

Information Data Book

2017 Edition



Cambridge University Engineering Department

Revised 2019 & 2021

Information Data Book

2017 version, corrections added in 2019 and 2021

Contents

1	FOURIER TRANSFORMS	1
2	DISCRETE FOURIER TRANSFORMS	2
3	Z-TRANSFORMS	3
4	CONTROL	4
4.1	Stability of the Closed-loop System	4
4.2	Routh-Hurwitz Stability Criteria	4
4.3	Nyquist Stability Criterion	4
4.4	Root Locus	4
4.5	Bode Diagrams	5
5	COMMUNICATION	7
5.1	Analogue Communication	7
5.2	Digital Communication	7
5.3	Wireless Communication	7
6	PROBABILITY AND INFERENCE	9
6.1	Random variables	9
6.2	The multivariate Gaussian distribution	9
7	INFORMATION THEORY	10
7.1	Entropy	10
7.2	Mutual Information	10
7.3	Inequalities	11
7.4	Differential entropy	11
8	CODING THEORY	12
8.1	Linear block codes	12
8.2	Binary LDPC Codes and Message Passing Algorithms	12
8.3	Finite Fields and Reed-Solomon Codes	13

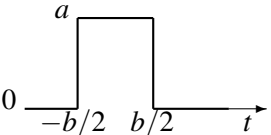
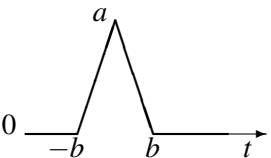
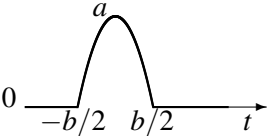
Corrections added in 2019

- Section 6.2: Added missing $\frac{1}{2}$ in the formula of differential entropy of multivariate Gaussian.
- Section 7.1: Removed spurious dx in formula for entropy.
- Section 8.2: Edited the definition of p_t in the density evolution equation.

Corrections added in 2021

- Section 6.2: Missing power of D restored to the formula for the pdf of a multivariate Gaussian distribution.

1 FOURIER TRANSFORMS

Waveform: $g(t) = \frac{1}{2\pi} \int_{-\infty}^{\infty} G(\omega) e^{j\omega t} d\omega$		Spectrum ($\omega = 2\pi f$): $G(\omega) = \int_{-\infty}^{\infty} g(t) e^{-j\omega t} dt$
1	DC level	$2\pi\delta(\omega) = \delta(f)$
$u(t)$	unit step	$\pi\delta(\omega) + \frac{1}{j\omega}$
$e^{j\omega_0 t}$		$2\pi\delta(\omega - \omega_0)$
$\cos(\omega_0 t)$		$\pi[\delta(\omega - \omega_0) + \delta(\omega + \omega_0)]$
$\sin(\omega_0 t)$		$\frac{\pi}{j}[\delta(\omega - \omega_0) - \delta(\omega + \omega_0)]$
$\sum_{n=-\infty}^{\infty} \delta(t - nT)$	impulse train	$\frac{2\pi}{T} \sum_{m=-\infty}^{\infty} \delta\left(\omega - \frac{2\pi m}{T}\right)$
	rectangular pulse	$ab \operatorname{sinc}\left(\frac{\omega b}{2}\right)$ Note: $\operatorname{sinc}(x) = \frac{\sin(x)}{x}$
	triangular pulse	$ab \operatorname{sinc}^2\left(\frac{\omega b}{2}\right)$
	half-cosine pulse	$\frac{ab}{2} \left[\operatorname{sinc}\left(\frac{\omega b - \pi}{2}\right) + \operatorname{sinc}\left(\frac{\omega b + \pi}{2}\right) \right]$
$g(t - t_0)$	time shift	$e^{-j\omega t_0} G(\omega)$
$e^{j\omega_0 t} g(t)$		$G(\omega - \omega_0)$ frequency shift
$\frac{d^n g}{dt^n}$	differentiation	$(j\omega)^n G(\omega)$
$g_1(t) * g_2(t)$ $= \int_{-\infty}^{\infty} g_1(t - \tau) g_2(\tau) d\tau$	convolution	$G_1(\omega) G_2(\omega)$
$g_1(t) g_2(t)$	multiplication	$\frac{1}{2\pi} G_1(\omega) * G_2(\omega) =$ $\frac{1}{2\pi} \int_{-\infty}^{\infty} G_1(\omega - \Omega) G_2(\Omega) d\Omega$

Duality: If $g(t)$ transforms to $p(\omega)$, then $p(t)$ transforms to $2\pi g(-\omega)$.

Symmetry: If $g(t)$ is real, then $G(-\omega) = G^*(\omega)$ (* means complex conjugate).

If $g(t)$ is real and even, then $G(\omega)$ is real and even.

