vektorraums und wird als $\dim(V)$ geschrieben. Jede Auswahl von $\dim(V)$ linear unabhängigen Vektoren bildet eine *Basis* für den Vektorraum. Die Mächtigkeit jeder Basis beträgt also $\dim(V)$.

Eine äquivalente Kennzeichnung einer Basis ist, daß sie aus linear unabhängigen Vektoren besteht, die den gesamten Vektorraum aufspannen. Eine weitere äquivalente Kennzeichnung ist, daß jeder Vektor aus dem Vektorraum auf genau eine Weise als Linearkombination der Vektoren aus der Basis dargestellt werden kann.

Example A.8. (1) Zu jedem Körper $\mathbb{K}$ und jeder natürlichen Zahl n gehört ein Vektorraum $\mathbb{K}^n$, der aus allen Vektoren der Länge n mit Koeffizienten aus $\mathbb{K}$ besteht. Dabei werden die Verknüpfungen komponentenweise erklärt:

$$\begin{aligned} \boldsymbol{a} + \boldsymbol{b} &= (a_0, \ldots, a_{n-1}) + (b_0, \ldots, b_{n-1}) = (a_0 + b_0, \ldots, a_{n-1} + b_{n-1}) \\ \alpha \cdot \boldsymbol{a} &= \alpha \cdot (a_0, \ldots, a_{n-1}) = (\alpha a_0, \ldots, \alpha a_{n-1}). \end{aligned}$$

Klar ist $\dim(\mathbb{K}^n) = n$ und die *kanonische Basis* für $\mathbb{K}^n$ wird von den n *Einheitsvektoren*

$$(1, 0, 0, \ldots, 0), \quad (0, 1, 0, \ldots, 0), \quad \ldots, \quad (0, 0, 0, \ldots, 1) \tag{A.7.3}$$

gebildet. Durch $(1,0,0,\ldots,0)$, $(1,1,0,\ldots,0)$, $\ldots$, $(1,1,1,\ldots,1)$ wird ein Example einer weiteren Basis gegeben.

(2) $\mathbb{R}^n$ ist ein Vektorraum über $\mathbb{R}$, aber nicht über $\mathbb{C}$; $\mathbb{C}^n$ ist Vektorraum sowohl über $\mathbb{R}$ wie über $\mathbb{C}$.

(3) Die Menge aller (k,n)-dim. Matrizen mit Koeffizienten aus $\mathbb{K}$ ist ein Vektorraum über $\mathbb{K}$, wobei die Matrixmultiplikation allerdings überhaupt nicht eingeht. ■

Es sei V ein Vektorraum über $\mathbb{K}$ und $U \subseteq V$. Dann ist U ebenfalls ein Vektorraum über $\mathbb{K}$ genau dann, wenn für alle $\boldsymbol{a}, \boldsymbol{b} \in U$ und $\alpha \in \mathbb{K}$ stets $\boldsymbol{a} + \boldsymbol{b} \in U$ und $\alpha \boldsymbol{a} \in U$ gilt.

Proof. U ist nach diesen Forderungen abgeschlossen und alle in V gültigen Regeln sind erst recht in der Teilmenge U gültig. Für $\boldsymbol{a} \in U$ folgt $-\boldsymbol{a} = (-1) \cdot \boldsymbol{a} \in U$ und somit $\boldsymbol{0} = \boldsymbol{a} + (-\boldsymbol{a}) \in U$. Also existieren in U die inversen Elemente und das neutrale Element. ■

In Abschnitt 3.1 wird ein $(n,k)_q$-block code $\mathcal{C} \subset \mathbb{F}_q^n$ als linear dadurch definiert, daß $\mathcal{C}$ ein Untervektorraum von $\mathbb{F}_q^n$ (mit der Dimension k) ist. Eine Basis wird durch die Zeilen der generator matrix gegeben.

A.8 Polynomials

Die Menge aller Polynome beliebigen Grades in der Unbestimmten x mit Koeffizienten aus einem Ring $\mathcal{R}$ wird mit $\mathcal{R}[x]$ bezeichnet und bildet einen Ring mit der üblichen Addition und Multiplikation von Polynomen.

Entsprechend wird die Menge aller Polynome beliebigen Grades mit Koeffizienten aus einem Körper $\mathbb{K}$ bzw. einem Galois field $\mathbb{F}_q$ mit $\mathbb{K}[x]$ bzw. $\mathbb{F}_q[x]$ bezeichnet. Die Polynome bilden einen Integritätsbereich, aber keinen Körper, da multiplikative inverse Elemente zu Polynomen als Polynome natürlich nicht existieren (siehe jedoch Theorem A.9).

$\mathbb{K}[x]$ ist ein Vektorraum über $\mathbb{K}$ mit unendlicher Dimension. Es sei $\mathbb{K}[x]_{n-1}$ die Menge aller Polynome vom Grad $\leq n-1$. Dann ist $\mathbb{K}[x]_{n-1}$ ein Untervektorraum von $\mathbb{K}[x]$ mit der Dimension n und der Basis $1, x, x^2, \ldots, x^{n-1}$. Bei einem linearen $(n,k)_q$-block code kann $\mathcal{C}$ als Untervektorraum von $\mathbb{K}[x]_{n-1}$ aufgefaßt werden, indem die Vektoren der Länge n mit einem Polynom vom Grad $\leq n-1$ identifiziert werden.

Ein Polynom, bei dem der höchste Koeffizient ungleich Null den Wert 1 hat, wird als *normiertes Polynom* bezeichnet. Allgemein gilt die *Gradformel*:

$$\deg\Big(a(x)b(x)\Big) = \deg\, a(x) + \deg\, b(x). \tag{A.8.1}$$

Dabei wird festgelegt: Skalare ungleich Null haben den Grad 0 und die Null hat den Grad $-\infty$.

Ein Polynom aus $\mathbb{K}[x]$ wird als *irreduzibel* (unzerlegbar) bezeichnet, wenn es nicht als Produkt von zwei Polynomen aus $\mathbb{K}[x]$ darstellbar ist, die jeweils

mindestens vom Grad 1 sind. Jedes Polynom vom Grad 1 ist also irreduzibel. Wichtig ist daß sich der Begriff irreduzibel immer auf einen bestimmten Körper bezieht.

Example A.9. Das Polynom $x^2 - 2$ ist irreduzibel über $\mathbb{Q}$, aber wegen der Darstellung $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$ reduzibel über $\mathbb{R}$.