If $g(t)$ is real and odd, then $G(\omega)$ is imaginary and odd.

Caution: Some books handle the 2π factor differently and define transforms with differences in the sign of the exponent.

Parseval's theorem of energy conservation: $\int_{-\infty}^{\infty} |g(t)|^2 dt = \frac{1}{2\pi} \int_{-\infty}^{\infty} |G(\omega)|^2 d\omega$

2 DISCRETE FOURIER TRANSFORMS

The DFT of a sequence $(x_n, n = 0, 1, \dots, N - 1)$ is defined by

$$X_k = \sum_{n=0}^{N-1} x_n e^{-i2\pi kn/N} \quad \text{for } 0 \leq k \leq N - 1$$

with inverse DFT

$$x_n = \frac{1}{N} \sum_{k=0}^{N-1} X_k e^{i2\pi kn/N} \quad \text{for } 0 \leq n \leq N - 1$$

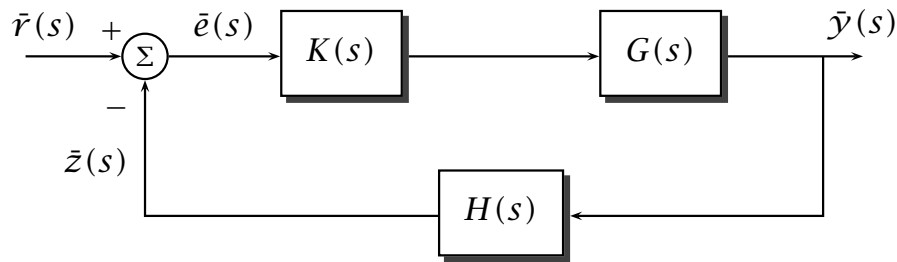
Caution: Some books handle the $\frac{1}{N}$ factor differently and define transforms with differences in signs of the exponent.

If the sequence x_n is obtained by regular sampling of a continuous function $x(t)$ at times $t_n = n/f_0$, where f_0 is the sampling frequency in Hz, the DFT gives a discrete approximation to the frequency spectrum of the continuous function. The total sampling time is $T = N/f_0$, and the frequency spectrum will contain frequencies equally spaced by a resolution $1/T$ Hz, from 0 Hz to the **Nyquist frequency** $f_0/2$.

3 Z-TRANSFORMS

Sequence:	z Transform:
$g_k, k = 0, 1, 2, \dots$	$G(z) = \sum_{k=0}^{\infty} g_k z^{-k}$
1 (unit step)	$\frac{1}{1 - z^{-1}}$
kT	$\frac{Tz^{-1}}{(1 - z^{-1})^2}$
$\frac{(k+m-1)!}{k!(m-1)!}$	$\frac{1}{(1 - z^{-1})^m}$
e^{-akT}	$\frac{1}{1 - e^{-aT}z^{-1}}$
$\sin(\omega_0 kT)$	$\frac{\sin(\omega_0 T)z^{-1}}{1 - 2\cos(\omega_0 T)z^{-1} + z^{-2}}$
$\cos(\omega_0 kT)$	$\frac{1 - \cos(\omega_0 T)z^{-1}}{1 - 2\cos(\omega_0 T)z^{-1} + z^{-2}}$
$\frac{r^{k-1}}{\sin \omega_0 T} [r \sin(\omega_0(k+1)T) - a \sin(\omega_0 kT)]$	$\frac{1 - az^{-1}}{1 - 2r \cos(\omega_0 T)z^{-1} + r^2 z^{-2}}$
$r^k [A \cos(\omega_0 kT) + B \sin(\omega_0 kT)]$	$\frac{A + rz^{-1}(B \sin(\omega_0 T) - A \cos(\omega_0 T))}{1 - 2r \cos(\omega_0 T)z^{-1} + r^2 z^{-2}}$
$r^k g_k$	$G(r^{-1}z)$
g_{k+1}	$zG(z) - zg_0$
g_{k-1}	$z^{-1}G(z) + g_{-1}$
g_{k+m}	$z^m G(z) - z^m g_0 - \dots - zg_{m-1}$
g_{k-m}	$z^{-m} G(z) + z^{-(m-1)} g_{-1} + \dots + g_{-m}$
$g_0 = \lim_{z \rightarrow \infty} G(z)$	(initial value theorem)
$\lim_{k \rightarrow \infty} g_k = \lim_{z \rightarrow 1} (z-1)G(z)$	(final value theorem when poles of $(z-1)G(z)$ are inside unit circle)

4 CONTROL



$$\bar{z}(s) = H(s)G(s)K(s)\bar{e}(s) = L(s)\bar{e}(s)$$

where $L(s) = H(s)G(s)K(s)$ is called the *Return Ratio*.

$$\bar{y}(s) = \frac{G(s)K(s)}{1 + H(s)G(s)K(s)}\bar{r}(s) = \frac{G(s)K(s)}{1 + L(s)}\bar{r}(s)$$

where $\frac{G(s)K(s)}{1+L(s)}$ is the closed-loop transfer function relating y and r .