Das Polynom x^2+1 ist irreduzibel über $\mathbb{R}$, aber wegen $x^2+1 = (x-j)(x+j)$ reduzibel über $\mathbb{C}$ und wegen $x^2+1 = x^2+2x+1 = (x+1)^2$ auch reduzibel über dem Galois field $\mathbb{F}_2$. ■

Jedes beliebige Polynom $f(x) \in \mathbb{K}[x]$ kann in ein Produkt

$$f(x) = f_1(x) \cdots f_l(x) \tag{A.8.2}$$

von irreduziblen Polynomen $f_i(x) \in \mathbb{K}[x]$ zerlegt werden. Bis auf skalare Faktoren und die Reihenfolge ist diese Zerlegung eindeutig.

Zu einem Polynom $g(x) = g_0 + g_1 x + \cdots + g_{m-1}x^{m-1} + g_m x^m$ wird das *reziproke Polynom* als

$$\bar{g}(x) = g_m + g_{m-1}x + \cdots + g_1 x^{m-1} + g_0 x^m = x^m g(x^{-1}) \tag{A.8.3}$$

definiert. Mit $g(x)$ ist auch $\bar{g}(x)$ irreduzibel. Mit $g(a) = 0$ bei $a \neq 0$ gilt auch $\bar{g}(a^{-1}) = 0$.

Theorem A.4 (Division algorithm (or theorem) **for polynomials).** *For every pair of polynomials $b(x)$ and $g(x) \neq 0$ from $\mathbb{K}[x]$, there is a unique pair of polynomials $\alpha(x)$ and $r(x)$ from $\mathbb{K}[x]$ such that*

$$b(x) = \alpha(x)g(x) + r(x) \quad \textit{mit} \quad \deg\, r(x) < \deg\, g(x). \tag{A.8.4}$$

The polynomials in equation (A.8.4) are named as follows

$$\textit{dividend} = \textit{quotient} \cdot \textit{divisor} + \textit{remainder}.$$

Für den remainder (also called residue) $r(x)$ of $b(x)$ when divided by $g(x)$ werden die beiden folgenden compact notations verwendet

$$r(x) = R_{g(x)}[b(x)] \quad , \quad r(x) = b(x) \bmod g(x). \tag{A.8.5}$$

The right-hand side notation is also called a congruence *and is read as "$r(x)$ is congruent to $b(x)$ modulo $g(x)$. Again we emphasize the relation* $\deg\, R_{g(x)}[b(x)] < \deg\, g(x)$ *for the degrees. Computing modulo $g(x)$ means that $g(x)$ can be replaced by zero.*

The division algorithm and the following theorem were already cited in Subsection 6.1.2. Usually, the polynomial $\alpha(x)$ is of minor importance and we will

be more interested in the remainder polynomial $r(x)$. Hint: die eckigen Klammern of the modulo computation (allgemeiner Äquivalenzklassen ????????) sind nicht zu verwechseln mit der Bildung der conjugacy classes in ??????

Proof of the division algorithm. The quotient polynomial $\alpha(x)$ and remainder polynomial $r(x)$ can be found by *elementary long division* as demonstrated with the following example. Both polynomials are unique because if

$$b(x) = \alpha_1(x)g(x) + r_1(x) = \alpha_2(x)g(x) + r_2(x),$$

then $r_2(x) - r_1(x) = (\alpha_1(x) - \alpha_2(x))g(x)$. Since the degree of $r_2(x) - r_1(x)$ is smaller than the degree of $g(x)$, hence, both sides are zero. Thus, $\alpha_1(x) = \alpha_2(x)$ and $r_1(x) = r_2(x)$, so the representation is unique. ■

Example A.10. Divisionsverfahren in $\mathbb{F}_2[x]$ mit $b(x) = x^7$, $g(x) = x^3 + x + 1$:

$$\begin{array}{rcl}
x^7 & : & (x^3+x+1) \quad = \quad x^4+x^2+x+1 \quad = \quad \alpha(x) \\
\underline{x^7 + x^5 + x^4} & & \\
x^5 + x^4 & & \\
\underline{x^5 + x^3 + x^2} & & \\
x^4 + x^3 + x^2 & & \\
\underline{x^4 + x^2 + x} & & \\
x^3 + x & & \\
\underline{x^3 + x + 1} & & \\
1 & = & r(x).
\end{array}$$

Also gilt $x^7 = \alpha(x)(x^3+x+1)+1$ bzw. $x^7+1 = \alpha(x)g(x)$ sowie $R_{x^3+x+1}[x^7] = 1$. Rechnen modulo x^3+x+1 bedeutet, daß $x^3+x+1 = 0$ bzw. $x^3 = x+1$ gesetzt werden kann:

$$\begin{aligned}
x^7 &= x^3x^3x = (x+1)(x+1)x = (x^2+2x+1)x \\
&= x^3+x = (x+1)+x = 1 \mod g(x).
\end{aligned}$$

Damit ergibt sich $r(x)$ schneller als beim Divisionsverfahren – allerdings ohne das Polynom $\alpha(x)$. ■

Theorem A.5 (Restklassen-Arithmetik). *Für die Restklassen-Arithmetik gelten folgende Regeln in* $\mathbb{K}[x]$*:*

$$R_{g(x)}[a(x) + b(x)] = R_{g(x)}[a(x)] + R_{g(x)}[b(x)] \tag{A.8.6}$$

$$R_{g(x)}[a(x) \cdot b(x)] = R_{g(x)}\Big[R_{g(x)}[a(x)] \cdot R_{g(x)}[b(x)]\Big] \tag{A.8.7}$$

$$R_{g(x)}[a(x)g(x)] = 0 \tag{A.8.8}$$

$$R_{g(x)}[a(x)] = R_{g(x)}\Big[R_{g(x)h(x)}[a(x)]\Big] \tag{A.8.9}$$

$$\deg\, a(x) < \deg\, g(x) \quad \Longrightarrow \quad R_{g(x)}[a(x)] = a(x) \tag{A.8.10}$$

$$R_{x^n-1}[x^m] = x^{m \bmod n} = x^{R_n[m]}. \tag{A.8.11}$$

Beim Rechnen modulo $(x^n - 1)$ *wird* x^n *durch 1 ersetzt bzw. die Potenz* m *durch* $m \bmod n$. *Die Potenzrechnung erfolgt dabei in* $\mathbb{Z}$ *unabhängig von* $\mathbb{K}$.

Beweis von (A.6.9): Sei $s(x) = R_{g(x)h(x)}[a(x)]$, d.h. mit einem passenden $\alpha(x)$ gilt $s(x) = a(x) - \alpha(x)g(x)h(x)$. Dann folgt:

$$\begin{aligned} R_{g(x)}[s(x)] &= R_{g(x)}[a(x) - \alpha(x)g(x)h(x)] \\ &= R_{g(x)}[a(x)] - R_{g(x)}[g(x) \cdot \alpha(x)h(x)] \\ &= R_{g(x)}[a(x)]. \end{aligned}$$

Alle anderen Regeln sind offensichtlich. ■

Example A.11. Zur Anwendung von Theorem A.5 in $\mathbb{F}_2[x]$ mit $g(x) = x^3 + x + 1$: Nach Example A.9 ist $g(x)$ ein Teiler von $x^7 + 1$, d.h. es existiert ein $h(x)$ mit $g(x)h(x) = x^7 + 1$. Gesucht ist $R_{g(x)}[x^{25}]$. Direkt wäre das eine längere Rechnung, die jedoch mit

$$\begin{aligned} R_{g(x)}[x^{25}] &= R_{g(x)}[R_{g(x)\alpha(x)}[x^{25}]] \\ &= R_{g(x)}[R_{x^7-1}[x^{25}]] \\ &= R_{g(x)}[x^{R_7[25]}] \\ &= R_{g(x)}[x^4] \\ &= R_{g(x)}[x \cdot R_{g(x)}[x^3]] \\ &= R_{g(x)}[x(x+1)] \\ &= x^2 + x \end{aligned}$$

erheblich vereinfacht wird. ■

Theorem A.6. *Für Polynome aus* $\mathbb{K}[x]$ *gelten folgende Eigenschaften:*

(1) Ein Polynom vom Grad m *hat höchstens* m *Nullstellen.*

(2) Wenn ein Polynom $f(x)$ *eine Nullstelle* a *hat, so ist* $x - a$ *ein Teiler von* $f(x)$, *d.h. der* Linearfaktor $x - a$ *wird abgespalten:*

$$f(x) = (x - a) \cdot f_1(x) \quad \textit{mit passendem } f_1(x). \tag{A.8.12}$$

Im Fall $f(x) = (x - a)^l f_1(x)$ *mit* $f_1(a) \neq 0$ *ist* a *eine* l*-fache Nullstelle, die auch* l*-fach gezählt wird.*

(3) Wenn ein normiertes Polynom $f(x)$ *vom Grad* m *die maximal* m *Nullstellen* $a_1, \ldots, a_m$ *hat, so zerfällt* $f(x)$ *vollständig in Linearfaktoren:*

$$f(x) = \prod_{i=1}^{m} (x - a_i). \tag{A.8.13}$$

Proof. Zu zeigen ist nur (2), da (1) und (3) daraus unmittelbar folgen. Nach dem Divisionstheorem existieren zu $f(x)$ und $x-a$ Polynome $f_1(x)$ und $r(x)$ mit

$$f(x) = f_1(x)(x-a) + r(x) \quad \text{mit} \quad \deg r(x) < \deg (x-a) = 1.$$

Somit muß $r(x) = r_0$ konstant sein. Für $x = a$ folgt $0 = f(a) = r(a) = r_0$. ■

Example A.12. Sei $\mathbb{K} = \mathbb{F}_2$:

(1) Ein Linearfaktor $x+1$ wird genau dann abgespalten, wenn 1 eine Nullstelle des Polynoms ist bzw. wenn die Anzahl der Koeffizienten des Polynoms eine gerade Zahl ist.

(2) Das einzige irreduzible Polynom vom Grad 2 ist $1 + x + x^2$.

(3) Die einzigen irreduziblen Polynome vom Grad 3 sind $1 + x + x^3$ und das reziproke Polynom $1 + x^2 + x^3$.

(4) Ein Polynom vom Grad 4 oder 5 ist irreduzibel, wenn 1 keine Nullstelle ist und wenn $1 + x + x^2$ kein Teiler ist, denn als reduzibles Polynom müßte es einen Linearfaktor abspalten oder einen (irreduziblen!) Teiler vom Grad 2 besitzen. ■

A.9 The Extended Version of the Euclidean Algorithm for Polynomials

Der Euclidean Algorithm (EA) bildet die Grundlage vieler Eigenschaften von Galois fieldsn sowie verschiedener Decodierverfahren. Der EA gilt zwar allgemein für Ringe wie beispielsweise $\mathbb{Z}$, aber er wird hier vorrangig für Polynome benötigt und zudem lassen sich einige Eigenschaften des EA nur mit Polynomen formulieren.

Der *größte gemeinsame Teiler* (GCD) von zwei Polynomen ist mit der Festlegung als normiertes Polynom eindeutig bestimmt. Zur Vorbereitung des EA wird folgender Theorem notiert:

Theorem A.7. *Für beliebige Polynome $a(x)$, $b(x)$ und $v(x)$ aus $\mathbb{K}[x]$ gilt für den größten gemeinsamen Teiler:*

$$\begin{aligned} \mathrm{GCD}\Big(a(x)\ ,\ b(x)\Big) &= \mathrm{GCD}\Big(a(x)\ ,\ b(x) - v(x)a(x)\Big) \\ &= \mathrm{GCD}\Big(a(x)\ ,\ R_{a(x)}[b(x)]\Big). \end{aligned}$$

Proof. Zu zeigen ist nur die erste Aussage. Wenn $d(x)$ ein Teiler von $a(x)$ und $b(x)$ ist, dann ist $d(x)$ auch ein Teiler von $a(x)$ und $b(x) - v(x)a(x)$. Wenn umgekehrt $d(x)$ ein Teiler von $a(x)$ und $b(x) - v(x)a(x)$ ist, dann ist $d(x)$ auch ein Teiler von $a(x)$ und $v(x)a(x) + (b(x) - v(x)a(x)) = b(x)$. Insgesamt ist also die Menge der gemeinsamen Teiler von $a(x)$ und $b(x)$ gleich der Menge der

gemeinsamen Teiler von $a(x)$ und $b(x) - v(x)a(x)$. Folglich ist auch der größte gemeinsame Teiler gleich. ■