4.1 Stability of the Closed-loop System

The closed-loop system is stable if the roots of the characteristic equation, $1 + L(s) = 0$, have negative real parts.

4.2 Routh-Hurwitz Stability Criteria

The roots of the polynomial $a_n s^n + a_{n-1} s^{n-1} + \dots + a_0$, with $a_0 > 0$, have negative real part:

for $n = 2$, if and only if all $a_i > 0$;

for $n = 3$, if and only if all $a_i > 0$ and $a_1 a_2 > a_0 a_3$;

for $n = 4$, if and only if all $a_i > 0$ and $a_1 a_2 a_3 > a_0 a_3^2 + a_4 a_1^2$;

(Further relationships exist for $n > 4$.)

For the following conditions it is convenient to write $L(s) = kg(s)$, an explicit function of the gain k .

4.3 Nyquist Stability Criterion

For a stable closed-loop system, the full Nyquist plot of $g(s)$, for $s = j\omega$ and $-\infty < \omega < \infty$, should encircle the $(-\frac{1}{k}, j0)$ point as many times as there are poles of $g(s)$ (i.e. open-loop poles) in the right half of the s -plane. The encirclements, for the path traced by increasing ω , are counted positive in a counterclockwise direction.

4.4 Root Locus

The roots of $1 + kg(s) = 0$, the closed loop poles, trace loci as k varies from 0 to ∞ , starting at the open-loop poles and ending at the open-loop zeros or at infinite distances.

All sections of the real axis with an odd number of poles and zeros to their right are sections of the root locus (even number of poles and zeros to their right if $k < 0$).

At the breakaway points (coincident roots): $\frac{dg}{ds} = 0$.

Angle condition: $\angle g(s) = (2m + 1)\pi$ if $k > 0$ ($\angle g(s) = 2m\pi$ if $k < 0$),

where m is an integer.

Magnitude condition: $|g(s)| = \frac{1}{k}$.

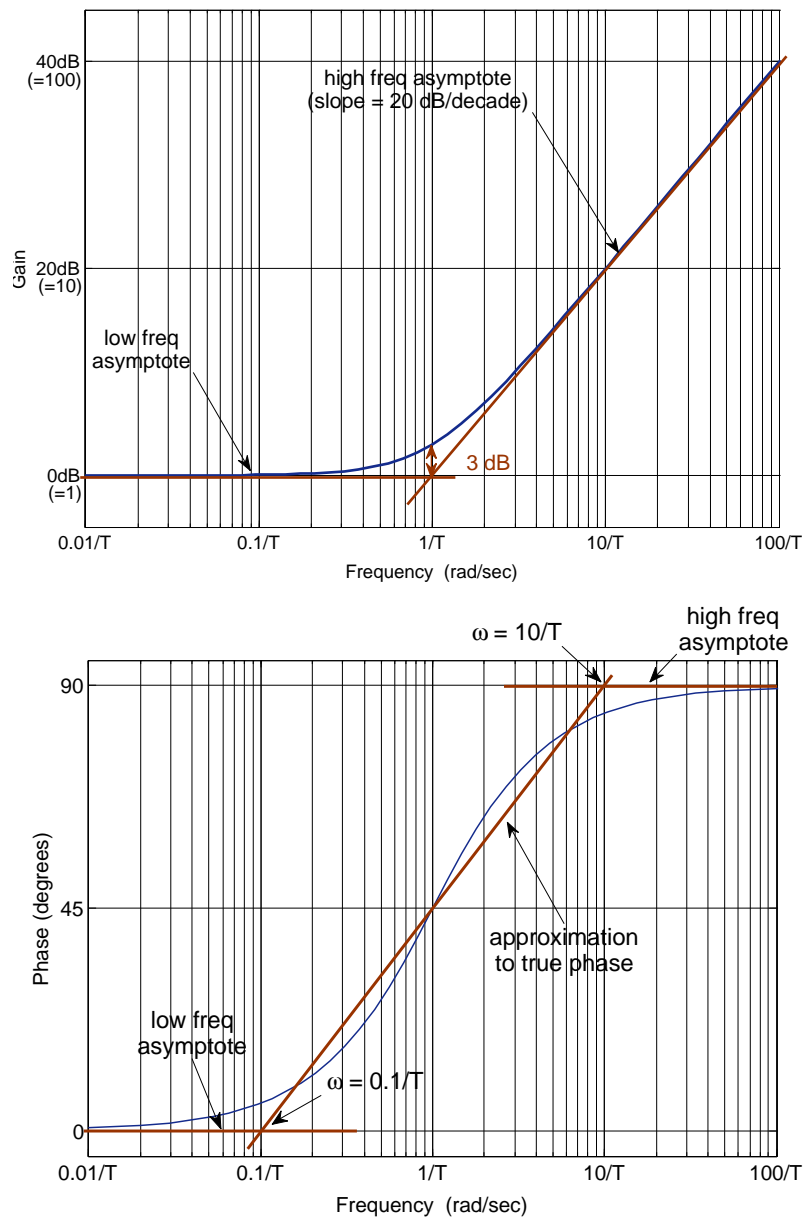
Asymptotes: If $g(s)$ has P poles and Z zeros, the asymptotes of the loci as $k \rightarrow \infty$ are straight lines at angles $\frac{(2m+1)\pi}{P-Z}$ to the real axis if $k > 0$ ($\frac{2m\pi}{P-Z}$ if $k < 0$).