Theorem A.8 (Euclidean Algorithm (EA)). *Es seien $a(x)$ und $b(x)$ zwei Polynome mit Koeffizienten aus einem beliebigen Körper $\mathbb{K}$ mit der Eigenschaft* $\deg a(x) \geq \deg b(x)$. *Setze*

$$\begin{array}{lll} r_{-2}(x) = a(x) & s_{-2}(x) = 1 & t_{-2}(x) = 0 \\ r_{-1}(x) = b(x) & s_{-1}(x) = 0 & t_{-1}(x) = 1. \end{array} \tag{A.9.1}$$

Für $i = 0, 1, \ldots, l+1$ existieren nach dem Divisionstheorem aus Theorem A.4 jeweils Polynome $\alpha_i(x)$ und $r_i(x)$ aus $\mathbb{K}[x]$ mit

$$r_{i-2}(x) \;=\; \alpha_i(x) r_{i-1}(x) + r_i(x) \quad \textit{mit} \quad \deg\, r_i(x) < \deg\, r_{i-1}(x), \tag{A.9.2}$$

$$\textit{d.h.} \quad r_i(x) \;=\; R_{r_{i-1}(x)}[r_{i-2}(x)] \;=\; r_{i-2}(x) \bmod r_{i-1}(x).$$

Wegen der abnehmenden Grade existiert ein l mit $r_l(x) \neq 0$ und $r_{l+1}(x) = 0$. Insgesamt ergibt sich folgendes Rekursionsschema:

$$\begin{array}{rcl} r_{-2}(x) & = & \alpha_0(x) r_{-1}(x) + r_0(x) \\ r_{-1}(x) & = & \alpha_1(x) r_0(x) + r_1(x) \\ r_0(x) & = & \alpha_2(x) r_1(x) + r_2(x) \\ & \vdots & \\ r_{l-2}(x) & = & \alpha_l(x) r_{l-1}(x) + r_l(x) \\ r_{l-1}(x) & = & \alpha_{l+1}(x) r_l(x). \end{array}$$

Ferner werden begleitende Rekursionen für $i = 0, 1, \ldots, l+1$ betrachtet:

$$\begin{array}{l} s_i(x) = s_{i-2}(x) - \alpha_i(x) s_{i-1}(x) \\ t_i(x) = t_{i-2}(x) - \alpha_i(x) t_{i-1}(x). \end{array} \tag{A.9.3}$$

Diese insgesamt 3 Rekursionen weisen eine Vielzahl von Eigenschaften auf. Zunächst ergibt sich eine (allerdings nicht eindeutige) Lineardarstellung des größten gemeinsamen Teilers:

$$\mathrm{GCD}(a(x), b(x)) \;=\; r_l(x) \;=\; s_l(x) a(x) + t_l(x) b(x), \tag{A.9.4}$$

$$\frac{a(x)}{\mathrm{GCD}(a(x), b(x))} = (-1)^l t_{l+1}(x) \quad , \quad \frac{b(x)}{\mathrm{GCD}(a(x), b(x))} = (-1)^{l+1} s_{l+1}(x). \tag{A.9.5}$$

Im einzelnen gilt für $i = -2, -1, \ldots, l+1$:

$$s_i(x) a(x) + t_i(x) b(x) = r_i(x) \tag{A.9.6}$$

sowie für $i = -1, 0, \ldots, l+1$*:*

$$\begin{aligned} s_i(x)r_{i-1}(x) - s_{i-1}(x)r_i(x) &= (-1)^i b(x) && \text{(A.9.7)}\\ t_i(x)r_{i-1}(x) - t_{i-1}(x)r_i(x) &= (-1)^{i+1} a(x) && \text{(A.9.8)}\\ s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) &= (-1)^i && \text{(A.9.9)}\\ \mathrm{GCD}(s_i(x), t_i(x)) &= 1. && \text{(A.9.10)} \end{aligned}$$

Ferner gelten folgende Grad-Eigenschaften für $i = 0, 1, \ldots, l+1$*:*

$$\begin{aligned} \deg\, \alpha_i(x) &= \deg\, r_{i-2}(x) - \deg\, r_{i-1}(x) \quad (i \le l) && \text{(A.9.11)}\\ &= \deg\, s_i(x) - \deg\, s_{i-1}(x) \quad (i \ge 1) && \text{(A.9.12)}\\ &= \deg\, t_i(x) - \deg\, t_{i-1}(x) && \text{(A.9.13)}\\ \deg\, r_i(x) &= \deg\, a(x) - \sum_{j=0}^{i+1} \deg\, \alpha_j(x) && \text{(A.9.14)}\\ \deg\, s_i(x) &= \sum_{j=1}^{i} \deg\, \alpha_j(x) \;=\; \deg\, b(x) - \deg\, r_{i-1}(x) && \text{(A.9.15)}\\ \deg\, t_i(x) &= \sum_{j=0}^{i} \deg\, \alpha_j(x) \;=\; \deg\, a(x) - \deg\, r_{i-1}(x). && \text{(A.9.16)} \end{aligned}$$

Proof. Die Existenz von l ist klar. Es gilt dann:

$$\begin{aligned} r_l(x) &= \mathrm{GCD}(r_l(x), \alpha_{l+1}(x)r_l(x))\\ &= \mathrm{GCD}(r_l(x), r_{l-1}(x))\\ &= \mathrm{GCD}(r_l(x) - \alpha_l(x)r_{l-1}(x), r_{l-1}(x)) \quad \text{nach Theorem A.7}\\ &= \mathrm{GCD}(r_{l-2}(x), r_{l-1}(x))\\ &\;\;\vdots\\ &= \mathrm{GCD}(r_{-1}(x), r_{-2}(x)) \;=\; \mathrm{GCD}(a(x), b(x)). \end{aligned}$$

Die nicht eindeutige Lineardarstellung macht ein Beispiel in den ganzen Zahlen klar: $\mathrm{GCD}(2,3) = 1 = 2 \cdot 2 - 1 \cdot 3 = -1 \cdot 2 + 1 \cdot 3$. Es wird jetzt (A.7.6) nachgewiesen, woraus dann auch (A.7.4) vollständig folgt. (A.7.6) ist für $i = -2$ und $i = -1$ erfüllt. Induktionsschluß von $i-2$ und $i-1$ auf i für $i \ge 0$:

$$\begin{aligned} &s_i(x)a(x) + t_i(x)b(x)\\ &= (s_{i-2}(x) - \alpha_i(x)s_{i-1}(x))a(x) + (t_{i-2}(x) - \alpha_i(x)t_{i-1}(x))b(x)\\ &= (s_{i-2}(x)a(x) + t_{i-2}(x)b(x)) - \alpha_i(x)(s_{i-1}(x)a(x) + t_{i-1}(x)b(x))\\ &= r_{i-2}(x) - \alpha_i(x)r_{i-1}(x) \qquad \text{nach Induktionsvoraussetzung}\\ &= r_i(x) \quad \text{nach (A.7.2).} \end{aligned}$$

(A.7.7) ist für $i = -1$ erfüllt. Induktionsschluß von $i-1$ auf i für $i \geq 0$:

$$\begin{aligned} & s_i(x)r_{i-1}(x) - s_{i-1}(x)r_i(x) \\ &= (s_{i-2}(x) - \alpha_i(x)s_{i-1}(x))r_{i-1}(x) - s_{i-1}(x)(r_{i-2}(x) - \alpha_i(x)r_{i-1}(x)) \\ &= s_{i-2}(x)r_{i-1}(x) - s_{i-1}(x)r_{i-2}(x) \\ &= -(-1)^{i-1}b(x) \;=\; (-1)^i b(x). \end{aligned}$$

(A.7.8) und (A.7.9) ergeben sich in gleicher Weise. Zum Nachweis von (A.7.10) sei $d(x) = \mathrm{GCD}(s_i(x), t_i(x))$. Also ist $d(x)$ ein Teiler von $s_i(x)$ und $t_i(x)$ und somit auch von $s_i(x)t_{i-1}(x) - s_{i-1}(x)t_i(x) = (-1)^i$. Somit folgt $d(x) = 1$. Aus (A.7.7) und (A.7.8) folgt für $i = l+1$ mit $r_{l+1}(x) = 0$ und $r_l(x) = \mathrm{GCD}(a(x), b(x))$ direkt (A.7.5).

Die Gradformel (A.7.11) folgt direkt aus (A.7.2). Aus (A.7.3) folgt $s_0(x) = 1$ und damit ist $\deg s_{i-1}(x) < \deg s_i(x)$ für $i = 0$ bewiesen. Für $i \geq 1$ folgt diese Relation per Induktionsschluß und somit folgt direkt (A.7.12). Entsprechend ergibt sich (A.7.13). Die Summation über $\deg \alpha_j(x)$ in (A.7.11) bis (A.7.13) ergibt direkt (A.7.14) bis (A.7.16). ■

Der EA kann auch kompakt mit Polynom-Matrizen formuliert werden. Mit

$$\boldsymbol{Q}_i = \begin{pmatrix} -\alpha_i(x) & 1 \\ 1 & 0 \end{pmatrix} \quad \boldsymbol{B}_i = \begin{pmatrix} s_i(x) & s_{i-1}(x) \\ t_i(x) & t_{i-1}(x) \end{pmatrix} \quad \boldsymbol{r}_i = \begin{pmatrix} r_i(x) & r_{i-1}(x) \end{pmatrix}$$

gelten die Rekursionen

$$\begin{array}{rclcl} \boldsymbol{r}_i & = & \boldsymbol{r}_{i-1} \cdot \boldsymbol{Q}_i & = & \boldsymbol{r}_{-1} \cdot \boldsymbol{Q}_0 \cdots \boldsymbol{Q}_i \\ \boldsymbol{B}_i & = & \boldsymbol{B}_{i-1} \cdot \boldsymbol{Q}_i & = & \boldsymbol{B}_{-1} \cdot \boldsymbol{Q}_0 \cdots \boldsymbol{Q}_i. \end{array} \tag{A.9.17}$$

Example A.13. EA in $\mathbb{F}_2[x]$ mit $a(x) = x^4 + x^3 + 1$, $b(x) = x^4 + x^2 + x + 1$:

i	$r_i(x)$	$\alpha_i(x)$	$s_i(x)$	$t_i(x)$
-2	$x^4 + x^3 + 1$		1	0
-1	$x^4 + x^2 + x + 1$		0	1
0	$x^3 + x^2 + x$	1	1	1
1	$x^2 + 1$	$x + 1$	$x + 1$	x
$l = 2$	1	$x + 1$	x^2	$x^2 + x + 1$
3	0	$x^2 + 1$	$x^4 + x^2 + x + 1$	$x^4 + x^3 + 1$

Es gilt also für dieses Example:

$$\mathrm{GCD}(a(x), b(x)) = 1 = \underbrace{(x^2)}_{s_2(x)}\underbrace{(x^4 + x^3 + 1)}_{a(x)} + \underbrace{(x^2 + x + 1)}_{t_2(x)}\underbrace{(x^4 + x^2 + x + 1)}_{b(x)}.$$

■

A.10 Polynom-Restklassenringe

Es sei $\mathcal{R} = \mathbb{K}[x]$ der Integritätsbereich aller Polynome mit Koeffizienten aus dem allgemeinen Körper $\mathbb{K}$ und durch ein normiertes Polynom $p(x) \in \mathbb{K}[x]$ vom Grad $m \geq 1$ werde das Hauptideal

$$\mathcal{I} \;=\; \langle p(x) \rangle \;=\; \{p(x)b(x) \mid b(x) \in \mathcal{R}\} \tag{A.10.1}$$

erzeugt. Die Restklassen sind von der Form

$$\begin{aligned} [r(x)] &= r(x) + \langle p(x) \rangle \\ &= \{r(x) + p(x)b(x) \mid b(x) \in \mathcal{R}\} \\ &= \{a(x) \mid a(x) \in \mathcal{R} \;\wedge\; R_{p(x)}[a(x)] = R_{p(x)}[r(x)]\}. \end{aligned} \tag{A.10.2}$$