Their point of intersection σ with the real axis is given by:

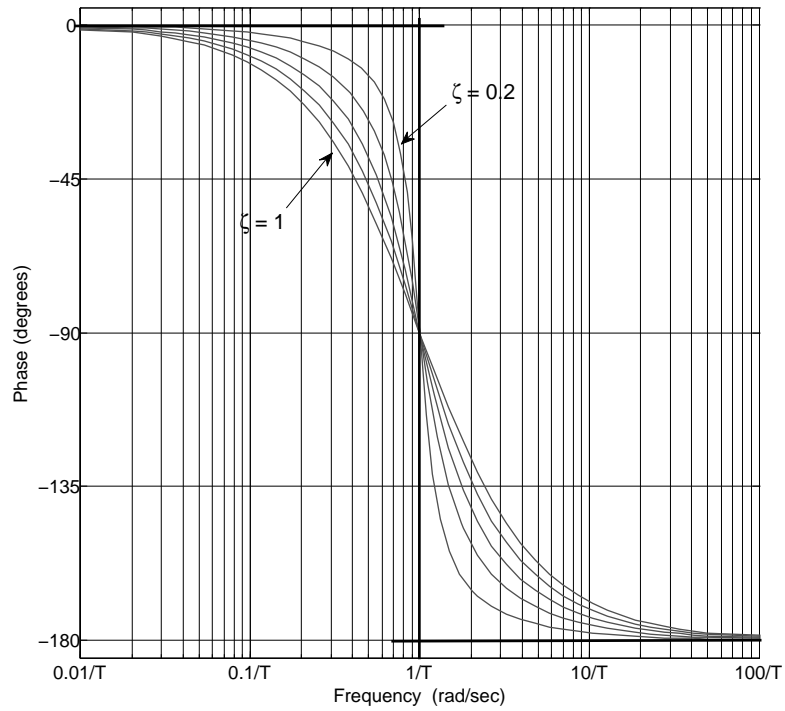
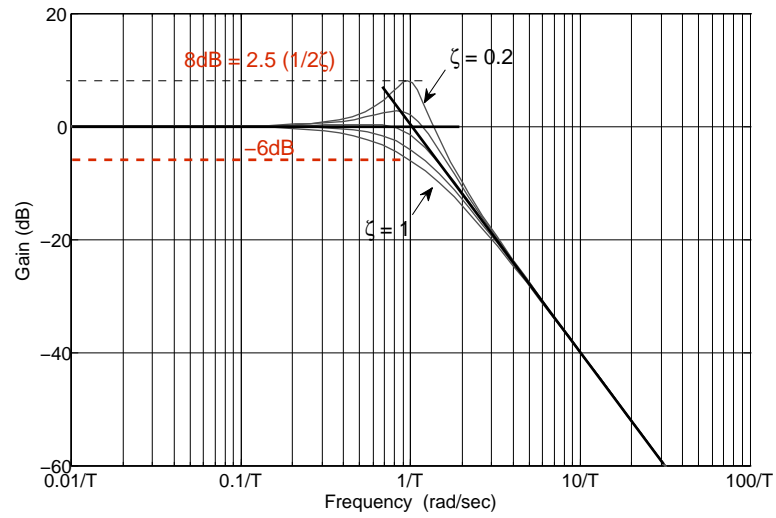
$$\sigma = \frac{\sum(\text{poles of } g(s)) - \sum(\text{zeros of } g(s))}{P - Z}$$

4.5 Bode Diagrams

Bode diagram of $(1 + sT)$:



Bode diagram of $\frac{1}{1 + 2\zeta sT + s^2 T^2}$ for $\zeta = 0.2, 0.4, 0.6, 0.8, 1.0$:



5 COMMUNICATION

5.1 Analogue Communication

- In *amplitude modulation*, the modulated signal $s(t)$ is related to the information signal $x(t)$ by

$$s(t) = [a_0 + x(t)] \cos(2\pi f_c t).$$

The modulation index is $m_A = \frac{\text{Peak amplitude of } x(t)}{a_0}$.