Insbesondere gilt $[r(x)] = [R_{p(x)}[r(x)]]$, d.h. der Restklassen-Repräsentant kann modulo $p(x)$ betrachtet werden. Für den Restklassenring gilt

$$\begin{aligned} \mathcal{R}\Big/\mathcal{I} &= \mathbb{K}[x]\Big/\langle p(x) \rangle \\ &= \{[r(x)] \mid r(x) \in \mathcal{R}\} \\ &= \{[r(x)] \mid r(x) \in \mathcal{R} \;\wedge\; \deg\, r(x) < m\} && \text{(A.10.3)} \\ &\cong \{\; r(x) \;\mid r(x) \in \mathcal{R} \;\wedge\; \deg\, r(x) < m\}, && \text{(A.10.4)} \end{aligned}$$

denn wenn $[r_1(x)] = [r_2(x)]$ für zwei Polynome vom Grad $< m$ gilt, so folgt $r_1(x) - r_2(x) = p(x)b(x)$ mit passendem $b(x) \in \mathcal{R}$. Aus der Gradformel folgt jedoch $r_1(x) - r_2(x) = 0$. Zwei verschiedene Polynome vom Grad $< m$ erzeugen also auch zwei verschiedene Restklassen. Die Restklassen-Zerlegung lautet

$$\mathcal{R} \;=\; \mathbb{K}[x] \;=\; \biguplus_{\substack{r(x) \in \mathcal{R} \\ \deg\; r(x) < m}} [r(x)]. \tag{A.10.5}$$

Speziell für $p(x) = 0$ gilt $\mathcal{I} = \{0\}$ sowie $[r(x)] = \{r(x)\}$ und für $p(x) = 1$ gilt $\mathcal{I} = \mathbb{K}[x]$ sowie $[r(x)] = [0] = \mathbb{K}[x]$ und somit folgt:

$$\mathbb{K}[x]\Big/\langle 0 \rangle \cong \mathbb{K}[x] \quad , \quad \mathbb{K}[x]\Big/\mathbb{K}[x] \cong \{0\}. \tag{A.10.6}$$

Theorem A.9. *Es sei $\mathbb{K}$ ein allgemeiner Körper und $p(x) \in \mathbb{K}[x]$ ein beliebiges Polynom vom Grad ≥ 1. Dann ist der Restklassenring $\mathbb{K}[x]\Big/\langle p(x) \rangle$ genau dann ein Körper, wenn $p(x)$ irreduzibel ist.*

Die Restklassenringe zu zwei verschiedenen irreduziblen Polynomen gleichen Grades sind isomorph (bei endlichem $\mathbb{K}$).

Proof. "⇐": Es sei $p(x)$ vom Grad m irreduzibel. Für ein beliebiges Polynom $a(x) \neq 0$ vom Grad $\leq m-1$ ist ein multiplikatives Inverses nachzuweisen. Wegen der Irreduzibilität haben $p(x)$ und $a(x)$ keine gemeinsamen Teiler und nach Theorem A.8 existieren dann Polynome $s(x)$ und $t(x)$ mit

$$1 = \mathrm{GCD}(p(x), a(x)) = s(x)p(x) + t(x)a(x).$$

Daraus folgt

$$1 = R_{p(x)}[t(x)a(x)] = R_{p(x)}[R_{p(x)}[t(x)] \cdot a(x)]$$

und somit ist $R_{p(x)}[t(x)]$ invers zu $a(x)$.

"⇒": Es ist zu zeigen, daß die Existenz eines multiplikativen Inversen die Irreduzibilität von $p(x)$ impliziert. Gegenannahme: $p(x) = \alpha(x)\beta(x)$ zerfällt in zwei Polynome vom Grad ≥ 1. Nach Voraussetzung existiert ein Polynom $\alpha'(x) \in \mathbb{K}[x]$ mit $R_{p(x)}[\alpha'(x)\alpha(x)] = 1$. Aus

$$\beta(x) = R_{p(x)}[\beta(x)] = R_{p(x)}[\alpha'(x)\alpha(x)\beta(x)] = R_{p(x)}[\alpha'(x)p(x)] = 0$$

folgt ein Widerspruch und somit ist $p(x)$ irreduzibel.

"Isomorphie": wird hier nicht gezeigt. ■

Bemerkungen zur Schreibweise: Anstelle der Restklassen wird praktisch natürlich immer mit den Repräsentanten minimalen Grades operiert. Für zwei Polynome $a(x), b(x) \in \mathbb{K}[x]/\langle p(x)\rangle$ vom Grad $\leq m-1$ wird die normale Polynom-Multiplikation in $\mathbb{K}[x]$ als $a(x)b(x)$ geschrieben, bei der also Grade bis $2(m-1)$ auftreten können. Die Multiplikation im Restklassenring könnte als

$$a(x) \odot b(x) = R_{p(x)}[a(x)b(x)] = a(x)b(x) \bmod p(x)$$

geschrieben werden, aber anstelle des Zeichens $\odot$ wird immer die ausführliche Schreibweise mit der normalen Multiplikation verwendet.

Example A.14. Sei $\mathbb{K} = \mathbb{F}_2$.

(1) Für das irreduzible Polynom $p(x) = 1 + x + x^2$ ist

$$\mathbb{F}_2[x] \Big/ \langle 1 + x + x^2 \rangle = \{[0], [1], [x], [1+x]\} \cong \{0, 1, x, 1+x\}$$

nach dem vorangehenden Theorem ein Körper. Wegen $[x^2] = [R_{p(x)}[x^2]] = [x+1]$ entspricht das Rechnen mit den Restklassen dem Rechnen modulo $1 + x + x^2$, d.h. x^2 kann durch $1 + x$ ersetzt werden. Damit ergeben sich folgende Verknüpfungstafeln:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	$1+x$	1
$1+x$	0	$1+x$	1	x

Hierbei gilt beispielsweise $-x = x$, $-(1+x) = 1+x$, $x^{-1} = 1+x$, $(1+x)^{-1} = x$.

(2) Für das reduzible Polynom $p(x) = 1 + x^2 = (1+x)^2$ gilt zwar wieder

$$\mathbb{F}_2[x] \Big/ \langle 1 + x^2 \rangle \cong \{0, 1, x, 1+x\},$$

aber nach dem vorangehenden Theorem kann das kein Körper sein. Wegen $[x^2] = [R_{p(x)}[x^2]] = [1]$ wird beim Rechnen x^2 durch 1 ersetzt und damit ergibt sich zwar die gleiche Additionstafel, aber eine veränderte Multiplikationstafel:

$+$	0	1	x	$1+x$
0	0	1	x	$1+x$
1	1	0	$1+x$	x
x	x	$1+x$	0	1
$1+x$	$1+x$	x	1	0

$\cdot$	0	1	x	$1+x$
0	0	0	0	0
1	0	1	x	$1+x$
x	0	x	1	$1+x$
$1+x$	0	$1+x$	$1+x$	0

Hierbei gibt es keine Polynom $a(x)$ mit $(1+x) \cdot a(x) = 1$, d.h. zu $1+x$ existiert kein multiplikatives Inverses. ■

Example A.15. (1) Die beiden Polynome $x^2 + 1$ und $x^2 - 3$ sind irreduzibel über $\mathbb{F}_7$, da sie keine Nullstelle in $\mathbb{F}_7$ haben. Also sind

$$\begin{aligned} \mathbb{F}_7[x] \Big/ \langle x^2 + 1 \rangle &\cong \{a + b\sqrt{-1} \mid a, b \in \mathbb{F}_7\} \\ \mathbb{F}_7[x] \Big/ \langle x^2 - 3 \rangle &\cong \{u + v\sqrt{3} \mid u, v \in \mathbb{F}_7\} \end{aligned}$$

jeweils Körper mit 49 Elementen, die zueinander und zu $\mathbb{F}_{49}$ isomorph sind. Ein Isomorphismus wird durch $\varphi(a + b\sqrt{-1}) = a + b \cdot 3\sqrt{3}$ vermittelt, denn die Multiplikation erweist sich als strukturgleich (für die Addition ist das trivialerweise erfüllt):

$$\begin{aligned} \varphi(a + b\sqrt{-1}) \cdot \varphi(a' + b'\sqrt{-1}) &= (a + b \cdot 3\sqrt{3}) \cdot (a' + b' \cdot 3\sqrt{3}) \\ &= aa' + 27bb' + (ab' + a'b)3\sqrt{3} \\ &= \varphi(aa' - bb' + (ab' + a'b)\sqrt{-1}) \\ &= \varphi((a + b\sqrt{-1}) \cdot (a' + b'\sqrt{-1})). \end{aligned}$$

Es gilt $0^2 = 0$, $1^2 = 6^2 = 1$, $3^2 = 4^2 = 2$, $2^2 = 5^2 = 4$. Dagegen haben $3, 5, 6$ keine Quadratwurzeln in $\mathbb{F}_7$, wohl aber in $\mathbb{F}_{49}$ wegen $(2\sqrt{-1})^2 = (\sqrt{3})^2 = 3$, $(3\sqrt{-1})^2 = (2\sqrt{3})^2 = 5$, $(\sqrt{-1})^2 = (3\sqrt{3})^2 = 6$. Für die multiplikativen Inversen gilt

$$\begin{aligned} (a + b\sqrt{-1})^{-1} &= \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}\sqrt{-1} \\ (u + v\sqrt{3})^{-1} &= \frac{u}{u^2 - 3v^2} + \frac{-v}{u^2 - 3v^2}\sqrt{3}, \end{aligned}$$

also beispielsweise $(1+\sqrt{-1})^{-1} = 4 + 3\sqrt{-1}$ und $(1+\sqrt{3})^{-1} = 3 + 4\sqrt{3}$.

(2) Die beiden Polynome x^2+1 und x^2-3 sind auch irreduzibel über $\mathbb{Q}$, aber die beiden resultierenden Restklassenkörper sind nicht isomorph zueinander, denn aus der Annahme

$$\begin{aligned} -1 = \varphi(-1) &= \varphi(\sqrt{-1}\cdot\sqrt{-1}) \\ &\stackrel{!}{=} \varphi(\sqrt{-1})\cdot\varphi(\sqrt{-1}) = (u+v\sqrt{3})^2 = u^2+3v^2+2uv\sqrt{3} \end{aligned}$$

mit $u, v \in \mathbb{Q}$ folgt ein Widerspruch. ■

Für $\mathbb{K} = \mathbb{F}_p$ besteht $\mathbb{F}_p[x]/\langle p(x)\rangle$ aus den Polynomen vom Grad $\leq m-1$, deren m Koeffizienten Elemente aus $\mathbb{F}_p$ sind. Es gibt p^m derartige Polynome. Bei irreduziblem $p(x)$ ist also der Restklassenring ein Körper mit $q = p^m$ Elementen, der dem Galois field $\mathbb{F}_q$ entsprechen muß, da die endlichen Körper bis auf Isomorphien eindeutig bestimmt sind:

$$\mathbb{F}_{p^m} \;\cong\; \mathbb{F}_p[x] \Big/ \langle p(x)\rangle. \tag{A.10.7}$$

Nicht nachgewiesen wird hier, daß es die irreduziblen Polynome überhaupt gibt, daß also Galois fields $\mathbb{F}_{p^m}$ zu jeder Primzahl p und jeder natürlichen Zahl m auch tatsächlich existieren. Mit der Methode aus Theorem A.9 können die Galois fields nun konstruiert werden. Um jedoch mehr Einsicht in die Struktur der endlichen Körper zu gewinnen, wird in Kapitel 6 diese Konstruktion wesentlich detaillierter durchgeführt. Dazu werden sogenannte primitive Polynome eingeführt, mit denen die multiplikative Gruppe als zyklisch dargestellt werden kann.

Bei einem $(n,k)_q$-block code besteht jedes Codewort aus n Codesymbolen, die jeweils Elemente von $\mathbb{F}_q$ sind. Die Linearität des Codes (siehe Definition 3.3) prägt sich darin aus, daß die Codemenge $\mathcal{C}$ ein Untervektorraum (der Dimension k) von $\mathbb{F}_q^n$ ist. Wenn jedes Codewort als Polynom vom Grad $\leq n-1$ aufgefaßt wird, ist $\mathcal{C}$ ein Untervektorraum von $\mathbb{F}_q[x]_{n-1}$, also der Menge aller Polynome vom Grad $\leq n-1$ mit Koeffizienten aus $\mathbb{F}_q$.