- In *frequency modulation*, the modulated signal $s(t)$ is related to the information signal $x(t)$ by:

$$s(t) = a_0 \cos \left[2\pi f_c t + 2\pi k_F \int_0^t x(u) du \right].$$

The frequency deviation is $\Delta f = k_F$ [maximum amplitude of $x(t)$].

If the information signal is $x(t) = a_x \cos(2\pi f_x t)$, then the modulation index is $m_F = \frac{\Delta f}{f_x} = \frac{k_F a_x}{f_x}$.

- Carson's rule for FM signals: If the information signal has bandwidth W and the frequency deviation is Δf , then

$$\text{Modulated signal bandwidth} \approx 2W + 2\Delta f$$

5.2 Digital Communication

- *Quantisation*: If a sinusoidal signal quantised with an n -bit quantiser, the signal-to-quantisation noise ratio is

$$\text{SNR} = 1.76 + 6.02n \text{ dB}.$$

- In baseband Pulse Amplitude Modulation (PAM), the modulated signal is

$$x(t) = \sum_k X_k p(t - kT),$$

where X_k are information symbols drawn from a real-valued constellation, $p(t)$ is a unit-energy baseband pulse waveform, and T is the symbol period.

- In Quadrature Amplitude Modulation (QAM), the modulated signal is

$$\begin{aligned} x(t) &= \sum_k \text{Re} [X_k e^{j2\pi f_c t}] p(t - kT) \\ &= \sum_k [\text{Re}[X_k] \cos(2\pi f_c t) - \text{Im}[X_k] \sin(2\pi f_c t)] p(t - kT) \\ &= \sum_k |X_k| \cos(2\pi f_c t + \arg(X_k)) p(t - kT). \end{aligned}$$

where X_k are information symbols drawn from a constellation (that can be complex-valued), $p(t)$ is a unit-energy baseband pulse waveform, and T is the symbol period.

5.3 Wireless Communication

- *Complex Gaussians*: $h \sim CN(0, \sigma^2)$ means that h is a complex random variable whose real and imaginary parts are independent Gaussian random variables, each distributed as $N(0, \frac{\sigma^2}{2})$
- If $h \sim CN(0, \sigma^2)$, then the squared-magnitude $|h|^2$ is exponentially distributed, i.e., if $X = |h|^2$, the pdf of X is

$$f_X(x) = \frac{1}{\sigma^2} \exp\left(\frac{-x}{\sigma^2}\right), \quad x \geq 0.$$

- The *Delay Spread* T_d of a multipath fading channel is the maximum difference between delays of the paths from transmitter to receiver. The number of channel taps is $\lceil 2WT_d \rceil$, where W is the one-sided baseband bandwidth of the transmitted signal.
- If $T_d \ll \frac{1}{2W}$, the channel is said to have *flat fading* (no inter-symbol interference). If $T_d > \frac{1}{2W}$, the fading channel has multiple taps and is said to be *frequency selective*.
- The *coherence bandwidth* of the channel is $1/(2T_d)$. If the one-sided baseband bandwidth of the transmitted signal is less than the coherence bandwidth, there will be only one channel tap, i.e., flat fading.

6 PROBABILITY AND INFERENCE

6.1 Random variables

In the following, for a random variable X , $p(x)$ denotes the probability mass function (pmf) if X is discrete-valued, or the probability density function (pdf) if X is continuous-valued.

- Mean or Expected value: discrete: $\mathbb{E}[X] = \sum_x xp(x)$ and continuous: $\mathbb{E}[X] = \int xp(x)dx$.
- Variance: $\mathbb{V}[X] = \mathbb{E}[(X - \mathbb{E}[X])^2] = \mathbb{E}[X^2] - (\mathbb{E}[X])^2$.

For jointly distributed random variables (X, Y) , let $p(x, y)$ denote the joint pmf if (X, Y) are discrete, or the joint pdf if (X, Y) are jointly continuous.

- Conditional pmf/pdf definition: $p(x|y) = \frac{p(x,y)}{p(y)}$, $p(y) \neq 0$.
- The above definition directly gives rise to the product rule: $p(x, y) = p(x|y)p(y)$ and to Bayes' rule: $p(x|y) = \frac{p(y|x)p(x)}{p(y)}$.
- Sum rule for the discrete case: $p(x) = \sum_y p(x, y)$, and for the continuous case: $p(x) = \int_y p(x, y)dy$.
- Covariance: $\mathbb{V}(X, Y) = \mathbb{E}[(X - \mathbb{E}[X])(Y - \mathbb{E}[Y])] = \mathbb{E}[XY] - \mathbb{E}[X]\mathbb{E}[Y]$.