Bei zyklischen Codes (siehe Kapitel 5) ist es sinnvoll, eine Multiplikation zwischen den Wörtern zu definieren – zwar werden nicht die Codewörter miteinander multipliziert, aber die Infowörter bzw. Infopolynome mit dem generator polynomial. In $\mathbb{F}_q[x]_{n-1}$ ist als Vektorraum natürlich keine Multiplikation erklärt, die ja nicht abgeschlossen wäre. Jedoch kann modulo x^n-1 gerechnet werden, d.h. es wird

$$\mathbb{K}[x]_{n-1} \;\cong\; \mathbb{K}[x] \Big/ \langle x^n - 1\rangle \tag{A.10.8}$$

gesetzt, wobei $\mathbb{K}$ ein allgemeiner Körper ist, der aber in der Anwendung für $\mathbb{F}_q$ steht. Insgesamt gilt also mit einem irreduziblen Polynom $p(x)$ vom Grad m:

$$\mathbb{F}_{p^m}[x]_{n-1} \;\cong\; \left(\left(\mathbb{Z}/\langle p\rangle \right)[x] \Big/ \langle p(x)\rangle \right)[x] \Big/ \langle x^n - 1\rangle. \tag{A.10.9}$$

Bei Codes mit primitiver Blocklänge, die über eine Spektraltransformation beschrieben werden (siehe Kapitel 7), erfolgt mit $n = q - 1 = p^m - 1$ eine weitere Spezialisierung. Aus der Summenformel für die *endliche geometrische Reihe* oder direkt einsehbar folgt

$$x^n - 1 \;=\; (x-1) \cdot \sum_{i=0}^{n-1} x^i. \tag{A.10.10}$$

Da also $x^n - 1$ reduzibel ist, kann $\mathbb{K}[x]_{n-1}$ nach Theorem A.9 kein Körper sein. Die beiden Faktoren in $x^n - 1$ bilden Nullteiler, so daß auch kein Integritätsbereich vorliegt. Auch in $\mathbb{K}[x]_{n-1}$ könnte die Multiplikation als

$$a(x) \odot b(x) = R_{x^n-1}[a(x)b(x)] = a(x)b(x) \bmod x^n - 1$$

mit einem besonderen Zeichen geschrieben werden, aber anstelle von $\odot$ wird immer die ausführliche Schreibweise mit der normalen Multiplikation verwendet.

Theorem A.10. *Sei $\mathbb{K}$ ein beliebiger Körper. Dann sind $\mathbb{K}[x]$ und $\mathbb{K}[x]_{n-1}$ jeweils Hauptidealringe. Jedes Ideal wird dabei durch ein Polynom minimalen Grades erzeugt.*

Beweis für $\mathbb{K}[x]_{n-1}$: Das Nullideal wird durch das Nullpolynom erzeugt. Sei nun $\mathcal{I} \neq \{0\}$ ein Ideal und sei darin das Polynom $r(x) \in \mathcal{I} \setminus \{0\}$ mit minimalem Grad fest gewählt. Für alle $b(x) \in \mathbb{K}[x]_{n-1}$ gilt dann nach Definiton eines Ideals $R_{x^n-1}[r(x)b(x)] \in \mathcal{I}$ und somit folgt $\langle r(x) \rangle \subseteq \mathcal{I}$.

Für ein beliebiges $0 \neq s(x) \in \mathcal{I}$ existieren nach Theorem A.4 Polynome $\alpha(x)$ und $\beta(x)$ mit

$$s(x) = \alpha(x)r(x) + \beta(x) \quad \text{mit} \quad \deg \beta(x) < \deg r(x) < n.$$

Wegen $\deg(\alpha(x)r(x)) = \deg(s(x) - \beta(x)) < n$ folgt nach Definition eines Ideals $\alpha(x)r(x) = R_{x^n-1}[\alpha(x)r(x)] \in \mathcal{I}$ sowie

$$\beta(x) = s(x) - \alpha(x)r(x) = s(x) - R_{x^n-1}[\alpha(x)r(x)] \in \mathcal{I}.$$

Da $r(x)$ minimalen Grad in $\mathcal{I}$ hat, muß folglich $\beta(x) = 0$ sein und somit ergibt sich $s(x) = \alpha(x)r(x)$ als Vielfaches von $r(x)$. Damit folgt $\mathcal{I} \subseteq \langle r(x) \rangle$ und insgesamt $\mathcal{I} = \langle r(x) \rangle$. ■

Lineare Codes werden in Abschnitt 5.1 als zyklisch dadurch definiert, daß die zyklische Verschiebung eines Codewortes wieder ein Codewort ist, d.h. mit $a(x)$ muß auch $R_{x^n-1}[xa(x)]$ ein Codewort sein. Damit erweist sich auch die i-fache zyklische Verschiebung $R_{x^n-1}[x^i a(x)]$ als Codewort. Die zyklische Verschiebung kann also mit der Rechnung modulo $x^n - 1$ sehr kompakt formuliert werden.

Theorem A.11. *Der $(n,k)_q$-block code $\mathcal{C}$ ist genau dann zyklisch, wenn $\mathcal{C}$ ein Ideal in $\mathbb{F}_q[x]_{n-1}$ ist. Somit existiert ein* generator polynomial *$g(x) \in \mathbb{F}_q[x]_{n-1}$ mit*

$$\mathcal{C} \;=\; \langle g(x) \rangle \;=\; \{R_{x^n-1}[u(x)g(x)] \mid u(x) \in \mathbb{F}_q[x]_{n-1}\}. \tag{A.10.11}$$

Proof. "Ein zyklischer Code ist ein Ideal": Wegen der Linearität des Codes ist $\mathcal{C}$ additiv abgeschlossen. Für ein beliebiges $a(x) \in \mathcal{C}$ gilt $R_{x^n-1}[x^i a(x)] \in \mathcal{C}$. Für ein beliebiges $b(x) = \sum_i b_i x^i \in \mathbb{F}_q[x]_{n-1}$ folgt somit wegen der Linearität des Codes

$$R_{x^n-1}[a(x)b(x)] = \sum_i b_i \cdot R_{x^n-1}[x^i b(x)] \in \mathcal{C}$$

und damit ist $\mathcal{C}$ als Ideal nachgewiesen.

"Ein Ideal ist ein zyklischer Code": Ein Ideal $\mathcal{C}$ ist nach Definition eine additive Gruppe. Nach Definition des Ideals gilt weiter $R_{x^n-1}[a(x)b(x)] \in \mathcal{C}$ für jedes $a(x) \in \mathcal{C}$ und $b(x) \in \mathbb{F}_q[x]_{n-1}$. Speziell mit $b \in \mathbb{F}_q$ erweist sich der Code als linear und mit $b(x) = x$ als zyklisch.

Nach Theorem A.10 ist jedes Ideal auch Hauptideal und umgekehrt. Das generator polynomial ist das normierte Polynom minimalen Grades (abgesehen vom Nullpolynom) in $\mathcal{C}$. ■

In Kapitel 5 wird (A.8.11) unter Berücksichtigung der Polynomgrade noch konkreter formuliert und gezeigt, daß als weitere äquivalente Kennzeichnung zyklischer Codes das generator polynomial $g(x)$ ein Teiler von $x^n - 1$ sein muß.