6.2 The multivariate Gaussian distribution

A D -dimensional Gaussian random vector \mathbf{X} with mean vector $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{\Sigma}$ has a joint pdf given by

$$N(\mathbf{x}; \boldsymbol{\mu}, \boldsymbol{\Sigma}) = \frac{1}{\sqrt{(2\pi)^D |\boldsymbol{\Sigma}|}} \exp\left(-\frac{1}{2}(\mathbf{x} - \boldsymbol{\mu})^\top \boldsymbol{\Sigma}^{-1}(\mathbf{x} - \boldsymbol{\mu})\right).$$

Here $\boldsymbol{\mu}$ is a D -dimensional vector, $\boldsymbol{\Sigma}$ is a $D \times D$ positive definite symmetric matrix, and $|\boldsymbol{\Sigma}|$ its determinant.

- If \mathbf{x} and \mathbf{y} are jointly Gaussian random vectors with joint pdf

$$p\left(\begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}\right) = N\left(\begin{bmatrix} \mathbf{x} \\ \mathbf{y} \end{bmatrix}; \begin{bmatrix} \mathbf{a} \\ \mathbf{b} \end{bmatrix}, \begin{bmatrix} A & C \\ C^\top & B \end{bmatrix}\right),$$

then the conditional pdf: $p(\mathbf{x}|\mathbf{y}) = N(\mathbf{x}; \mathbf{a} + CB^{-1}(\mathbf{y} - \mathbf{b}), A - CB^{-1}C^\top)$, and the marginal pdf: $p(\mathbf{x}) = N(\mathbf{x}; \mathbf{a}, A)$.

- Linear projection: $p(\mathbf{x}) = N(\mathbf{x}; \boldsymbol{\mu}, \boldsymbol{\Sigma})$ and $\mathbf{y} = A\mathbf{x} + \mathbf{b}$, then $p(\mathbf{y}) = N(\mathbf{y}; A\boldsymbol{\mu} + \mathbf{b}, A\boldsymbol{\Sigma}A^\top)$.
- The product of Gaussian densities is an un-normalised Gaussian:

$$N(\mathbf{x}; \mathbf{a}, A)N(\mathbf{x}; \mathbf{b}, B) = Z^{-1}N(\mathbf{x}; \mathbf{c}, C),$$

where $C = (A^{-1} + B^{-1})^{-1}$, $\mathbf{c} = C(A^{-1}\mathbf{a} + B^{-1}\mathbf{b})$, and the normalising constant is Gaussian in both \mathbf{a} and \mathbf{b} : $Z^{-1} = (2\pi)^{-D/2} |A + B|^{-1/2} \exp(-\frac{1}{2}(\mathbf{a} - \mathbf{b})^\top (A + B)^{-1}(\mathbf{a} - \mathbf{b}))$.

- The (differential) entropy of a D -dimensional Gaussian random vector \mathbf{X} with pdf $p(\mathbf{x}) = N(\mathbf{x}; \boldsymbol{\mu}, \boldsymbol{\Sigma})$ is

$$h(\mathbf{X}) = \int p(\mathbf{x}) \log \frac{1}{p(\mathbf{x})} d\mathbf{x} = \frac{1}{2} \log((2\pi e)^D |\boldsymbol{\Sigma}|).$$

- KL divergence between Gaussians: if $p(\mathbf{x}) = N(\mathbf{x}; \boldsymbol{\mu}_1, \boldsymbol{\Sigma}_1)$ and $q(\mathbf{x}) = N(\mathbf{x}; \boldsymbol{\mu}_2, \boldsymbol{\Sigma}_2)$, then

$$KL(p, q) = \int p(\mathbf{x}) \log \frac{p(\mathbf{x})}{q(\mathbf{x})} d\mathbf{x} = \frac{1}{2} \left(\log \frac{|\boldsymbol{\Sigma}_2|}{|\boldsymbol{\Sigma}_1|} - D + \text{tr}(\boldsymbol{\Sigma}_2^{-1}\boldsymbol{\Sigma}_1) + (\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2)^\top \boldsymbol{\Sigma}_2^{-1}(\boldsymbol{\mu}_1 - \boldsymbol{\mu}_2) \right).$$

7 INFORMATION THEORY

7.1 Entropy

- The entropy of a discrete random variable X with pmf P is

$$H(X) = \sum_x P(x) \log \frac{1}{P(x)} = -\mathbb{E}[\log(P(x))].$$

The entropy is measured in bits if the log is with base 2, and in nats if the log is base e .

- The *joint entropy* of random variables X_1, \dots, X_n with joint pmf $P_{X_1 \dots X_n}$ is

$$H(X_1, X_2, \dots, X_n) = \sum_{x_1, \dots, x_n} P_{X_1 \dots X_n}(x_1, \dots, x_n) \log \frac{1}{P_{X_1 \dots X_n}(x_1, \dots, x_n)}.$$

- The *conditional entropy* of Y given X is

$$H(Y|X) = \sum_x P_X(x) \underbrace{\sum_y P_{Y|X}(y|x) \log \frac{1}{P_{Y|X}(y|x)}}_{H(Y|X=x)} = \sum_x P_X(x) H(Y|X=x).$$

Note that a similar formula holds if we condition on a collection of random variables (X_1, \dots, X_n) instead of a single random variable X .

- Chain rule for entropy:* The joint entropy of X_1, \dots, X_n can be written as

$$\begin{aligned} H(X_1, X_2, \dots, X_n) &= H(X_1) + H(X_2|X_1) + H(X_3|X_2, X_1) + \dots + H(X_n|X_{n-1}, \dots, X_1) \\ &= \sum_{i=1}^n H(X_i|X_{i-1}, \dots, X_1), \quad \text{where} \end{aligned}$$

$$H(X_i|X_{i-1}, \dots, X_1) = -\sum_{x_1, \dots, x_i} P_{X_1, \dots, X_i}(x_1, \dots, x_i) \log P_{X_i|X_1, \dots, X_{i-1}}(x_i|x_1, \dots, x_{i-1}).$$

- The *relative entropy* or *KL divergence* between two pmfs P and Q (defined on the same alphabet) is

$$D(P||Q) = \sum_{x \in \mathcal{X}} P(x) \log \frac{P(x)}{Q(x)}.$$

7.2 Mutual Information

- The *mutual information* between random variables X and Y with joint pmf P_{XY} is

$$\begin{aligned} I(X;Y) &= H(X) - H(X|Y) \\ &= H(Y) - H(Y|X) \\ &= H(X) + H(Y) - H(X,Y) \\ &= D(P_{XY}||P_X P_Y). \end{aligned}$$

- Chain rule for mutual information:*

$$\begin{aligned} I(X_1, X_2, \dots, X_n; Y) &= I(X_1; Y) + I(X_2; Y|X_1) + \dots + I(X_n; Y|X_{n-1}, \dots, X_1) \\ &= \sum_{i=1}^n I(X_i; Y|X_{i-1}, X_{i-2}, \dots, X_1). \end{aligned}$$

7.3 Inequalities

- *Data-processing inequality*: If X, Y, Z form a Markov chain, then $I(X; Y) \geq I(X; Z)$.

Discrete random variables X, Y, Z are said to form a *Markov chain* if their joint pmf can be written as $P_{XYZ} = P_X P_{Y|X} P_{Z|Y}$.

- *Fano's inequality*: Let X be a random variable taking values in a set \mathcal{X} with cardinality denoted by $|\mathcal{X}|$. Let Y be a random variable jointly distributed with X , and $\hat{X} = f(Y)$ be any estimator of X from Y . Then the probability of error $P_e = \Pr(\hat{X} \neq X)$ satisfies

$$1 + P_e \log |\mathcal{X}| \geq H(X|Y).$$

7.4 Differential entropy

The *differential entropy* of a continuous random variable X with pdf p is

$$h(X) = \int_{-\infty}^{\infty} p(x) \log \frac{1}{p(x)} dx.$$

Joint differential entropy, conditional differential entropy, relative entropy/KL divergence, mutual information, chain rules for continuous random variables are all defined similarly to the discrete case with integrals replacing sums.

The formulas for the differential entropy and KL divergence for Gaussian random vectors are given in Section 6 of this databook.

8 CODING THEORY

8.1 Linear block codes

- A k -dimensional linear block code of codeword length n (an (n, k) linear code) has encoder matrices of size $k \times n$, parity-check matrices of size $(n - k) \times n$, and rate $R = k/n$.
- An (n, k) linear block code has a systematic encoder matrix of the form $\mathbf{G} = [\mathbf{I}_k, \mathbf{P}]$, to which corresponds a parity-check matrix of the form $\mathbf{H} = [-\mathbf{P}^T, \mathbf{I}_{n-k}]$.
- *Singleton Bound*: The minimum distance of any (n, k) block code satisfies $d_{\min} \leq n - k + 1$, with equality for Maximum Distance Separable (MDS) codes.
- A block code with minimum distance d_{\min} is guaranteed to correct any pattern of up to $\lfloor \frac{d_{\min}-1}{2} \rfloor$ errors. It can recover up to $d_{\min} - 1$ erasures.
- The minimum distance d_{\min} of a linear block code is the minimum Hamming weight of any non-zero codeword. For binary codes, it is also the minimum number of columns of \mathbf{H} that add up to the all-zero vector.

8.2 Binary LDPC Codes and Message Passing Algorithms

- Degree polynomials from a node perspective: $L(x) = \sum_{i=1}^{d_v^{\max}} L_i x^i$, $R(x) = \sum_{i=1}^{d_c^{\max}} R_i x^i$.
- Degree polynomials from an edge perspective: $\lambda(x) = \sum_{i=1}^{d_v^{\max}} \lambda_i x^{i-1}$, $\rho(x) = \sum_{i=1}^{d_c^{\max}} \rho_i x^{i-1}$.
- Average degrees $\bar{d}_v = L'(1) = \left(\int_0^1 \lambda(x) dx \right)^{-1}$ and $\bar{d}_c = R'(1) = \left(\int_0^1 \rho(x) dx \right)^{-1}$.
- Design rate of an LDPC code is

$$R = 1 - \frac{\bar{d}_v}{\bar{d}_c} = 1 - \frac{L'(1)}{R'(1)} = 1 - \frac{\int_0^1 \rho(x) dx}{\int_0^1 \lambda(x) dx}.$$

- Density evolution for binary erasure channels with erasure probability ε : The probability p_t of a variable-to-check message along a (randomly picked) edge remaining erased after $t \geq 1$ steps of message passing is

$$p_t = \varepsilon \lambda(1 - \rho(1 - p_{t-1})).$$

(Initialize with $p_0 = \varepsilon$.)

- Log-likelihood ratios for $j = 1, \dots, n$ are $L(y_j) = \ln \frac{P(y_j|c_j=0)}{P(y_j|c_j=1)}$.
- Log-likelihood ratio for a binary-input AWGN channel with inputs $\{+1, -1\}$ and noise variance σ^2 , for an output value y is $L(y) = \frac{2}{\sigma^2} y$.
- Log-likelihood ratio based decoding rules (for sum-product/ belief propagation algorithm), with a check node denoted by i and a variable node by j : The variable-to-check messages are

$$L_{ji} = L(y_j) + \sum_{i' \setminus i} L_{i'j}.$$

and the check-to-variable messages are

$$L_{ij} = 2 \tanh^{-1} \left[\prod_{j' \setminus j} \tanh \left(\frac{L_{j'i}}{2} \right) \right].$$

Here $i' \setminus i$ denotes all the check nodes i' connected to j except i . The notation $j' \setminus j$ is similarly defined.

- Min-sum simplified decoding rule for a check node:

$$\text{sign}(L_{ij}) = \prod_{j' \setminus j} \text{sign}(L_{j'i}) \quad \text{and} \quad |L_{ij}| = \min_{j' \setminus j} (|L_{j'i}|).$$

8.3 Finite Fields and Reed-Solomon Codes

- A Galois Field $\text{GF}(q)$ for $q = p^m$ where p is any prime number consists of a multiplicative group of order $q - 1$ and an additive group of order q .
- The order of an element α in a group is the smallest power ℓ such that $\alpha^\ell = 1$, where 1 is the neutral element of the group.
- *Lagrange Theorem*: The order of a subgroup (and thus the order of any element in a group) divides the order of the group.
- The Discrete Fourier Transform (DFT) of a vector $\mathbf{x} = [x_0, \dots, x_{n-1}]$ with elements over a finite field \mathcal{F} is defined by $X_k = \sum_{m=0}^{n-1} x_m \alpha^{mk}$, for $k = 0, \dots, (n-1)$. Here α must be an element of multiplicative order n in \mathcal{F} .
- The inverse DFT is $x_m = \frac{1}{n^*} \sum_{k=0}^{n-1} X_k \alpha^{-mk}$, for $m = 0, \dots, (n-1)$. Here $n^* = \sum_{j=1}^n 1$, where the sum is taken in \mathcal{F} .
- *Blahut's theorem*: The linear complexity of the DFT of a sequence of length n equals the Hamming weight of the sequence, provided the Hamming weight is less than $n/2$.
- *Reed-Solomon code*: An (n, k) linear code over $\text{GF}(q)$ with a parity-check matrix $\mathbf{H} = [\alpha^{ij}]$ for $i = 0, \dots, (n-k-1)$, and $j = 0, \dots, (n-1)$, where α is an element of multiplicative order n in $\text{GF}(q)$.
- A Reed-Solomon code has rate $R = k/n$, has minimum distance $d_{\min} = n - k + 1$ and hence satisfies the singleton bound with equality, i.e., it is Maximum Distance Separable (MDS).